Introduction to Factorization and Primality Testing

R. C. Vaughan

Pennsylvania State University

20th November 2024

Contents

Preface

This book is based on courses at Penn State University. It contains typically enough material for about thirty six hours of presentations and nine to twelve hours of problem solving and tutorials. All the exercises have been used at least once for homework or the basis of examination questions.

One word of warning. This is a subject which demands proofs, and it would be wise to also have some facility with constructing simple proofs in good English. If one wishes to understand the reasons for a particular phenomenon this can often only be seen by understanding why the proof works.

The ultimate aim of the course is to attempt the factorization of rather large numbers, for example with 65 or more decimal digits. Thus it is essential the student has some facility in writing computer programs, and should have available a programming language that facilitates multiple precision calculations, such as Pari-gp `https://pari.math.u-bordeaux.fr/`

Chapter 1

Background

1.1 Introduction

We are concerned with the basic theory and practice of the factorization of integers into primes. This combines the development and understanding of some quite deep mathematics with the creation of detailed computer programs.

It is essential that the reader should have some familiarity with the concept of mathematical proof. Factorization algorithms and primality tests give absolute proof for their assertions, and have to take account of all possibilities. Nevertheless a proof can be very easy. For example the statement

$$105 = 3.5.7$$

is a one-line proof of the factorization of 105.

A slightly longer example is the statement that $101 = d.q + r$ with

$$d = 2, q = 50, r = 1$$
$$d = 3, q = 33, r = 2$$
$$d = 5, q = 20, r = 1$$
$$d = 7, q = 14, r = 3$$

which gives a proof that 101 is prime.

How about a not very big number like

$$100006561?$$

Is this prime, and if not what are its factors? Anybody care to try it by hand?

And how about somewhat bigger numbers

$$11111111111111111 \quad \text{17 digits,}$$
$$111111111111111111 \quad \text{19 digits.}$$

One of them is prime, the other composite.

If you want to experiment I suggest using the package PARI which runs on most computer systems and is available at

`https://pari.math.u-bordeaux.fr/`

Here is an example where a bit of theory is useful. There is a theorem of Fermat which says that if p is prime, then 2^{p-1} leaves the remainder 1 on division by p. Now 2^{1000} leaves the remainder 562 on division by 1001, so 1001 has to be composite. Checking 2^{1000} might seem difficult but it is actually quite easy.

$$1000 = 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9, 2^{1000} = 2^{2^3}2^{2^5}2^{2^6}2^{2^7}2^{2^8}2^{2^9}$$

and the 2^{2^k} can be computed by successive squaring, so

$$2^{2^3} = 256,\ 2^{2^4} = 256^2 \equiv 471,\ \text{and so on.}$$

Thus any program which can perform double precision multliplication can compute 2^{p-1} modulo p in linear time.

This is a *proofs* based course. One is often asked why one needs formal proofs.There is an instructive example due to J. E. Littlewood in 1912. Let $\pi(x)$ denote the number of prime numbers not exceeding x. Gauss had suggested that

$$\int_0^x \frac{dt}{\log t}$$

should be a good approximation to $\pi(x)$

$$\pi(x) \sim \mathrm{li}(x).$$

For all values of x for which $\pi(x)$ has been calculated it has been found that

$$\pi(x) < \mathrm{li}(x).$$

Here is a table of values which illustrates this for various values of x out to 10^{27}.

x	$\pi(x)$	$\mathrm{li}(x)$	$\mathrm{li}(x) - \pi(x)$
2	1	1.04	0.04
10	4	5.12	1.12
10^2	25	29.08	4.08
10^3	168	176.56	8.56
10^4	1229	1245.09	16.09
10^5	9592	9628.76	36.76
10^6	78498	78626.50	128.50
10^7	664579	664917.36	338.36
10^8	5761455	5762208.33	753.33
10^9	50847534	50849233.90	1699.90
10^{10}	455052511	455055613.54	3102.54
10^{11}	4118054813	4118066399.58	11586.58
10^{12}	37607912018	37607950279.76	38261.76
10^{13}	346065536839	346065458090.05	108969.92
10^{14}	3204941750802	3204942065690.91	314888.91
10^{15}	29844570422669	29844571475286.54	1052617.54
10^{16}	279238341033925	279238344248555.75	3214630.75
10^{17}	2623557157654233	2623557165610820.07	7956587.07
10^{18}	24739954287740860	24739954309690413.98	21949553.98
10^{19}	234057667276344607	234057667376222382.22	99877775.22
10^{20}	2220819602560918840	2220819602783663483.55	222744643.55
10^{21}	21127269486018731928	21127269486616126182.33	597394254.33
10^{22}	201467286689315906290	201467286691248261498.15	1932355208.15
10^{23}	1925320391606803968923		7250186216.00
10^{24}	18435599767349200867866		17146907278.00
10^{25}	176846309399143769411680		55160980939.00
10^{26}	1699246750872437141327603		155891678121.00
10^{27}	16352460426841680446427399		508666658006.00

So is

$$\pi(x) < \mathrm{li}(x)$$

always true?

No! Littlewood in 1914 showed that there are infinitely many values of x for which

$$\pi(x) > \mathrm{li}(x)!$$

We now believe that the first sign change occurs when

$$x \approx 1.387162 \times 10^{316} \tag{1.1}$$

eq:one2011

well beyond what can be calculated directly. For many years it was only known that the first sign change in $\pi(x) - \mathrm{li}(x)$ occurs for *some* x satisfying

$$x < 10^{10^{10^{964}}}.$$

The number on the right was computed by Skewes. G. H. Hardy once wrote that this is probably the largest number which has ever had any *practical* (my emphasis) value! But still even now the only way of establishing this is by a proper mathematical proof.

Let me turn back to that table, as it illustrates something else very interesting. So is it really true that for any $\theta > \frac{1}{2}$ and all large x we have

$$|\pi(x) - \mathrm{li}(x)| < x^{\theta}?$$

This is the famous Riemann Hypothesis, the most important unsolved problem in mathematics. There is a million dollar prize for a proof, or a disproof. And probably an automatic professorship at the most prestigious universities for anyone who wins it. By the way, one might wonder if there is something random in the distribution of the primes. This is how random phenomena are supposed to behave.

1.2 The integers

Number theory in its most basic form is the study of the set of *integers*

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

and its important subset

$$\mathbb{N} = \{1, 2, 3, \ldots\},$$

the set of positive integers, sometimes called the *natural numbers*. The usual rules of arithmetic apply, and can be deduced from a set of axioms. If you multiply any two members of $\mathbb{Z}$ you get another one. Likewise for $\mathbb{N}$. If you subtract one member of $\mathbb{Z}$ from another, e.g.

$$173 - 192 = -19$$

you get a third. But this last fails for $\mathbb{N}$. You can do other standard things in $\mathbb{Z}$, such as

$$x(y + z) = xy + xz$$

and

$$xy = yx$$

is always true.

1.3 Divisibility

To understand factorization we need some concept of divisibility so we start with some definitions. Given two integers a and b we say that a divides b when there is a third integer c such that $ac = b$ and we write $a|b$.

ex:one1 **Example 1.1.** *If $a|b$ and $b|c$, then $a|c$.*

Proof. There are d and e so that $b = ad$ and $c = be$. Hence $a(de) = (ad)e = be = c$ and de is an integer. □

Here are some consequences which are useful. For any a we have $0a = 0$, and if $ab = 1$, then $a = \pm 1$ and $b = \pm 1$ (with the same sign in each case). Also if $a \neq 0$ and $ac = ad$, then $c = d$.

Now we can introduce the concept of a prime number

def:one1 **Definition 1.1.** *A member of* $\mathbb{N}$ *greater than* 1 *which is only divisible by* 1 *and itself is called a prime number.*

We will normally use the letter p to denote a prime number.

ex:one2 **Example 1.2.** 101 *is a prime number.*

Proof. How to prove this? One has to check for divisors d with $1 < d < 100$. Moreover if d is a divisor, then there is an e so that $de = 101$, and one of d, e is $\leq \sqrt{101}$ so we only need to check out to 10. Then we only need to check the primes $2, 3, 5, 7$. Obviously 2 and 5 are not divisors and 3 is easily checked, so only 7 needs any work, and this leaves remainder 3, not 0. □

Since we are dealing with proofs for facts about $\mathbb{N}$ there is one proof method which is very important. This is the principle of induction. It is actually embedded into the definition of $\mathbb{N}$. That is, we have $1 \in \mathbb{N}$ and 1 is the least member of $\mathbb{N}$, and given any $n \in \mathbb{N}$ the next member is $n + 1$. In this way one sees that $\mathbb{N}$ is itself *defined* inductively. Without the following fundamental theorem we could pack up and go home.

thm:one1 **Theorem 1.1.** *Every member of* $\mathbb{N}$ *is a product of prime numbers.*

Proof. 1 is an "empty product" of primes, so the case $n = 1$ holds. Suppose that we have proved the result for every m with $m \leq n$. If $n+1$ is prime we are done. Suppose $n+1$ is not prime. Then there is an a with $a|n+1$ and $1 < a < n+1$. Then also $1 < \frac{n+1}{a} < n+1$. But then on the inductive hypothesis both a and $\frac{n+1}{a}$ are products of primes. □

We can use this to deduce

thm:one2 **Theorem 1.2** (*Euclid*)**.** *There are infinitely many primes.*

Proof. We argue by contradiction. Suppose there are only a finite number of primes. Call them $p_1, p_2, \ldots, p_n$ and consider the number

$$m = p_1 p_2 \ldots p_n + 1.$$

Since we already know some primes it is clear that $m > 1$. Hence it is a product of primes, and in particular there is a prime p which divides m. But p is one of the primes $p_1, p_2, \ldots, p_n$ so $p|m - p_1 p_2 \ldots p_n = 1$. But 1 is not divisible by any prime. So our assumption must have been false. □

Hardy cites this proof as an example of beauty in mathematics.

There is a different proof of the infinitude of primes which is essentially due to Euler, and is analytic in nature and quite different from Euclid's. It tells us more about the distribution of primes and is the beginning of the modern approach. Let

$$S(x) = \sum_{n \le x} \frac{1}{n}.$$

Then

$$S(x) \ge \sum_{n \le x} \int_n^{n+1} \frac{dt}{t} \ge \int_1^x \frac{dt}{t} = \log x.$$

Now consider

$$P(x) = \prod_{p \le x} (1 - 1/p)^{-1}$$

where the product is over the primes not exceeding x. Then

$$P(x) = \prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \ge \sum_{n \le x} \frac{1}{n} \ge \log x.$$

Note that when one multiplies out the left hand side every fraction $\frac{1}{n}$ with $n \le x$ occurs. Since $\log x \to \infty$ as $x \to \infty$, there have to be infinitely many primes. Euler's result on primes is often quoted as follows.

thm:one3 **Theorem 1.3** (Euler)**.** *The sum*

$$\sum_p \frac{1}{p}$$

diverges.

Actually one can get something a bit more precise. Take logs on both sides. Thus

$$-\sum_{p \le x} \log(1 - 1/p) \ge \log\log x.$$

Moreover the expression on the left is

$$-\sum_{p \le x} \log(1 - 1/p) = \sum_{p \le x} \sum_{k=1}^{\infty} \frac{1}{kp^k}.$$

Here the terms with $k \ge 2$ contribute at most

$$\sum_{p \le x} \frac{1}{2} \sum_{k=2}^{\infty} \frac{1}{p^k} \le \frac{1}{2} \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \frac{1}{2}.$$

Hence we have just proved that

$$\sum_{p \le x} \frac{1}{p} \ge \log\log x - \frac{1}{2}.$$

1.3.1 Exercises

Divisibility and Factorisation

1. Let $a, b, c \in \mathbb{Z}$. Prove each of the following.
   (i) $a|a$.
   (ii) If $a|b$ and $b|a$, then $a = \pm b$.
   (iii) If $a|b$ and $b|c$, then $a|c$.
   (iv) If $ac|bc$ and $c \neq 0$, then $a|b$.
   (v) If $a|b$, then $ac|bc$.
   (vi) If $a|b$ and $a|c$, then $a|bx + cy$ for all $x, y \in \mathbb{Z}$.

2. The Fibonacci sequence (1202) is defined iteratively by $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n = 2, 3, \ldots)$. Show that if m, $n \in \mathbb{N}$ satisfy $m|F_n$ and $m|F_{n+1}$, then $m = 1$.

3. Prove that if n is odd, then $8|n^2 - 1$.

4. (i) Show that if m and n are integers of the form $4k + 1$, then so is mn.
   (ii) Show that if $m, n \in \mathbb{N}$, and mn is of the form $4k - 1$, then so is one of m and n.
   (iii) Show that every number of the form $4k - 1$ has a prime factor of this form.
   (iv) Show that there are infinitely many primes of the form $4k - 1$.

5. (i) Show that if m and n are integers of the form $6k + 1$, then so is mn.
   (ii) Show that if $m, n \in \mathbb{N}$, and mn is of the form $6k - 1$, then so is one of m and n.
   (iii) Show that every number of the form $6k - 1$ has a prime factor of this form.
   (iv) Show that there are infinitely many primes of the form $6k - 1$.

6. Show that if p is a prime number and $1 \leq j \leq p - 1$, then p divides the binomial coefficient $\binom{p}{j}$.

7. Show that $n|(n-1)!$ for all composite $n > 4$.

8. Prove that if $2^m + 1$ is an odd prime, then there is an $n \in \mathbb{N}$ such that $m = 2^n$. These are the Fermat primes. Fermat thought that all numbers of the form $2^{2^n} + 1$ are prime. Show that $641|2^{2^5} + 1$.

9. Prove that if n is a natural number and α is a real number, then

$$\sum_{k=0}^{n-1} \left\lfloor \alpha + \frac{k}{n} \right\rfloor = \lfloor n\alpha \rfloor.$$

10. Let $n \in \mathbb{N}$ and p be a prime number, show that the largest t such that $p^t|n$ satisfies

$$t = \sum_{h=1}^{\infty} \left\lfloor \frac{n}{p^h} \right\rfloor.$$

1.4 The fundamental theorem of arithmetic

We now come to something very important

thm:one3a **Theorem 1.4** (The division algorithm)**.** *Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that $a = dq + r, \quad 0 \leq r < d$.*

We call q the quotient and r the remainder.

Proof. Let $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$. If $a \geq 0$, then $a \in \mathcal{D}$, and if $a < 0$, then $a - d(a-1) > 0$. Hence $\mathcal{D}$ has non-negative elements, so has a least non-negative element r. Let $q = x$. Then $a = dq + r, \quad 0 \leq r$. Moreover if $r \geq d$, then $a = d(q+1) + (r-d)$ gives another solution, but with $0 \leq r - d < r$ contradicting the minimality of r.

For uniqueness note that a second solution $a = dq' + r'$, $0 \leq r' < d$ gives $0 = a - a = (dq' + r') - (dq + r) = d(q' - q) + (r' - r)$, and if $q' \neq q$, then $d \leq d|q' - q| = |r' - r| < d$ which is impossible. So $q' = q$ and $r' = r$. □

It is exactly this which one uses when one performs long division

ex:one4 **Example 1.3.** *Try dividing* 17 *into* 192837465 *by the method you were taught at primary school.*

We will make frequent use of the division algorithm

thm:one4 **Theorem 1.5.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote the least positive element. Then (a,b) has the properties

(i) $(a,b)|a$,

(ii) $(a,b)|b$,

(iii) if the integer c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

def:one2 **Definition 1.2.** *The number (a,b) is called the greatest common divisor of a and b. The symbol (a,b) has many uses in mathematics, so to be clear one sometimes writes $GCD(a,b)$.*

Proof. If a is positive, then so is $a.1 + b.0$. Likewise if b is positive. If a is negative, then $a(-1) + b.0$ is positive, and again likewise if b is negative. The only remaining case is $a = b = 0$ which is expressly excluded. Thus $\mathcal{D}(a,b)$ does indeed have positive elements. Thus (a,b) exists. Suppose (i) is false. By the division algorithm we have $a = (a,b)q + r$ with $0 \leq r < (a,b)$. But the falsity of (i) means that $0 < r$. Thus $r = a - (a,b)q = a - (ax + by)q$ for some integers x and y. Hence $r = a(1 - xq) + b(-yq)$. Since $0 < r < (a,b)$ this contradicts the minimality of (a,b).

Likewise for (ii). Now suppose $c|a$ and $c|b$, so that $a = cu$ and $b = cv$ for some integers u and v. Then

$$(a,b) = ax + by = cux + cvy = c(ux + vy)$$

so (iii) holds. □

The GCD has some interesting properties. Here is one

ex:one5 **Example 1.4.** *We have* $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

To see this observe that if $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$, *then* $d|\frac{a}{(a,b)}$ *and* $d|\frac{b}{(a,b)}$, *and hence* $d(a,b)|a$ *and* $d(a,b)|b$. *But then* $d(a,b)|(a,b)$ *and so* $d|1$, *whence* $d = 1$.

Here is another

ex:one6 **Example 1.5.** *Suppose that* a *and* b *are not both* 0. *Then for any integer* x *we have* $(a + bx, b) = (a, b)$. *Here is a proof. First of all* $(a,b)|a$ *and* $(a,b)|b$, *so* $(a,b)|a + bx$. *Hence* $(a,b)|(a + bx, b)$. *On the other hand* $(a + bx, b)|a + bx$ *and* $(a + bx, b)|b$ *so that* $(a + bx)|a + bx - bx = a$. *Hence* $(a + bx, b)|(a,b)|(a + bx, b)$ *and so* $(a,b) = (a + bx, b)$.

Here is yet another

ex:one7 **Example 1.6.** *Suppose that* $(a,b) = 1$ *and* $ax = by$. *Then there is a* z *such that* $x = bz$, $y = az$. *It suffices to show that* $b|x$, *for then the conclusion follows on taking* $z = x/b$. *To see this observe that there are* u *and* v *so that* $au + bv = (a,b) = 1$. *Hence* $x = aux + bvx = byu + bvx = b(yu + vx)$ *and so* $b|x$.

Following from the previous theorem we immediately have the following

thm:one5 **Corollary 1.6.** *Suppose that* a *and* b *are integers not both* 0. *Then there are integers* x *and* y *such that*

$$(a,b) = ax + by.$$

Later we will look at a way of finding suitable x and y in examples. As it stands the theorem gives no constructive way of finding them. It is a pure existence proof. As a first application we establish

thm:one6 **Theorem 1.7** (Euclid)**.** *Suppose that* p *is a prime number, and* a *and* b *are integers such that* $p|ab$. *Then either* $p|a$ *or* $p|b$.

You might think this is obvious, but look at the following

ex:one8 **Example 1.7.** *Consider the set* $\mathcal{A}$ *of integers of the form* $4k + 1$. *If you multiply two of them together, e.g.* $(4k_1 + 1)(4k_2 + 1) = 16k_1k_2 + 4k_2 + 4k_1 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$ *you get another integer of the same kind. We define a "prime"* p *in this system if it is only divisible by* 1 *and itself in the system. Here is a list of "primes" in* $\mathcal{A}$.

$$5, 9, 13, 17, 21, 29, 33, 37, 41, 49 \ldots$$

9 *is one because* 3 *is not in the system. Likewise* 21 *and* 49 *because* 3 *and* 7 *are not in the system. Also the "prime" factorisation of* 45 *is* 5×9. *Now look at* 441. *We have*

$$441 = 9 \times 49 = 21^2.$$

Wait a minute, here factorisation is not unique! The theorem is false in $\mathcal{A}$ *because* $21|9 \times 49$ *but* 21 *does not divide* 9 *or* 49*!*

What is the difference between $\mathbb{Z}$ and $\mathcal{A}$? Well $\mathbb{Z}$ has an additive structure and $\mathcal{A}$ does not. Add two members of $\mathbb{Z}$ and you get another one. Add two members of $\mathcal{A}$ and you get a number which leaves the remainder 2 on division by 4, so is not in $\mathcal{A}$. Amazingly we have to use the additive structure to get something fundamental about the multiplicative structure. This is of huge significance and underpins some of the most fundamental questions in mathematics.

Euclid's theorem. If a or b are 0, then clearly $p|a$ or $p|b$. Thus we may assume $ab \neq 0$. Suppose that $p \nmid a$. We know from the previous theorem that there are x and y so that $(a,p) = ax + py$ and that $(a,p)|p$ and $(a,p)|a$. Since p is prime we must have $(a,p) = 1$ or p. But we are supposing that $p \nmid a$ so $(a,p) \neq p$, i.e. $(a,p) = 1$. Hence $1 = ax + py$. But then $b = abx + pby$ and since $p|ab$ we have $p|b$ as required. □

We can use Euclid's theorem to establish the following

thm:one7 **Theorem 1.8.** *Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and*

$$p|p_1p_2\ldots p_r.$$

Then $p = p_j$ for some j.

Proof. The case $r = 1$ is immediate from the definition of prime. Suppose we have established the r-th case and that we have $p|p_1p_2\ldots p_{r+1}$. Then by the previous theorem we have $p|p_{r+1}$ or $p|p_1p_2\ldots p_r$. In the first case we must have $p = p_{r+1}$. In the second by the inductive hypothesis we must have $p = p_j$ for some j with $1 \leq j \leq r$. □

We can now establish the main result of this section.

thm:one8 **Theorem 1.9** (The Fundamental Theorem of Arithmetic)**.** *Factorization into primes is unique apart from the order of the factors. More precisely if a is a non-zero integer and $a \neq \pm 1$, then*

$$a = (\pm 1)p_1p_2\ldots p_r$$

for some $r \geq 1$ and prime numbers $p_1, \ldots, p_r$, and r and the choice of sign is unique and the primes p_j are unique apart from their ordering.

Proof. Clearly we may suppose that $a > 0$ and hence $a \geq 2$. Theorem 1.1 tells us that a will be a product of r primes, say $a = p_1p_2\ldots p_r$ with $r \geq 1$. It remains to prove uniqueness. We prove that by induction on r. Suppose $r = 1$ and it is another product of primes $a = p'_1\ldots p'_s$ where $s \geq 1$. Then $p'_1|p_1$ and so $p'_1 = p_1$ and $p'_2\ldots p'_s = 1$, whence $s = 1$ also. Now suppose that $r \geq 1$ and we have established uniqueness for all products of r primes, and we have a product of $r+1$ primes, and

$$a = p_1p_2\ldots p_{r+1} = p'_1\ldots p'_s.$$

Then we see from the previous theorem that $p'_1 = p_j$ for some j and then

$$p'_2\ldots p'_s = p_1p_2\ldots p_{r+1}/p_j$$

and we can apply the inductive hypothesis to obtain the desired conclusion. □

There are various other properties of GCDs which can now be described.

Suppose a and b are positive integers. Then by the previous theorem we can write

$$a = p_1^{r_1} \dots p_k^{r_k}, \quad b = p_1^{s_1} \dots p_k^{s_k}$$

where the $p_1, \dots p_k$ are the different primes in the factorization of a and b and we allow the possibility that the exponents r_j and s_j may be zero. Then it can be checked easily that

$$(a, b) = p_1^{\min(r_1, s_1)} \dots p_k^{\min(r_k, s_k)}$$

and this could be taken as the definition of GCD. We can now introduce the idea of the least common multiple

def:one3 **Definition 1.3.** *The least common multiple LCM*

$$[a, b] = \frac{ab}{(a, b)}$$

of a and b is defined by

$$[a, b] = p_1^{\max(r_1, s_1)} \dots p_k^{\max(r_k, s_k)}.$$

Then $LCM[a, b]$ has the property that it is the smallest positive integer c so that $a|c$ and $b|c$.

At this point it is useful to remind ourselves of some further terminology

def:one4 **Definition 1.4.** *A composite number is a number $n \in \mathbb{N}$ with $n > 1$ which is not prime. In particular a compositie number n can be written*

$$n = m_1 m_2$$

with $1 < m_1 < n$, and so $1 < m_2 < n$ also.

1.4.1 Exercises

1. Suppose that $l, m, n \in \mathbb{N}$. Prove that $(lm, ln) = l(m, n)$.

2. The squarefree numbers are the natural numbers which have no repeated prime factors, e.g 6, 105. Note that 1 is the only natural number which is both squarefree and a perfect square. Prove that every $n \in \mathbb{N}$ can be written uniquely as the product of a perfect square and a squarefree number.

3. Let $a, b, c \in \mathbb{Z}$ with a and b not both zero. Prove each of the following.
   (i) If $(a, b) = 1$ and $a|bc$, then $a|c$.
   (ii) $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
   (iii) $(a, b) = (a + cb, b)$.

4. Show that if $(a, b) = 1$, then $(a - b, a + b) = 1$ or 2. Exactly when is the value 2?

5. Show that if $ad - bc = \pm 1$, then $(a + b, c + d) = 1$.

6. Suppose that a, $b \in \mathbb{N}$. Prove that $(a, b)[a, b] = ab$.

7. Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Prove that the equations $(x, y) = a$ and $xy = b$ can be solved simultaneously in integers x and y if and only if $a^2|b$.

8. Prove that if $m \in \mathbb{N}$ and $n \in \mathbb{N}$, then there are integers a, b such that $(a, b) = m$ and $[a, b] = n$ if and only if $m|n$.

9. Let $a, b, c, d \in \mathbb{Z}$ with ab and cd not both 0. Prove that

$$(ab, cd) = (a, c)(b, d)\left(\frac{a}{(a, c)}, \frac{d}{(b, d)}\right)\left(\frac{c}{(a, c)}, \frac{b}{(b, d)}\right).$$

10. Prove that there are no positive integers a, b, n with $n > 1$ such that

$$(a^n - b^n)|(a^n + b^n).$$

1.5 Trial Division

As I hope was clear from the example 101 the simplest way to try to factorize a number n is by trial division. If n has a proper factor m_1, so that $n = m_1 m_2$ with $1 < m_1 < n$, whence $1 < m_2 < n$ also, then we can suppose that $m_1 \leq m_2$. Hence $m_1^2 \leq m_1 m_2 = n$ and

$$m_1 \leq \sqrt{n}.$$

Thus we can try each $m_1 \leq \sqrt{n}$ in turn. If we find no such factor, then we can deduce that n is prime.

Since the smallest proper divisor of n has to be the smallest prime factor of n we need only check the primes p with

$$2 \leq p \leq \sqrt{n}.$$

Even so, for large n this is hugely expensive in time. The number $\pi(x)$ of primes $p \leq x$ is approximately

$$\pi(x) \sim \int_2^x \frac{d\alpha}{\log \alpha} \sim \frac{x}{\log x}$$

where log denotes the natural logarithm. Thus if n is about k bits in size and turns out to be prime or the product of two primes of about the same size, then the number of operations will be

$$\approx \frac{2^{k/2}}{\frac{k}{2}\log 2}.$$

Still exponential in the bit size.

Trial division is feasible for n out to about 40 bits on a modern PC. Much beyond that it becomes hopeless.

One area where trial division, or sophisticated variants thereof, are useful is in the production of tables of primes, or counts of primes such as the value of $\pi(x)$. This is how the table I showed you earlier with gives values of $\pi(x)$ for $x \leq 10^{27}$ was constructed. The simplest form of this is the 'Sieve of Eratosthenes'. Construct a $\lfloor\sqrt{N}\rfloor \times \lfloor\sqrt{N}\rfloor$ array. Here $N = 100$.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Forget about 0 and 1, and then for each successive element remaining remove the proper multiples. Thus for 2 we remove $4, 6, 8, \ldots, 98$.

X	X	2	3	X	5	X	7	X	9
X	11	X	13	X	15	X	17	X	19
X	21	X	23	X	25	X	27	X	29
X	31	X	33	X	35	X	37	X	39
X	41	X	43	X	45	X	47	X	49
X	51	X	53	X	55	X	57	X	59
X	61	X	63	X	65	X	67	X	69
X	71	X	73	X	75	X	77	X	79
X	81	X	83	X	85	X	87	X	89
X	91	X	93	X	95	X	97	X	99

Then for the next remaining element 3 remove $6, 9, \ldots, 99$.

X	X	2	3	X	5	X	7	X	X
X	11	X	13	X	X	X	17	X	19
X	X	X	23	X	25	X	X	X	29
X	31	X	X	X	35	X	37	X	X
X	41	X	43	X	X	X	47	X	49
X	X	X	53	X	55	X	X	X	59
X	61	X	X	X	65	X	67	X	X
X	71	X	73	X	X	X	77	X	79
X	X	X	83	X	85	X	X	X	89
X	91	X	X	X	95	X	97	X	X

Likewise for 5 and 7.

X	X	2	3	X	5	X	7	X	X
X	11	X	13	X	X	X	17	X	19
X	X	X	23	X	X	X	X	X	29
X	31	X	X	X	X	X	37	X	X
X	41	X	43	X	X	X	47	X	X
X	X	X	53	X	X	X	X	X	59
X	61	X	X	X	X	X	67	X	X
X	71	X	73	X	X	X	X	X	79
X	X	X	83	X	X	X	X	X	89
X	X	X	X	X	X	X	97	X	X

After that the next remaining element is 11 and for that and its successors all the proper multiples have already been removed. Thus we now have a table of all the primes $p \leq 100$. This is relatively efficient. The sieve of Eratosthenes produces approximately

$$\frac{n}{\log n}$$

numbers in about

$$\sum_{p \leq \sqrt{n}} \frac{n}{p} \sim n \log \log n$$

operations. Another big constraint is storage.

Now by counting the entries that remain one finds that

$$\pi(100) = 25,$$

1.5.1 Exercises

1. Use trial division to factorize 221 and 223.

1.6 Differences of Squares

Here is an idea that goes back to Fermat. Given n suppose we can find integers x and y so that

$$n = x^2 - y^2, \quad 0 \leq y < x.$$

Since the polynomial on the right factorises as

$$(x - y)(x + y)$$

maybe we have a way of factoring n. We are only likely to try this if n is odd, say

$$n = 2k + 1$$

and then we might run in to

$$n = 2k + 1 = (k + 1)^2 - k^2 = 1.(2k + 1)$$

which does not help much. Of course if n is prime, then perforce $x - y = 1$ and $x + y = 2k + 1$ so this would be the only solution. But if we could find a solution with $x - y > 1$, then that would show that n is composite and would give a factorization.

Moreover if

$$n = m_1 m_2$$

with n odd and $m_1 \leq m_2$, then m_1 and m_2 are both odd and there is a solution with

$$x - y = m_1,\ x + y = m_2,\ x = \frac{m_2 + m_1}{2},\ y = \frac{m_2 - m_1}{2}.$$

ex:one9 **Example 1.8.**

$$91 = 100 - 9 = 10^2 - 3^2,$$

$$x = 10,\ y = 3,\ m_1 = x - y = 7,\ m_2 = x + y = 13.$$

ex:one10 **Example 1.9.**

$$1001 = 2025 - 1024 = 45^2 - 32^2$$

$$x = 45,\ y = 32,\ m_1 = x - y = 13,\ m_2 = x + y = 77.$$

$$1001 = 13 \times 77 = 7 \times 11 \times 13.$$

This method has the obvious downside that $x^2 = n + y^2$ so already one is searching among x which are greater than $\sqrt{n}$ and one could end up searching among that many possibilities. The chances of solving this easily for large n are quite small. Nevertheless we will see that this is a very fruitful idea. For example suppose instead of $n = x^2 - y^2$ we could solve

$$x^2 - y^2 = kn$$

for a relatively small value of k such that

$$1 < x - y < x + y < kn.$$

It is not very likely that $x - y$ or $x + y$ are factors of n, but if we could compute

$$g = GCD(x + y, n)$$

then we might find that g differs from 1 or n and so gives a factorization. Moreover there is a very fast way of computing greatest common divisors.

ex:one11 **Example 1.10.** *Let $n = 10001$. Then*

$$8n = 80008 = 80089 - 81 = 283^2 - 9^2 = 274 \times 292.$$

Now

$$GCD(292, 10001) = 73,\ 10001 = 73 \times 137$$

We will come back to this, but as a first step we want to explore the computation of greatest common divisors. We also want to find fast ways of solving equations like

$$kn = x^2 - y^2.$$

1.6.1 Exercises

1. Factorise 9991.

1.7 The Floor Function

There is a function which we will use from time to time. This is the floor function. It is defined for all real numbers.

def:one5 **Definition 1.5.** *For real numbers α we define the* **floor function** $\lfloor \alpha \rfloor$ *to be the largest integer not exceeding α.*

Occasionally it is also useful to define the **ceiling function** $\lceil x \rceil$ *as the smallest integer u such that $x \leq u$. The difference $x - \lfloor x \rfloor$ is often called* **the fractional part** *of x and is sometimes denoted by $\{x\}$.*

ex:one12 **Example 1.11.** $\lfloor \pi \rfloor = 3$, $\lceil \pi \rceil = 4$, $\lfloor \sqrt{2} \rfloor = 1$, $\lfloor -\sqrt{2} \rfloor = -2$, $\lceil -\sqrt{2} \rceil = -1$.

The floor function has some useful properties.

thm:one9 **Theorem 1.10** (Properties of the floor function)**.** *(i) For any $x \in \mathbb{R}$ we have $0 \leq x - \lfloor x \rfloor < 1$.*
(ii) For any $x \in \mathbb{R}$ and $k \in \mathbb{Z}$ we have $\lfloor x + k \rfloor = \lfloor x \rfloor + k$.
(iii) For any $x \in \mathbb{R}$ and any $n \in \mathbb{N}$ we have $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$.
(iv) For any $x, y \in \mathbb{R}$ we have $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.

Proof. (i) For any $x \in \mathbb{R}$ we have $0 \leq x - \lfloor x \rfloor < 1$. This is pretty obvious. If $x - \lfloor x \rfloor < 0$, then $x < \lfloor x \rfloor$ contradicting the definition. If $1 \leq x - \lfloor x \rfloor$, then $1 + \lfloor x \rfloor \leq x$ also contradicting the definition. This also shows that $\lfloor x \rfloor$ is unique.

(ii) For any $x \in \mathbb{R}$ and $k \in \mathbb{Z}$ we have $\lfloor x + k \rfloor = \lfloor x \rfloor + k$. One way to see this is to observe that by (i) we have $x = \lfloor x \rfloor + \theta$ for some θ with $0 \leq \theta < 1$. Then $x + k - \lfloor x \rfloor - k = \theta$ and since there is only one integer l with $0 \leq x + k - l < 1$, and this l is $\lfloor x + k \rfloor$ we must have $\lfloor x + k \rfloor = \lfloor x \rfloor + k$.

(iii) For any $x \in \mathbb{R}$ and any $n \in \mathbb{N}$ we have $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$. We know by (i) that $\theta = x/n - \lfloor x/n \rfloor$ satisfies $0 \leq \theta < 1$. Now $x = n\lfloor x/n \rfloor + n\theta$ and so by (ii) $\lfloor x \rfloor = n\lfloor x/n \rfloor + \lfloor n\theta \rfloor$. Hence $\lfloor x \rfloor / n = \lfloor x/n \rfloor + \lfloor n\theta \rfloor / n$ and so $\lfloor x/n \rfloor \leq \lfloor x \rfloor / n < \lfloor x/n \rfloor + 1$ and so $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$.

(iv) For any $x, y \in \mathbb{R}$ we have $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$. Put $x = \lfloor x \rfloor + \theta$ and $y = \lfloor y \rfloor + \phi$ where $0 \leq \theta, \phi < 1$. Then $\lfloor x + y \rfloor = \lfloor \theta + \phi \rfloor + \lfloor x \rfloor + \lfloor y \rfloor$ and $0 \leq \theta + \phi < 2$. □

1.7.1 Exercises

1. Prove that if n is a natural number and α is a real number, then

$$\sum_{k=0}^{n-1} \left\lfloor \alpha + \frac{k}{n} \right\rfloor = \lfloor n\alpha \rfloor.$$

2. Let $n \in \mathbb{N}$ and p be a prime number, show that the largest t such that $p^t | n$ satisfies

$$t = \sum_{h=1}^{\infty} \left\lfloor \frac{n}{p^h} \right\rfloor .$$

1.8 Notes

§1 Littlewood's theorem is in J. E. Littlewood, J. E. (1914). "Sur la distribution des nombres premiers", Comptes Rendus, 158, 1869–1872. The number (1.1) is computed in D. Stoll, P. Demichel (2011), "The impact of $\zeta(s)$ complex zeros on $\pi(x)$ for $x < 10^{10^{13}}$", Mathematics of Computation, 80 (276), 2381–2394. Skewes work is in S. Skewes (1933), "On the difference $\pi(x) - \mathrm{li}(x)$", Journal of the London Mathematical Society, 8, 277–283 and S. Skewes (1955), "On the difference $\pi(x) - \mathrm{li}(x)$ (II)", Proceedings of the London Mathematical Society, 5, 48–70.

The seminal paper of B. Riemann (1860) stating a connection between π and the zeros of the Riemann zeta function is "Über die Anzahl der Primzahlen unter einer gegebenen Grösse", Monatsberichte der Königlichen Preussichen Akademie der Wissenschaften zu Berlin aus dem Jahre 1859, 671-680. The first proofs of the prime number theorem are by J. Hadamard (1896), "Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques", Bull. Soc. Math. France 24, 199-220 and Charles-Jean Étienne Gustave Nicolas, baron de la Vallée Poussin (1896), "Recherches analytiques sur la théorie des nombres premiers", I–III, Ann. Soc. Sci. Bruxelles 20, 183–256,281–362, 363–397. The strongest form we currently know of the prime number theorem which does not assume any unproven hypothesis is in N. M. Korobov (1958), "Weyl's estimates of sums and the distribution of primes", Dokl. Akad. Nauk SSSR 123, 28–31 and "Estimates of trigonometric sums and their applications", Uspehi Mat. Nauk, 13(4 (82)), 185–192, and I. M. Vinogradov (1958), "A new evaluation of $\zeta(1+it)$", Izv. Akad. Nauk SSSR 22, 161-164, again independently (Vinogradov is a little hand-wavy and, presumably mistakenly, omits the $\log\log$ factor). The result is

$$\pi(x) - \mathrm{li}(x) \ll x \exp\left(-\frac{C(\log x)^{3/5}}{(\log\log x)^{1/5}} \right)$$

for some positive constant C.

Fermat's theorem is and its generalizations due to Euler is discussed in Chapter 3.

§2 The usual approach to the definition of $\mathbb{N}$ and $\mathbb{Z}$ is to assume $\mathbb{N}$ satisfies a version of the Peano axioms

N1. 1 is a natural number.

N2. Every natural number has a successor which is also a natural number.

N3. 1 is not the successor of any natural number.

N4. If the successor of x equals the successor of y then $x = y$

N5. **Induction Axiom.** If a statement $S(n)$ is true for $n = 1$, and if for each $n \in \mathbb{N}$ the truth of $S(n)$ implies the truth for the successor of n, then the statement is true for every $n \in \mathbb{N}$.

There is an increasing tendency to include 0 in $\mathbb{N}$ and make it play the rôle of 1 in the above axioms, and then define 1 to be the successor of 0. Perhaps the most satisfying way of defining $\mathbb{N}$ is due to Von Neumann.

One can also axiomatise $\mathbb{Z}$ by supposing that there are two operations $+$ and $\times$ and an order relationship $<$ on pairs of elements of $\mathbb{Z}$ such that for every $a, b, c \in \mathbb{Z}$ we have

Z1 Closure. $a + b \in \mathbb{Z}$, $a \times b \in \mathbb{Z}$.

Z2 Associativity. $a + (b + c) = (a + b) + c$, $a \times (b \times c) = (a \times b) \times c$.

Z3 Commutativity. $a + b = b + a$, $a \times b = b \times a$.

Z4 Identities. There are elements 0 and $1 \in \mathbb{Z}$ such that $a + 0 = a$, $a \times 1 = a$.

Z5 Inverse. Given $a \in \mathbb{Z}$ there is an element $(-a) \in \mathbb{Z}$ such that $a + (-a) = 0$.

Z6 Distributivity. $a \times (b + c) = (a \times b) + (a \times c)$ and $(a + b) \times c = (a \times c) + (b \times c)$.

Z7 No zero divisors. If $a \times b = 0$, then $a = 0$ or $b = 0$.

Z8 Order. Exactly one of $a < b$, $a = b$, $b < a$ holds.

Z9 Order $+$. If $a < b$, then $a + c < b + c$.

Z10 Order $\times$. If $a < b$ and $0 < c$, then $a \times c < b \times c$.

By dividing the ordered pairs $(m, n) \in \mathbb{N}^2$ into equivalence classes by putting in the same class those (m, n), (m', n') for which $m + n' = m' + n$ one can construct $\mathbb{Z}$ from $\mathbb{N}$. One can then spend considerable effort deducing all the usual rules of arithmetic from these axioms. For more details see the Wikipedia articles on Natural Numbers and Integers.

§3 The Dirichlet box principle is usually attributed to a paper of J. P. G. L. Dirichlet from 1834, although it does appear to have been known as early as 1624. See `https://en.wikipedia.org/wiki/Pigeonhole_principle`

§4 The division algorithm is in Euclid, Book VII, Proposition 1.

The fundamental theorem of arithmetic in special cases is buried in Euclid Book VII and Book IX.

§5 Trial division was first described by Fibonacci in his book "Liber Abaci" of 1202.

Chapter 2

Euclid's algorithm

ch:two

2.1 Euclid's algorithm

sec:two1

The question arises. We know that given integers a, b not both 0, there are integers x and y so that

$$(a, b) = ax + by. \tag{2.1}$$ eq:two1

How do we find x and y? A method for solving this problem, known as Euclid's algorithm, first appeared in Euclid's *Elements* more than 2000 years ago. Moreover this solution gives a very efficient algorithm and it is still the basis for many numerical methods in arithmetical applications. For example in factorisation routines.

We may certainly suppose that $a > 0$ and $b > 0$ since multiplying either by (-1) does not change the (a, b) - we can replace x by $-x$ and y by $-y$. We can also suppose that $b \leq a$, and in practice that $b < a$. For convenience of notation put $r_0 = b$, $r_{-1} = a$. Now apply the division algorithm iteratively as follows

$$\begin{aligned}
r_{-1} &= r_0 q_1 + r_1, \quad 0 < r_1 \leq r_0, \\
r_0 &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{s-3} &= r_{s-2} q_{s-1} + r_{s-1}, \quad 0 < r_{s-1} < r_{s-2}, \\
r_{s-2} &= r_{s-1} q_s.
\end{aligned}$$

That is, we stop the moment that there is a remainder equal to 0. This could be r_1 if $b|a$, for example, although the way it is written out above it is as if s is at least 3. The important point is that because $r_j < r_{j-1}$, sooner or later we must have a zero remainder.

Euclid proved that $(a, b) = r_{s-1}$. This is easy to see. First of all we know that $(a, b)|a$ and $(a, b)|b$. Thus from the first line we have $(a, b)|r_1$. Repeating this argument we get that successively $(a, b)|r_j$ for $j = 2, 3, \dots, s-1$. On the other hand, starting at the bottom line $r_{s-1}|r_{s-2}$, $r_{s-1}|r_{s-3}$ and so on until we have $r_{s-1}|b$ and $r_{s-1}|a$. Recall that this means

that $r_{s-1}|(a,b)$. Thus we have just proved that

$$r_{s-1}|(a,b), \quad (a,b)|r_{s-1}$$

and so $r_{s-1} = (a,b)$.

Example 2.1. *Let* $a = 10678$, $b = 42$

$$\begin{aligned} 10678 &= 42 \times 254 + 10 \\ 42 &= 10 \times 4 + 2 \\ 10 &= 2 \times 5. \end{aligned}$$

Thus $(10678, 42) = 2$.

But how to compute the x and y in $(a,b) = ax + by$? We could just work backwards through the algorithm using back substitution, but this is tedious and computationally wasteful since it requires all our calculations to be stored. A simpler way is as follows.

alg:Euclid **Algorithm 2.1 (Extended Euclid Algorithm).** *Define* $r\_1 = a$, $r_0 = b$, $x_{-1} = 1$, $y_{-1} = 0$, $x_0 = 0$, $y_0 = 1$ *and then lay the calculations out as follows.*

$$\begin{array}{lll} r_{-1} = r_0 q_1 + r_1, & x_1 = x_{-1} - q_1 x_0, & y_1 = y_{-1} - q_1 y_0 \\ r_0 = r_1 q_2 + r_2, & x_2 = x_0 - q_2 x_1, & y_2 = y_0 - q_2 y_1 \\ r_1 = r_2 q_3 + r_3, & x_3 = x_1 - q_3 x_2, & y_3 = y_1 - q_3 y_2 \\ \vdots & \vdots & \vdots \\ r_{s-3} = r_{s-2} q_{s-1} + r_{s-1}, & x_{s-1} = x_{s-3} - q_{s-1} x_{s-2}, & y_{s-1} = y_{s-3} - q_{s-1} y_{s-2} \\ r_{s-2} = r_{s-1} q_s. & & \end{array}$$

Now the claim is that we have $x = x_{s-1}$, $y = y_{s-1}$.

More generally we have

$$r_j = ax_j + by_j \tag{2.2}$$ eq:one

and again this can be proved by induction. First, by construction we have

$$r_{-1} = ax_{-1} + by_{-1}, \quad r_0 = ax_0 + by_0.$$

Suppose we have established (2.2) for all $j \le k$. Then

$$\begin{aligned} r_{k+1} &= r_{k-1} - q_{k+1} r_k \\ &= (ax_{k-1} + by_{k-1}) - q_{k+1}(ax_k + by_k) \\ &= ax_{k+1} + by_{k+1}. \end{aligned}$$

In particular

$$(a,b) = r_{s-1} = ax_{s-1} + by_{s-1}.$$

Hence laying out the example above in this expanded form we have

$$r_{-1} = 10678,\ r_0 = 42,\ x_{-1} = 1,\ x_0 = 0,\ y_{-1} = 0,\ y_0 = 1,$$

$$\begin{array}{lll} 10678 = 42 \times 254 + 10, & x_1 = 1 - 254 \times 0 = 1, & y_1 = 0 - 1 \times 254 = -254 \\ 42 = 10 \times 4 + 2, & x_2 = 0 - 4 \times 1 = -4, & y_2 = 1 - 4 \times (-254) = 1017 \\ 10 = 2 \times 5. & & \end{array}$$

$$(10678, 42) = 2 = 10678 \times (-4) + 42 \times (1017).$$

It is also possible to set this up using matrices. Lay out the sequences in rows

$$\begin{array}{lll} r_{-1}, & x_{-1}, & y_{-1} \\ r_0, & x_0, & y_0 \\ \vdots & \vdots & \vdots \end{array}$$

Now proceed to compute each successive row as follows. If the s-th row is the last one to be computed, calculate $q_s = \lfloor r_{s-1}/r_s \rfloor$. Then take the last two rows computed and pre multiply by $(1, -q_s)$

$$(1, -q_s) \begin{pmatrix} r_{s-1}, & x_{s-1}, & y_{s-1} \\ r_s, & x_s, & y_s \end{pmatrix} = (r_{s+1}, x_{s+1}, y_{s+1})$$

to obtain the $s+1$-st row.

Example 2.2. *Let $a = 4343$, $b = 973$. We can lay this out as follows*

	4343	1	0
4	973	0	1
2	451	1	−4
6	71	−2	9
2	25	13	−58
1	21	−28	125
5	4	41	−183
	1	−233	1040

Thus $(4343, 973) = 1 = (-233)4343 + (1040)973$.

2.1.1 Exercises

1. Find integers x and y such that $182x + 1155y = (182, 1155)$.

2. Let $\{F_n : n = 0, 1, \ldots\}$ be the Fibonacci sequence defined by $F_0 = 1$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ and let

$$\theta = \frac{1 + \sqrt{5}}{2} = 1.6180339887498948482045868343656\ldots.$$

(i) Prove that

$$F_n = \frac{\theta^n - (-\theta)^{-n}}{\sqrt{5}}.$$

(ii) Suppose that a and b are positive integers with $b < a$ and we adopt the notation used in the description of Euclid's algorithm above. Prove that for $k = 0, 1, \ldots, s-1$ we have $F_k \leq r_{s-1-k}$ and

$$s \leq 1 + \frac{\log 2b\sqrt{5}}{\log \theta}.$$

This shows that Euclid's algorithm runs in time at most linear in the bit size of $\min(a, b)$.

2.2 Linear Diophantine Equations

We can use Euclid's algorithm to find the complete solution in integers to linear diophantine equations of the kind

$$ax + by = c.$$

Here a, b, c are integers and we wish to find all integers x and y which satisfy this. There are some obvious necessary conditions. First of all if $a = b = 0$, then it is not soluble unless $c = 0$ and then it is soluble by any x and y, which is not very interesting. Thus it makes sense to suppose that one of a or b is non-zero. Then since (a, b) divides the left hand side, we can only have solutions if $(a, b)|c$. If we choose x and y so that $ax + by = (a, b)$, then we have

$$a(xc/(a, b)) + b(yc/(a, b)) = (ax + by)c/(a, b) = c$$

so we certainly have a solution of our equation. Call it x_0, y_0. Now consider any other solution. Then

$$ax + by - ax_0 - by_0 = c - c = 0.$$

Thus

$$a(x - x_0) = b(y_0 - y).$$

Hence

$$\frac{a}{(a, b)}(x - x_0) = \frac{b}{(a, b)}(y_0 - y).$$

Then since

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$$

we have by an earlier example that $y_0 - y = z\frac{a}{(a,b)}$ and $x - x_0 = z\frac{b}{(a,b)}$ for some integer z. But any x and y of this form give a solution, so we have found the complete solution set.

Theorem 2.1. *Suppose that a and b are not both 0 and $(a,b)|c$. Suppose further that $ax_0 + by_0 = c$. Then every solution of*

$$ax + by = c$$

is given by

$$x = x_0 + z\frac{b}{(a,b)}, \quad y = y_0 - z\frac{a}{(a,b)}$$

where z is any integer.

One can see here that the solutions x all leave the same remainder on division by $\frac{b}{(a,b)}$ and likewise for y on division by $\frac{a}{(a,b)}$. This suggests that there may be a useful way of classifying integers.

2.2.1 Exercises

1. Find all pairs of integers x and y such that $922x + 2163y = 7$.

2. Find all pairs of integers x and y such that $812x + 2013y = 5$.

3. Find $(1819, 3587)$, and find the complete solution in integers x and y to $1819x+3587y = (1819, 3587)$.

4. Find integers x and y such that $1547x + 2197y = (1547, 2197)$.

5. Find integers m and n so that

$$4709m + 6188n = (4709, 6188).$$

6. Let $n_1, n_2, \ldots, n_s \in \mathbb{Z}$. Define the greatest common divisor d of $n_1, n_2, \ldots, n_s$ and prove that there exist integers $m_1, m_2, \ldots, m_s$ such that $n_1m_1 + n_2m_2 + \cdots + n_sm_s = d$.

7. Discuss the solubility of $a_1x_1 + a_2x_2 + \cdots + a_sx_s = c$ in integers.

2.3 An application to factorization

sec:two3

Here is an algorithm due to R. S. Lehmen and based on differences of squares which is a small improvement on trial division.

alg:Lehman **Algorithm 2.2 (R. S. Lehman).** *After trial division this computes a sequence of pairs t, x.*

1. *Apply trial division with $d = 2, 3, \ldots$, $d \le n^{1/3}$.*

2. *For $1 \le t \le n^{1/3} + 1$ consider the numbers x with*

$$\sqrt{4tn} \le x \le \sqrt{4tn + n^{2/3}}.$$

Check each $x^2 - 4tn$ to see if it is a perfect square y^2 (compute $4tn - \lfloor\sqrt{4tn}\rfloor^2$).

3. *If there are x and y such that*

$$x^2 - 4tn = y^2,$$

then compute

$$GCD(x + y, n).$$

4. *If there is no t for which there are x and y, then n is prime.*

Example 2.3. *Let $n = 10001$. Then $\lfloor(10001)^{1/3}\rfloor = 21$.*

Trial division with $d = 2, 3, 5, 7, 11, 13, 17, 19$ finds no factors.

Let $t = 1$, so that $4tn = 40004$. Then

$$\lfloor\sqrt{4n}\rfloor = 200,\ \lfloor\sqrt{4n + n^{2/3}}\rfloor = \lfloor(40445)^{1/2}\rfloor = 201,$$

$$(201)^2 = 40401,\ 397 \neq y^2.$$

Let $t = 2$, so that $4tn = 80008$. Then

$$\lfloor\sqrt{8n}\rfloor = 282,\ \lfloor\sqrt{8n + n^{2/3}}\rfloor = \lfloor(80449)^{1/2}\rfloor = 283,$$

$$x = 283,\ (283)^2 - 8n = 80089 - 80008 = 81 = 9^2,\ y = 9,\ x + y = 292,$$

$$(292, 10001) = 73.$$

The proof that Lehman's algorithm works depends on a subject called *diophantine approximation*. The normal way in to this subject is *via* a topic called continued fractions, which in turn has some connections with Euclid's algorithm. Fortunately we can take a short cut by appealing to a simple theorem of Dirichlet.

thm:two2 **Theorem 2.2** (Dirichlet)**.** *For any real number α and any integer $Q \geq 1$ there exist integers a and q with $1 \leq q \leq Q$ such that*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q(Q+1)}.$$

As an immediate consequence of casting out all common factors of a and q in a/q we have

Corollary 2.3. *The conclusion holds with the additional condition $(a, q) = 1$.*

Before embarking on the proof of the above we use it to show that Lehman's algorithm works.

Proof of Lehman's algorithm. We have to show that when there is a divisor d of n with $n^{1/3} < d \leq n^{1/2}$, then there is a t with $1 \leq t \leq n^{1/3} + 1$ and x, y such that

$$4tn \leq x^2 \leq 4tn + n^{2/3},\ x^2 - y^2 = 4tn.$$

We use Dirichlet's theorem with

$$\alpha = \frac{n}{d^2},\ Q = \left\lfloor \frac{d}{n^{1/3}} \right\rfloor.$$

Since $d > n^{1/3}$ we have $Q > 1$. Thus we know that there are $a \in \mathbb{Z}$, $q \in \mathbb{N}$ such that $1 \leq q \leq Q$ and

$$\left| \frac{n}{d^2} - \frac{a}{q} \right| \leq \frac{1}{q(Q+1)} < \frac{n^{1/3}}{qd},$$

and so

$$\left| \frac{n}{d} q - ad \right| < n^{1/3}.$$

Let

$$x = \frac{n}{d} q + ad,\ y = \left| \frac{n}{d} q - ad \right|,\ t = aq.$$

Then

$$x^2 = \frac{n^2}{d^2} q^2 + 2nqa + a^2 d^2 = y^2 + 4tn.$$

Moreover

$$y^2 < n^{2/3}$$

and

$$t = aq < \frac{n}{d^2} q^2 + n^{1/3} \frac{q}{d} \leq \frac{n}{d^2} Q^2 + n^{1/3} \frac{Q}{d} \leq n^{1/3} + 1.$$

We now return to the proof of Dirichlet's theorem.

Proof. Let I_n denote the interval $\left[\frac{n-1}{Q+1}, \frac{n}{Q+1} \right)$ and consider the Q numbers

$$\{\alpha\},\ \{2\alpha\},\ \ldots,\ \{Q\alpha\}.$$

(Here we use $\{*\} = * - \lfloor * \rfloor$ to denote the "fractional" part). If one of these numbers, say $\{q\alpha\}$, lies in I_1, then we are done. We take $a = \lfloor q\alpha \rfloor$ and then $0 \leq q\alpha - a < \frac{1}{Q+1}$. Similarly when one of the numbers lies in I_{Q+1}, then $1 - \frac{1}{Q+1} \leq q\alpha - \lfloor q\alpha \rfloor < 1$, whence $-\frac{1}{Q+1} \leq q\alpha - (\lfloor q\alpha \rfloor + 1) < 0$ and we can take $a = \lfloor q\alpha \rfloor + 1$.

When neither of these situations occurs the Q numbers must lie in the $Q-1$ intervals $I_2, \ldots, I_Q$, so there must be at least one interval which contains at least two of the numbers (the *pigeon hole principle*, or *box argument*, or *Schubfachprinzip*). Thus there are q_1, q_2 with $q_1 < q_2$ such that $|(\alpha q_2 - \lfloor \alpha q_2 \rfloor) - (\alpha q_1 - \lfloor \alpha q_1 \rfloor)| < \frac{1}{Q+1}$. We put $q = (q_2 - q_1)$, $a = (\lfloor \alpha q_2 \rfloor - \lfloor \alpha q_1 \rfloor)$. □

2.3.1 Computing Square Roots

In applying Lehman's algorithm, and in variants of this method we shall study later, it is necessary sometimes for a positive integer to check whether it is a perfect square, or more generally given n to find $\lfloor\sqrt{n}\rfloor$, and if necessary check whether or not $n = \lfloor\sqrt{n}\rfloor^2$. In any case, the simplest general method is to compute $\sqrt{n}$ to sufficient precision. Now if n is not a perfect square, then

$$1 \leq n^2 - \lfloor\sqrt{n}\rfloor^2 = (n - \lfloor\sqrt{n}\rfloor)(n + \lfloor\sqrt{n}\rfloor)$$

and so

$$\frac{1}{\sqrt{n} + \lfloor\sqrt{n}\rfloor} \leq n - \lfloor\sqrt{n}\rfloor.$$

Moreover we have equality in the special case $n = m^2 + 1$. Thus to be sure that n is not a perfect square we need to compute $n - \lfloor\sqrt{n}\rfloor$ to a precision

$$< \frac{1}{\sqrt{n} + \lfloor\sqrt{n}\rfloor},$$

That is, to a relative precision compared with $\sqrt{n}$ of

$$< \frac{1}{\sqrt{n}(\sqrt{n} + \lfloor\sqrt{n}\rfloor)}.$$

In other words we need at least as many decimal places after the decimal point as before it. Thus we need a rapid way of computing square roots. Fortunately many software packages do include such routines, but one should check. Try taking the square root of $10^{100} - 1$, and then the floor function. The answer should be less than 10^{50}.

Fortunately there is an incredibly rapid way of computing square roots, which goes back to Newton, and is what one would get if one applied the Newton-Raphson method to computing the positive solution to $x^2 - n = 0$.

Newton's Algorithm. *Let n be a positive integer and take x_1 to be a suitable guess to $\sqrt{n}$. One could get away with a rather poor guess, but we will suppose that λ is a constant with*

$$1 \leq \lambda < 1 + \sqrt{2}$$

and assume that

$$\lambda^{-1}\sqrt{n} \leq x_1 \leq \lambda\sqrt{n},$$

Then define inductively

$$x_{j+1} = \frac{1}{2}\left(x_j + \frac{n}{x_j}\right).$$

There are various observations we can make.

1. *It is a simple induction on j to show that $x_j > 0$ for every $j \in \mathbb{N}$.*

2. Squaring both sides and multiplying out gives

$$\begin{aligned} x_{j+1}^2 &= \frac{1}{4}(x_j^2 + 2n + n^2 x_j^{-2}), \\ x_{j+1}^2 - n &= \frac{1}{4}(x_j^2 - 2n + n^2 x_j^{-2}) \\ &= \frac{1}{4}(x_j - n/x_j)^2 \geq 0. \end{aligned}$$

Hence for $j \geq 2$ we have $x_j^2 \geq n$.

3. Again rearranging the original definition gives, for $j \geq 2$

$$x_j - x_{j+1} = \frac{x_j}{2} - \frac{n}{2x_n} = \frac{x_j^2 - n}{2x_j} \geq 0$$

$$x_{j+1} \leq x_j,$$

so $\{x_j : j \geq 2\}$ is decreasing and bounded below.

4. By the monotonic convergence theorem

$$\ell = \lim_{j\to\infty} x_j$$

exists.

5. By 1. and 2. for $j \geq 2$ we have $x_j^2 \geq n$. Thus, since $\ell = \inf\{x_j : j \geq 2\}$ we have $\ell \geq \sqrt{n}$.

6. Now adverting to the definition of x_j, the combination theorem for limits gives

$$\begin{aligned} \ell &= \lim_{j\to\infty} x_{j+1} \\ &= \lim_{j\to\infty} \frac{1}{2}\left(x_j + \frac{n}{2x_j}\right) \\ &= \frac{1}{2}\left(\ell + \frac{n}{2\ell}\right). \end{aligned}$$

Solving for ℓ we have

$$\frac{1}{2}\ell = \frac{n}{2\ell}, \quad \ell^2 = n.$$

7. By 2., when $j \geq 1$ we have

$$0 \leq x_{j+1}^2 - n = \frac{(x_j^2 - n)^2}{4x_j^2}$$

so that for $j \geq 2$

$$\begin{aligned} 0 \leq x_{j+1} - \sqrt{n} &= \frac{(x_j - \sqrt{n})^2 (x_j + \sqrt{n})^2}{4x_j^2 (x_{j+1} + \sqrt{n})} \\ &= \left(1 + \frac{\sqrt{n}}{x_j}\right)^2 \frac{(x_j - \sqrt{n})^2}{4(x_{j+1} + \sqrt{n})} \\ &\leq \frac{(x_j - \sqrt{n})^2}{2\sqrt{n}} \end{aligned}$$

since by 2. we have $x_j \geq \sqrt{n}$. *Thus*

$$0 \leq \frac{x_{j+1} - \sqrt{n}}{\sqrt{n}} \leq \frac{1}{2}\left(\frac{x_j - \sqrt{n}}{\sqrt{n}}\right)^2.$$

Hence by induction on j, *when* $j \geq 2$ *we have*

$$0 < \frac{x_{j+1} - \sqrt{n}}{\sqrt{n}} \leq \frac{1}{2^{j-1}}\left(\frac{x_2 - \sqrt{n}}{\sqrt{n}}\right)^{2^{j-1}}.$$

Morever, by 2.,

$$x_2^2 - n = \frac{1}{4}(x_1 - n/x_1)^2$$

and then by the initial choice of x_1 *we have*

$$\frac{|x_1 - n/x_1|}{2} \leq \theta\sqrt{n}$$

where

$$\theta = \frac{\lambda - 1/\lambda}{2} < 1.$$

Hence

$$0 \leq x^2 - n \leq \theta^2$$

and so

$$0 \leq \frac{x_{j+1} - \sqrt{n}}{\sqrt{n}} \leq \frac{\theta^{2^j}}{2^{j-1}}.$$

The convergence is doubly exponential. Note that with iterative methods of this kind, when one does arithmetic with real numbers on a computer, they are stored as approximations, and one has to be concerned with accumulated rounding errors. Fortunately with the above method there are typically only about $\log\log n$ steps to achieve a suitable approximation.

2.3.2 Exercises

1. Find a non–trivial factor of 19109.
2. Find a non–trivial factor of 39757.
3. Find a non–trivial factor of 238741
4. Find a non–trivial factor of 2048129.
5. Find a non–trivial factor of 3215031751.
6. Find a non–trivial factor of 9912409831
7. Find a non–trivial factor of 37038381852397.
8. Find a non–trivial factor of 341550071728321.

2.4 Notes

§1. The equation (2.1) is called Bézout's identity, and is in É. Bézout (1779), Théorie générale des équations algébriques, Paris, Ph.-D. Pierres. Euclid's algorithm is in Book VII, Propositions 1 and 2.
§3. The algorithm described here is extracted and simplified from R. Sherman Lehman, "Factoring large integers", Math. Comp., 28(1974), 637-646. The proof we give based on Dirichlet's theorem is simpler. See also F. W. Lawrence, "Factorisation of numbers", Messenger of Math., 24(1895), 100-109. For the history of cognate methods see the notes to Chapter 8.

A significant part of this course will be to develop a technique which speeds up considerable the process of finding t, x and y to satisfy $x^2 - y^2 = 4tn$ for very large n.

There is an alternative method which is slower than Newton's method for extracting squareroots, but which has the advantage that it leads directly to $m = \lfloor \sqrt{n} \rfloor$ and so enables an immediate check on whether n is a perfect square. This method simply extracts the digits of m to a given base. There is a description of it at `https://en.wikipedia.org/wiki/Methods_of_computing_square_roots#Digit-by-digit_calculation`

Chapter 3

Congruences and Residue Classes

3.1 Residue Classes

We now introduce a topic that was first developed by Gauss.

def:three1 **Definition 3.1.** *Let $m \in \mathbb{N}$ and define the residue class $\overline{r}$ modulo m by*

$$\overline{r} = \{x \in \mathbb{Z} : m|(x - r)\}.$$

By the division algorithm every integer is in one of the residue classes

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}.$$

This is often called a complete system of residues modulo m.

The remarkable thing is that we can perform arithmetic on the residue classes just as if they were numbers.

The residue class $\overline{0}$ behaves like the number 0. The reason is that $\overline{0}$ just consists of the integral multiples of m and adding any one of them to an element of the residue class $\overline{r}$ does not change the remainder. Thus for any r

$$\overline{0} + \overline{r} = \overline{r} = \overline{r} + \overline{0}.$$

Suppose that we are given any two residue classes $\overline{r}$ and $\overline{s}$ modulo m. Let t be the remainder of $r + s$ on division by m. Then each element of $\overline{r}$ and $\overline{s}$ is of the form $r + mx$ and $s + my$ respectively, and we know that $r + s = t + mz$ for some z. Thus $r + mx + s + my = t + m(z + x + y)$ is in $\overline{t}$, and it is readily seen that the converse is true. Thus it makes sense to write $\overline{r} + \overline{s} = \overline{t}$, and then we have $\overline{r} + \overline{s} = \overline{s} + \overline{r}$.

One can also check that

$$\overline{r} + \overline{-r} = \overline{0}.$$

In connection with this there is a notation that was introduced by Gauss.

def:three2 **Definition 3.2.** *Let $m \in \mathbb{N}$. If two integers x and y satisfy $m|x-y$, then we write*

$$x \equiv y \pmod{m}$$

and we say that x is congruent to y modulo m.

Here are some of the properties of congruences.

$$x \equiv x \pmod{m},$$

$$x \equiv y \pmod{m} \text{ iff } y \equiv x \pmod{m},$$

$$x \equiv y \pmod{m}, y \equiv z \pmod{m} \text{ implies } x \equiv z \pmod{m}.$$

These say that the relationship $\equiv$ is reflexive, symmetric and transitive. Thus congruences modulo m partition the integers into equivalence classes. I leave their proofs as an exercise.

One can also check the following

If $x \equiv y \pmod{m}$ and $z \equiv t \pmod{m}$, then $x+z \equiv y+t \pmod{m}$ and $xz \equiv yt \pmod{m}$.

If $x \equiv y \pmod{m}$, then for any $n \in \mathbb{N}$, $x^n \equiv y^n \pmod{m}$ (use induction on n).

If f is a polynomial with integer coefficients, and $x \equiv y \pmod{m}$, then $f(x) \equiv f(y) \pmod{m}$.

Wait a minute, this means that one can use congruences just like doing arithmetic on the integers!

Here is a very useful result that begins to tell us something about the structure that we have just created.

thm:three1 **Theorem 3.1.** *Suppose that $m \in \mathbb{N}$, $k \in \mathbb{Z}$, $(k,m) = 1$ and*

$$\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$$

form a complete set of residues modulo m. Then so does

$$\overline{ka_1}, \overline{ka_2}, \ldots, \overline{ka_m}.$$

Proof. Since we have m residue classes, we need only check that they are disjoint. Consider any two of them, $\overline{ka_i}$ and $\overline{ka_j}$. Let $ka_i + mx$ and $ka_j + my$ be typical members of each class. If they were the same integer, than $ka_i + mx = ka_j + my$, so that $k(a_i - a_j) = m(y-x)$. But then $m|k(a_i - a_j)$ and since $(k,m) = 1$ we would have $m|a_i - a_j$ so $\overline{a}_i$ and $\overline{a}_j$ would be identical residue classes, which would contradict them being part of a complete system. □

An important rôle is played by the residue classes r modulo m with $(r,m) = 1$. In connection with this we introduce an important arithmetical function ϕ, called Euler's function.

def:three3 **Definition 3.3.** *A real or complex valued function defined on $\mathbb{N}$ is called an arithmetical function.*

def:three4 **Definition 3.4.** *Euler's function $\phi(n)$ is defined to be the number of $x \in \mathbb{N}$ with $1 \leq x \leq n$ and $(x, n) = 1$.*

ex:three1 **Example 3.1.** *Since $(1, 1) = 1$ we have $\phi(1) = 1$.*

If p is prime, then the x with $1 \leq x \leq p - 1$ satisfy $(x, p) = 1$, but $(p, p) = p \neq 1$. Hence $\phi(p) = p - 1$.

The numbers x with $1 \leq x \leq 30$ and $(x, 30) = 1$ are

$$1, 7, 11, 13, 17, 19, 23, 29,$$

so $\phi(30) = 8$.

def:three5 **Definition 3.5.** *A set of $\phi(m)$ distinct residue classes $\overline{r}$ modulo m with $(r, m) = 1$ is called a reduced set of residues modulo m.*

One way of thinking about this is to start from a complete set of fractions with denominator m in the interval $(0, 1]$

$$\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m}{m}.$$

Now remove just the ones whose numerator has a common factor $d > 1$ with m. What is left are the $\phi(m)$ *reduced* fractions with denominator m.

Suppose instead of removing the non-reduced ones we just write them in their lowest form. Then for each divisor k of m we obtain all the reduced fractions with denominator k. In fact we just proved the following.

thm:three2 **Theorem 3.2.** *For each $m \in \mathbb{N}$ we have*

$$\sum_{k|m} \phi(k) = m.$$

Example 3.2. *We have $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(10) = 4$, $\phi(15) = 8$, $\phi(30) = 8$ and*

$$\phi(1) + \phi(2) + \phi(3) + \phi(5) + \phi(6) + \phi(10) + \phi(15) + \phi(30) = 30.$$

Now we can prove a companion theorem to Theorem 3.1 for reduced residue classes.

thm:three3 **Theorem 3.3.** *Suppose that $(k, m) = 1$ and that*

$$a_1, a_2, \ldots, a_{\phi(m)}$$

form a set of reduced residue classes modulo m. Then

$$ka_1, ka_2, \ldots, ka_{\phi(m)}$$

also form a set of reduced residues modulo m.

Proof. In view of the earlier theorem the residue classes ka_j are distinct, and since $(a_j, m) = 1$ we have $(ka_j, m) = 1$ so they give $\phi(m)$ distinct reduced residue classes, so they are all of them in some order. □

We can now begin to examine the structure of complete and reduced systems of residue classes.

thm:three4 **Theorem 3.4.** *Suppose that m, $n \in \mathbb{N}$ and $(m, n) = 1$ and consider the mn numbers*

$$xn + ym$$

with $1 \leq x \leq m$ and $1 \leq y \leq n$. Then they form a complete set of residues modulo mn. If instead x and y are further restricted to $(x, m) = 1$ and $(y, n) = 1$, then they form a reduced set of residues modulo mn.

Proof. In the unrestricted case we have mn objects. Moreover if $xn + ym \equiv x'n + y'm \pmod{mn}$ then we would have $xn \equiv x'n \pmod{m}$, so that $x \equiv x' \pmod{m}$ and thus $x = x'$, and likewise $y = y'$. Hence we have mn distinct residues modulo mn and so a complete set. In the restricted case the same argument shows that the $xn + ym$ are distinct modulo mn. Moreover $(xn + ym, m) = (xn, m) = (x, m) = 1$ and likewise $(xn + ym, n) = 1$, so $(xn + ym, mn) = 1$ and the $xn + ym$ all belong to reduced residue classes. Now let z be an arbitrary reduced residue modulo mn. Choose x' and y' so that $x'n + y'm = 1$ and choose $x \in \overline{x'z}$ modulo m and $y \in \overline{y'z}$ modulo n. Then one can check that $xn + ym \equiv x'zn + y'zm = z \pmod{mn}$ and hence every reduced residue class modulo mn is of the form $\overline{xn + ym}$ with $(x, m) = (y, n) = 1$. □

Example 3.3. *Here is a table of $xn + ym \pmod{mn}$ when $m = 5$, $n = 6$.*

y \ x	1	2	3	4	5
1	11	17	23	29	5
2	16	22	28	4	10
3	21	27	3	9	15
4	26	2	8	14	20
5	1	7	13	19	25
6	6	12	18	24	30

The 30 numbers 1 through 30 appear exactly once each. The 8 reduced residue classes occur precisely in the intersection of rows 1 and 5 and columns 1 through 4.

Immediate from Theorem 3.4 we have

cor:three5 **Corollary 3.5.** *If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

def:three6 **Definition 3.6.** *If an arithmetical function f which is not identically 0 satisfies*

$$f(mn) = f(m)f(n)$$

whenever $(m, n) = 1$ we say that f is multiplicative.

cor:three6 **Corollary 3.6.** *Euler's function is multiplicative.*

This enables a full evaluation of $\phi(n)$. If $n = p^k$, then the number of reduced residue classes modulo p^k is simply the number of x with $1 \leq x \leq p^k$ and $p \nmid x$. This is $p^k - N$ where N is the number of x with $1 \leq x \leq p^k$ and $p|x$, and $N = p^{k-1}$. Thus $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$. Putting this all together gives

thm:three7 **Theorem 3.7.** *Let $n \in \mathbb{N}$. Then*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where, when $n = 1$ we interpret the product as an "empty" product 1.

Example 3.4. *We have $\phi(9) = 6$, $\phi(5) = 4$, $\phi(45) = 24$. Note that $\phi(3) = 2$ and $\phi(9) \neq \phi(3)^2$.*

Here is a beautiful and as we shall see, useful, theorem.

thm:three8 **Theorem 3.8** (Euler)**.** *Suppose that $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, m) = 1$. Then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof. Let

$$a_1, a_2, \ldots, a_{\phi(m)}$$

be a reduced set of residues modulo m. Then

$$aa_1, aa_2, \ldots, aa_{\phi(m)}$$

is another. Hence

$$\begin{aligned} a_1 a_2 \ldots a_{\phi(m)} &\equiv aa_1 aa_2 \ldots aa_{\phi(m)} \pmod{m} \\ &\equiv a_1 a_2 \ldots a_{\phi(m)} a^{\phi(m)} \pmod{m}. \end{aligned}$$

Since $(a_1 a_2 \ldots a_{\phi(m)}, m) = 1$ we may cancel the

$$a_1 a_2 \ldots a_{\phi(m)}.$$

□

cor:three9 **Corollary 3.9** (Fermat)**.** *Let p be a prime number and a an integer. Then*

$$a^p \equiv a \pmod{p}.$$

If $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

One might hope that Fermat's theorem could give a necessary and sufficient condition for primality. Unfortunately it is possible that

$$a^{n-1} \equiv 1 \pmod{n}$$

when n is not prime, although this is rare. Examples of

$$2^{n-1} \equiv 1 \pmod{n}$$

are $n = 341, 561, 645$. Such n are called *pseudoprimes*. There are only 245 less than 10^6, compared with 78498 primes. Moreover

$$3^{341-1} \equiv 56 \neq 1 \pmod{341}$$

suggests a possible primality test. Given n try trial division a few times, say for $d = 2, 3, 5, 7$ and then check successively

$$a^{n-1} \equiv 1 \pmod{n}$$

for $a = 2, 3, 5, 7$. Unfortunately one can still have false positives. Thus

$$561 = 3.11.17$$

satisfies

$$a^{560} \equiv 1 \pmod{561}$$

for *all* a with $(a, 561) = 1$.

def:three8 **Definition 3.7.** *A composite n which satisfies*

$$a^{n-1} \equiv 1 \pmod{n}$$

for all a with $(a, n) = 1$ is called a Carmichael number

There are infinitely many Carmichael numbers. The smallest is 561 and there are 2163 of them below

$$25 \times 10^9.$$

Captain: I am never known to quail At the fury of a gale, and I'm never, never sick at sea!
All: What, never?
Captain: No, never!
All: What, never?
Captain: Hardly ever!

Gilbert & Sullivan, HMS Pinafore, 1878.

def:three9 **Definition 3.8.** *For $n \in \mathbb{N}$ define $M(n) = 2^n - 1$. A Mersenne prime is a prime of the form $M(n)$.*

Note that if n is composite, $n = ab$, then $M(n)$ is composite,

$$M(ab) = (2^a - 1)(2^{a(b-1)} + \cdots + 2^a + 1).$$

Thus for $M(n)$ to be prime it is necessary that n be prime.

Example 3.5. *We have*

$$\begin{aligned} 3 &= 2^2 - 1, \\ 7 &= 2^3 - 1, \\ 31 &= 2^5 - 1 \\ 127 &= 2^7 - 1. \end{aligned}$$

However that is not sufficient

$$2^{11} - 1 = 2047 = 23 \times 89.$$

3.1.1 Exercises

Euler's function, congruences

1. Prove that if m, $n \in \mathbb{N}$ and $(m, n) = 1$, then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

2. For which values of $n \in \mathbb{N}$ is $\phi(n)$ odd?

3. Find all n such that $\phi(n) = 12$.

4. Show that if $f(x)$ is a polynomial with integer coefficients and if $f(a) \equiv k \pmod{m}$, then $f(a + tm) \equiv k \pmod{m}$ for every integer t.

5. Let $f(x)$ denote a polynomial of degree at least 1 with integer coefficients and positive leading coefficient.
   (i) Show that if $f(x_0) = m > 0$, then $f(x) \equiv 0 \pmod{m}$ whenever $x \equiv x_0 \pmod{m}$.
   (ii) Show that there are infinitely many $x \in \mathbb{N}$ such that $f(x)$ is not prime. 6. Suppose that $m_1, m_2 \in \mathbb{N}$, $(m_1, m_2) = 1$, $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ if and only if $a \equiv b \pmod{m_1 m_2}$. 7. Prove that when a natural number is written in the usual decimal notation, (i) it is divisible by 3 if and only if the sum if its digits is divisible by 3 and (ii) it is divisible by 9 if and only if the sum if its digits is divisible by 9.5. Prove that for any integer n
   (i) $n^7 - n$ is divisible by 42,
   (ii) $n^{13} - n$ is divisible by 2730.

8. Prove that if m is an odd positive integer, then the sum of any complete set of residues modulo m is $0 \pmod{m}$. If m is any integer with $m > 2$, then prove the analogous result for any reduced system of residues modulo m.

9. The numbers $F_n = 2^{2^n} + 1$ for $n \geq 0$ are called Fermat numbers. F_0 through F_4 are prime. Fermat had conjectured that F_n is always prime.

(i) Show that $641|F_5$ (Euler 1732).

We now know that $F_5, \ldots, F_{19}$ are composite and it is now conjectured that there are no further Fermat primes!

Suppose that p is a prime with $p|F_n$ and let e denote the smallest positive integer such that $2^e \equiv 1 \pmod{p}$.

(ii) Show that e exists and $e|2^{n+1}$.

(iii) Show that $e \nmid 2^n$.

(iv) Show that $p \equiv 1 \pmod{2^{n+1}}$.

(v) Prove that

$$F_n - 2 = F_{n-1}\big(F_{n-1} - 2\big) = F_{n-1} \ldots F_1 F_0$$

and deduce that if $m \neq n$, then $(F_m, F_n) = 1$.

10. Prove that (i) if $(a, m) = (a - 1, m) = 1$, then

$$1 + a + a^2 + \cdots + a^{\phi(m)-1} \equiv 0 \pmod{m},$$

and

(ii) prove that every prime other than 2 or 5 divides infinitely many of the integers 1, 11, 111, 1111, ...

11. Prove that if p is prime, and $a, b \in \mathbb{Z}$, then

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

12. (i) Prove that if p is an odd prime and $0 < k < p$, then (assuming $0! = 1$) $(p-k)!(k-1)! \equiv (-1)^k \pmod{p}$.

(ii) Prove that if $p \equiv 1 \pmod{4}$, then the congruence $x^2 + 1 \equiv 0 \pmod{p}$ is soluble.

13. Write a program to compute $2^{n-1} \pmod{n}$ and apply it to 12341137 and 12341141 to determine which one is certainly composite.

14. A "probable prime" p is a number such that $a^{p-1} \equiv 1 \pmod{p}$ for $a = 2, 3, 5, 7$. For each of the numbers n with $100000000000 \leq n \leq 100000000025$ list the ones which are probable primes and for those which are not list the values of a for which the test fails.

15. Prove that when a natural number is written in the usual decimal notation, (i) it is divisible by 3 if and only if the sum if its digits is divisible by 3 and (ii) it is divisible by 9 if and only if the sum if its digits is divisible by 9.

16. Show that the last decimal digit of a perfect square cannot be $2, 3, 7$ or 8.

17. Prove that, for any integer a, $6|a(a + 1)(2a + 1)$.

18. Prove that any fourth power must have one of 0, 1, 5, 6 for its unit digit.

19. Let $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ be a sequence of n integers (not necessarily distinct). Show that some non-empty subsequence of $\mathcal{A}$ has a sum which is divisible by n.

20. Let a, b, and x_0 be positive integers and define x_n iteratively for $n \geq 1$ by $x_n = ax_{n-1} + b$. Prove that not all the x_n are prime.

21. The Möbius function $\mu(n)$ is defined as follows. If there is a prime p such that $p^2|n$, then $\mu(n) = 0$. If $n = p_1 \ldots p_k$ where the p_j are distinct, then $\mu(n) = (-1)^k$ (the case k=0 corresponds to $n = 1$).

(i) Prove that μ is a multiplicative function.

(ii) Prove that $f(n) = \sum_{m|n} \mu(m)$ is multiplicative. Here the sum is over all positive divisors m of n. Thus for $n = 12$ it is $\mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$.

(iii) Prove that if p is prime and $k \geq 1$, then $f(p^k) = 0$. Deduce that $f(1) = 1$ but $f(n) = 0$ whenever $n > 1$.

(iv) Prove that $g(n) = \sum_{m|n} \frac{\mu(m)}{m}$ is multiplicative. Deduce that

$$g(n) = \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product is over the distinct prime factors of n.

(v) Prove that $\phi(n) = ng(n)$.

3.2 Linear congruences

Just as linear equations are the easiest to solve, so one might expect that linear congruences

$$ax \equiv b \pmod{m}$$

are the easiest to solve. In fact we have already solved this in principle since it is equivalent to the linear diophantine equation

$$ax + my = b.$$

thm:three9 **Theorem 3.10.** *The congruence*

$$ax \equiv b \pmod{m}$$

is soluble if and only if $(a, m)|b$, and then the general solution is given by the members of a residue class x_0 modulo $m/(a, m)$. The residue class x_0 can be found by applying Euclid's algorithm to solve $ax_0 + my_0 = b$.

Proof. The congruence is equivalent to the equation $ax + my = b$ and there can be no solution if $(a, m) \nmid b$. We know from Euclid's algorithm that if $(a, m)|b$, then

$$\frac{a}{(a,m)}x + \frac{m}{(a,m)}y = \frac{b}{(a,m)}$$

is soluble. Let x_0, y_0 be such a solution. Obviously every member of the residue class x_0 modulo $m/(a, m)$ gives a solution. Let x, y be another solution. Then

$$\frac{a}{(a,m)}(x - x_0) \equiv 0 \pmod{\frac{m}{(a,m)}}$$

and since

$$\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$$

it follows that x is in the residue class x_0 modulo $m/(a, m)$. □

A curious, but sometimes useful, application which uses somewhat similar ideas is the following

thm:three12 **Theorem 3.11** (Wilson)**.** *Let p be a prime number, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. The cases $p = 2$ and $p = 3$ are $(2-1)! = 1 \equiv -1 \pmod 2$ and $(3-1)! = 2 \equiv -1 \pmod 3$. Thus we may suppose that $p \geq 5$. Then $x^2 \equiv 1 \pmod p$ implies $x \equiv \pm 1 \pmod p$. Hence the numbers $2, 3, \ldots, p-2$ can be paired off into $\frac{p-3}{2}$ mutually exclusive pairs a, b such that $ab \equiv 1 \pmod p$. Thus $(p-1)! \equiv p - 1 \equiv -1 \pmod p$. □

This theorem actually gives a necessary and sufficient condition for p to be a prime, since if p were to be composite, then we would have $((p-1)!, p) > 1$. However this is useless since $(p-1)!$ grows very rapidly.

What about simultaneous linear congruences?

$$\begin{cases} a_1 x & \equiv b_1 \pmod{q_1}, \\ \ldots & \ldots \\ a_r x & \equiv b_r \pmod{q_r}. \end{cases} \tag{3.1}$$

There can only be a solution when each individual equation is soluble, so we require $(a_j, q_j)|b_j$ for every j. Then we know that each individual equation is soluble for all the members of some residue class c_j modulo $q_j/(a_j, q_j)$. Thus the above system reduces to a collection of simultaneous congruences

$$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \ldots & \ldots \\ x & \equiv c_r \pmod{m_r} \end{cases} \tag{3.2}$$ eq:three3

for some values of c_j and m_j. Now suppose that for some i and $j \neq i$ we have $(m_i, m_j) = d > 1$. Then x has to satisfy $c_i \equiv x \equiv c_j \pmod{d}$. This imposes further conditions on c_j which can get very complicated. To avoid this one can make the following observations. Suppose that $p_1, \ldots, p_s$ are all the prime factors of $m_1 \ldots m_r$. Then for each j we have

$$m_j = p_1^{u_{1j}} \ldots p_s^{u_{sj}}$$

where the u_{ij} are non-negative integers. Now

$$x \equiv c_j \pmod{m_j}$$

if and only if

$$\begin{cases} x & \equiv c_j \pmod{p_1^{u_{1j}}}, \\ \ldots & \ldots \\ x & \equiv c_j \pmod{p_s^{u_{sj}}}, \end{cases}$$

so we can reduce to the case when all the moduli are prime powers. If a prime divides more than one m_j, so there are i, j, k so that $u_{ij} > 0$ and $u_{ik} > 0$, then we can certainly suppose, if necessary by switching indices, that $0 < u_{ij} \leq u_{ik}$. Moreover there will be no solution unless

$$c_j \equiv c_k \pmod{p_i^{u_{ij}}},$$

and in the latter case every solution of

$$x \equiv c_k \pmod{p_i^{u_{ik}}}$$

will also be a solution of

$$x \equiv c_j \pmod{p_i^{u_{ij}}}.$$

Thus we either have no solution or we can reduce to a system in which each modulus is a power of a different prime. Thus it suffices to study the system $(m_i, m_j) = 1$ when $i \neq j$. Moreover every system can, with some work, be reduced to this case.

thm:three10 **Theorem 3.12** (Chinese Remainder Theorem)**.** *Suppose that $(m_i, m_j) = 1$ for every $i \neq j$. Then the system (3.2) has as its complete solution precisely the members of a unique residue class modulo $m_1 m_2 \ldots m_r$.*

Proof. We first show that there is a solution. Let $M = m_1 m_2 \ldots m_r$ and $M_j = M/m_j$, so that $(M_j, m_j) = 1$. We know that there is an N_j so that $M_j N_j \equiv c_j \pmod{m_j}$ (solve $yM_j \equiv c_j \pmod{m_j}$ in y). Let x be any member of the residue class

$$N_1 M_1 + \cdots + N_r M_r \pmod{M}.$$

Then for every j, since $m_j | M_i$ when $i \neq j$ we have

$$\begin{aligned} x &\equiv N_j M_j \pmod{m_j} \\ &\equiv c_j \pmod{m_j} \end{aligned}$$

so the residue class $x \pmod M$ gives a solution.

Now we have to show that this is unique. Suppose y is also a solution of the system. Then for every j we have

$$\begin{aligned} y &\equiv c_j \pmod{m_j} \\ &\equiv x \pmod{m_j} \end{aligned}$$

and so $m_j | y - x$. Since the m_j are pairwise co-prime we have $M | y - x$, so y is in the residue class x modulo M. □

ex:three2 **Example 3.6.** *Consider the system of congruences*

$$\begin{aligned} x &\equiv 3 \pmod 4, \\ x &\equiv 5 \pmod{21}, \\ x &\equiv 7 \pmod{25}. \end{aligned}$$

We have $m_1 = 4$, $m_2 = 21$, $m_3 = 25$, $M = 2100$, $M_1 = 525$, $M_2 = 100$, $M_3 = 84$. *First we have to solve*

$$\begin{aligned} 525N_1 &\equiv 3 \pmod 4, \\ 100N_2 &\equiv 5 \pmod{21}, \\ 84N_3 &\equiv 7 \pmod{25}. \end{aligned}$$

Reducing the constants gives

$$\begin{aligned} N_1 &\equiv 3 \pmod 4, \\ (-5)N_2 &\equiv 5 \pmod{21}, \\ 9N_3 &\equiv 7 \pmod{25}. \end{aligned}$$

Thus we can take $N_1 = 3$, $N_2 = 20$, $7 \equiv -18 \pmod{25}$ *so* $N_3 \equiv -2 \equiv 23 \pmod{25}$. *Then the complete solution is given by*

$$\begin{aligned} x &\equiv N_1M_1 + N_2M_2 + N_3M_3 \\ &= 3 \times 525 + 20 \times 100 + 23 \times 84 \\ &= 5507 \\ &\equiv 1307 \pmod{2100}. \end{aligned}$$

3.2.1 Exercises

1. Solve where possible.
   (i) $91x \equiv 84 \pmod{143}$
   (ii) $91x \equiv 84 \pmod{147}$

2. Solve $11x \equiv 21 \pmod{105}$.

3. Solve the simultaneous congruences

$$x \equiv 4 \pmod{19}$$
$$x \equiv 5 \pmod{31}$$

4. Solve the simultaneous congruences

$$x \equiv 6 \pmod{17}$$
$$x \equiv 7 \pmod{23}$$

5. Solve the simultaneous congruences

$$x \equiv 3 \pmod{6}$$
$$x \equiv 5 \pmod{35}$$
$$x \equiv 7 \pmod{143}$$
$$x \equiv 11 \pmod{323}$$

6. Eggs in basket problem (Brahmagupta 7th century A.D.). Find the smallest number of eggs such that when eggs are removed 2, 3, 4, 5 or 6 at a time 1 remains, but when eggs are removed 7 at a time none remain.

7. Show that every integer satisfies at least one of the following congruences; $x \equiv 0 \pmod{2}$, $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 1 \pmod{6}$, $x \equiv 11 \pmod{12}$. Such a collection of congruences (with the moduli all different) is known as a covering class. Paul Erdős asked whether there are covering classes with all the moduli arbitrarily large. For a long time it was an open question. Eventually Bob Hough showed that there are none.

3.3 General Polynomial Congruences

The solution of a general polynomial congruence can be quite tricky, even for a polynomial with a single variable

$$f(x) := a_0 + a_1 x + \cdots + a_j x^j + \cdots a_J x^J \equiv 0 \pmod{m} \tag{3.3}$$

eq:threea

where the a_j are integers. The largest k such that $a_k \not\equiv 0 \pmod{m}$ is the degree of f modulo m. If $a_j \equiv 0 \pmod{m}$ for every j, then the degree of f modulo m is not defined, and so does not exist.

We have already seen that

$$x^2 \equiv 1 \pmod 8$$

is solved by any odd x, so that it has four solutions modulo 8, $x \equiv 1,\ 3,\ 5,\ 7 \pmod 8$. That is, more than the degree 2. However, when the modulus is prime we have the more familiar conclusion.

When we have a solution x to a polynomial congruence such as (3.3) we may sometimes refer to such values as a *root* of the polynomial modulo m.

thm:three11 **Theorem 3.13** (Lagrange)**.** *Suppose that p is prime, and $f(x) = a_0 + a_1x + \cdots + a_jx^j + \cdots$ is a polynomial with integer coefficients a_j and it has degree k modulo p. Then the number of incongruent solutions of*

$$f(x) \equiv 0 \pmod p$$

is at most k.

Proof. The case of degree 0 is obvious. Thus we can suppose $k \geq 1$. We use induction on the degree k. If a polynomial f has degree 1 modulo p, so that $f(x) = a_0 + a_1x$ with $p \nmid a_1$, then the congruence becomes

$$a_1x \equiv -a_0 \pmod p$$

and since $a_1 \not\equiv 0 \pmod p$ (because f has degree 1) we know that this is soluble by precisely the members of a unique residue class modulo p.

Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that f has degree $k+1$. If

$$f(x) \equiv 0 \pmod p$$

has no solutions, then we are done. Hence we may suppose it has (at least) one, say $x \equiv x_0 \pmod p$. By the division algorithm for polynomials we have

$$f(x) = (x - x_0)q(x) + f(x_0)$$

where $q(x)$ is a polynomial of degree k with integer coefficients. [To see this observe first that $x^j - x_0^j = (x - x_0)(x^{j-1} + x^{j-2}x_0 + \cdots x_0^{j-1})$ and so collecting together the terms we get $f(x) - f(x_0) = (x - x_0)q(x)$. Moreover the leading coefficient of $q(x)$ is $a_k \not\equiv 0 \pmod p$]. But $f(x_0) \equiv 0 \pmod p$, so that

$$f(x) \equiv (x - x_0)q(x) \pmod p$$

If $f(x_1) \equiv 0 \pmod p$, with $x_1 \not\equiv x_0 \pmod p$, then $p \nmid x_1 - x_0$ so that $p|q(x_1)$. [Note that if the modulus is not prime we cannot make this deduction; $m_1m_2|ab$ could hold because $m_1|a$ and $m_2|b$]. By the inductive hypothesis there are at most k possibilities for x_1, so at most $k+1$ in all. □

It is useful at this stage to consider generally the number of solutions of a polynomial congruence.

def:three7 **Definition 3.9.** *Suppose that f is a polynomial with integer coefficients. Given a modulus $m \in \mathbb{N}$, we define the $N_f(m)$ to be the number of different residue classes x modulo m such that $f(x) \equiv 0 \pmod{m}$.*

For example when $f(x) = x^2 - 1$ we have $N_f(8) = 4$, and for an odd prime p, $N_f(p) = 2$, but $N_f(2) = 1$. If $g(x) = x^2 + 5$, then $N_g(2) = 1$, $N_g(3) = 2$, $N_g(5) = 1$, $N_g(7) = 2$, $N_g(11) = 0$, $N_g(21) = 4$. Is there a general formula here? The answer is yes, but we don't yet have the tools to decide this. To get the last example you could compute all 21 values modulo 21, but it is easier to use the following.

thm:three14 **Theorem 3.14.** *Suppose that f is a polynomial with integer coefficients. Then $N_f(m)$ is a multiplicative function of m.*

Note that in the first case above $N_f(8) \neq N_f(2)^3$.

Proof. Suppose that $(m_1, m_2) = 1$. Choose n_j so that $n_2 m_2 \equiv 1 \pmod{m_1}$ and $n_1 m_1 \equiv 1 \pmod{m_2}$. Suppose that x_1, x_2 are such that $f(x_j) \equiv 0 \pmod{m_j}$. Let

$$x \equiv x_1 n_2 m_2 + x_2 n_1 m_1 \pmod{m_1 m_2}.$$

Then

$$x \equiv x_1 n_2 m_2 \equiv x_1 \pmod{m_1}$$

and

$$f(x) \equiv f(x_1) \equiv 0 \pmod{m_1}.$$

Likewise $f(x) \equiv 0 \pmod{m_2}$. Hence $f(x) \equiv 0 \pmod{m_1 m_2}$. Moreover the x are distinct modulo $m_1 m_2$. Thus we have constructed $N_f(m_1)N_f(m_2)$ solutions to the latter congruence, so that $N_f(m_1)N_f(m_2) \leq N_f(m_1 m_2)$.

On the other hand, if we have $f(x) \equiv 0 \pmod{m_1 m_2}$, then we can choose x_1, x_2 uniquely modulo m_1 and m_2 respectively so that $x_1 n_2 m_2 \equiv x \pmod{m_1}$ and $x_2 n_1 m_1 \equiv x \pmod{m_2}$, and then $x \equiv x_1 n_2 m_2 + x_2 n_1 m_1 \pmod{m_1 m_2}$. Hence

$$f(x_1) \equiv f(x_1 n_2 m_2 + x_2 n_1 m_1) \equiv 0 \pmod{m_1}$$

and likewise $f(x_2) \equiv 0 \pmod{m_2}$. Thus $N_f(m_1 m_2) \leq N_f(m_1) n_f(m_2)$. □

In view of the multiplicative of the structure of the roots of a polynomial congruence it suffices to concentrate on the case when m is a prime power. It turns out that the really hard case is when the modulus is prime. If we can deal with that, then the case of higher powers of primes becomes more amenable. Incredibly we can imitate Newton's method from calculus. This gives a possible method of lifting from solutions modulo p to solutions modulo higher powers of p. Note that if we have a solution to

$$f(x) \equiv 0 \pmod{p^{t+1}}, \tag{3.4}$$ eq:three5

then it must also be a solution to

$$f(x) \equiv 0 \pmod{p^t}. \tag{3.5}$$ eq:three6

Theorem 3.15 (Hensel's Lemma)**.** *Suppose that f is a polynomial with integer coefficients and there is an x_1 such that $f(x_1) \equiv 0 \pmod{p^t}$. There are three cases.*

(i) If $p|f'(x_1)$ but $p^{t+1} \nmid f(x_1)$, then there is no solution x to (3.4) with $x \equiv x_1 \pmod{p^t}$.

(ii) If $p|f'(x_1)$ and $p^{t+1}|f(x_1)$, then there are p solutions x_2 to (3.4) with $x_2 \equiv x_1 \pmod{p^t}$, given by taking all possible such x_2.

(iii) If $p \nmid f'(x_1)$, then there is a unique solution x_2 to (3.4) with $x_2 \equiv x_1 \pmod{p^t}$ given by

$$x_2 \equiv x_1 + p^t j \pmod{p^{t+1}}, \quad jf'(x_1) \equiv -f(x_1)p^{-t} \pmod{p}.$$

Proof. We use the Taylor expansion of f about x_1. We have

$$f(x_1 + h) = f(x_1) + hf'(x_1) + h^2 \frac{f''(x_1)}{2} + \cdots + h^j \frac{f^{(j)}(x_1)}{j!} + \cdots$$

Since f is a polynomial there are only a finite number of terms and each of the coefficients $\frac{f^{(j)}(x_1)}{j!}$ is an integer. Now put $h = p^t j$ where j is at our disposal. All the terms except the first two are divisible by p^{2t} and $2t \geq t + 1$. Thus

$$f(x_1 + p^t j) \equiv f(x_1) + p^t j f'(x_1) \pmod{p^{t+1}}.$$

The first case is clear; when $p|f'(x_1)$ but $p^{t+1} \nmid f(x_1)$, then there can be no solution. Also in the second case, $p|f'(x_1)$ and p^{t+1} then there is a solution for every choice of j, so for every x_2 modulo p^{t+1} with $x_2 \equiv x_1 \pmod{p^t}$. Finally in the third case there is exactly one solution j modulo p so that

$$jf'(x_1) \equiv -f(x_1)p^{-t} \pmod{p}$$

and so there is a unique $x_2 \equiv x_1 + p^t j \pmod{p^{t+1}}$ with $f(x_2) \equiv 0 \pmod{p^{t+1}}$.

If we think of this as saying

$$x_1 + p^t j \text{“} = \text{”} x_1 - \frac{f(x_1)}{f'(j)}$$

then we can see this exactly imitates Newton's method for finding roots. □

ex:three5 **Example 3.7.** *Find all roots of $x^2 - 2 \equiv 0 \pmod{7^r}$ with $1 \leq r \leq 3$.*

(i) It is easy to see that 3 and 4 are solutions modulo 7.

(ii) If we take $x_1 = 3$, as $f(x) = x^2 - 2$, $f'(x) = 2x$, $f(3) = 7$, $f'(3) = 6 \not\equiv 0 \pmod{7}$, it follows that 3 lifts to a unique solution modulo 7^2. Moreover $6j = jf'(3) \equiv -f(3)/7 \equiv -1 \pmod{7}$, $j = 1$, $x_1 + 7j = 3 + 7 = 10$, so $x_2 \equiv 10 \pmod{7^2}$.

(iii) Similarly $f(10) = 98 = 2 \times 7^2$, $f'(10) = 20 \not\equiv 0 \pmod 7$, *so* 10 *lifts to a unique solution modulo* 7^3. *Then* $20j = jf'(10) \equiv -f(10)/(7^2) = -2 \pmod 7$, $j \equiv 2 \pmod 7$, $x_3 = 10 + 2 \times 7^2 = 108$. $f(108) = 11662 \equiv 0 \pmod{7^3}$.

(iv) Now consider $x_1 = 4$. *Then* $f(4) = 14$, $f'(4) = 8 \not\equiv 0 \pmod 7$, *so* 4 *lifts to a unique solution.* $8j = jf'(4) \equiv -f(4)/7 = -2 \pmod 7$, $j = 5$, $x_2 = x_1 + 7j = 39 \pmod{7^2}$, $f(39) \equiv 0 \pmod{7^2}$.

(v) Now we have $x_2 = 39$, $f(39) = 1519$, $f'(39) = 78 \equiv 1 \pmod 7$, $j \equiv jf'(39) \equiv -f(39)/(7^2) = -31 \equiv 4 \pmod 7$. $x_3 = x_2 + 7^2 j = 39 + 196 = 235 \pmod{7^3}$. $f(235) = 55223 = 161 \times 7^3$.

ex:three6 **Example 3.8.** *Find all solutions of* $x^3 - 2 \pmod{3^r}$. *By trial, the only solution modulo* 3 *is* $x_1 = 2$. $f(x) = x^3 - 2$, $f'(x) = 3x^2$. *Thus* $f'(2) \equiv 0 \pmod 3$ *and* $f(2) = 6$. *But* $3^2 \nmid f(2)$ *so we are in case (i) so there is no solution modulo* 3^2 *and hence none modulo* 3^r *with* $r \geq 2$.

3.3.1 Exercises

1. Let p denote a prime number and define

$$f(x) = \prod_{i=1}^{p-1}(x - i) = x^{p-1} + \sum_{i=0}^{p-2} a_i x^i.$$

(i) Show that if $i = 1, 2, \ldots, p-2$, then $p|a_i$.

(ii) Suppose that $p > 3$. When $(a, p) = 1$, a^* denotes a solution of $ax \equiv 1 \pmod{p^2}$. Show that $1^* + 2^* + \cdots + (p-1)^* \equiv 0 \pmod{p^2}$ (Wolstenholme's congruence).

2. Show that $61! + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$.

3. Prove that $3n^2 - 1$ can never be a perfect square.

4. (i) Prove that if $x \in \mathbb{Z}$, then $x^2 \equiv 0$ or $1 \pmod 4$.
(ii) Prove that $5y^2 + 2 = z^2$ has no solutions with $y, z \in \mathbb{Z}$.

5. (i) Prove that if $x \in \mathbb{Z}$, then $x^3 \equiv 0$ or $\pm 1 \pmod 7$.
(ii) Prove that $y^3 - z^3 = 3$ has no solutions with $y, z \in \mathbb{Z}$.

6. Let $f(x)$ denote a polynomial of degree at least 1 with integer coefficients and positive leading coefficient.
(i) Show that if $f(x_0) = m > 0$, then $f(x) \equiv 0 \pmod m$ whenever $x \equiv x_0 \pmod m$.
(ii) Show that there are infinitely many $x \in \mathbb{N}$ such that $f(x)$ is not prime.

7. (i) Suppose that p is an odd prime and x is an integer with $p|x^2 + 1$. Prove that x has order 4 and $p \equiv 1 \pmod 4$.
(ii) Prove that there are infinitely many primes $p \equiv 1 \pmod 4$.

8. Find all solutions (if there are any) to each of the following congruences
(i) $x^2 \equiv -1 \pmod 7$, (ii) $x^2 \equiv -1 \pmod{13}$, (iii) $x^5 + 4x \equiv 0 \pmod 5$. 9. (i) Let

$m \in \mathbb{N}$. Prove that

$$(y-1)(y^{m-1}+y^{m-2}+\cdots+y+1) = y^m - 1.$$

(ii) Let $n \in \mathbb{N}$. Prove that

$$(x^2+1)(x^2-1)(x^{4n-4}+x^{4n-8}+\cdots+x^4+1) = x^{4n}-1.$$

(iii) Let p be a prime number with $p \equiv 1 \pmod 4$. Prove that $x^2 \equiv -1 \pmod p$ has exactly two solutions.

10. Let $n \in \mathbb{Z}$. Prove that if $p|n^2+n+1$ and $p > 3$, then $p \equiv 1 \pmod 6$. Deduce that there are infinitely many primes $p \equiv 1 \pmod 6$.

11. Suppose that p is a prime number and $q|p-1$. Prove that the congruence $1 + x + \cdots + x^{q-1} \equiv 0 \pmod p$ has exactly $q-1$ solutions.

3.4 Notes

§1 The concept of residue classes and the idea that the residue classes modulo n partition the integers was introduced by Euler about 1750. The notation $\equiv$ was introduced by Gauss in 1801. For a modern translation see C. F. Gauss, Disquisitiones Arithmeticæ, Yale University Press, 1965. Euler introduced the eponymous function in 1763.

W. R. Alford, A. Granville & C. Pomerance proved that "There are Infinitely Many Carmichael Numbers", Annals of Mathematics. 140(1994), 703–722.

The first complete solution of the Chinese Remainder Theorem in the general case occurs in the treatise of Ch'in Chiu-shao of 1247.

Wilson's thereom was first stated by Ibn al-Haytham about 1000AD. The first proof was given by Lagrange in 1771. Hensel proved his lemma in 1897. The proof in the non-singular case is motivated by Newton's method in numerical analysis.

Chapter 4

Primitive Roots and RSA

4.1 Primitive Roots

We have seen that on the residue classes modulo m we can perform many of the standard operations of arithmetic. Such an object is called a ring. In this case it is usually denoted by $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}_m$. In this chapter we will look at its multiplicative structure. In particular we will consider the reduced residue classes modulo m. An obvious question is what happens if we take powers of a fixed residue a?

def:four0 **Definition 4.1.** *Given $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$ we define the order $\mathrm{ord}_m(a)$ of a modulo m to be the smallest positive integer t such that*

$$a^t \equiv 1 \pmod{m}.$$

We may express this by saying that a belongs to the exponent t modulo m.

Note that by Euler's theorem, $a^{\phi(m)} \equiv 1 \pmod{m}$, so that $\mathrm{ord}_m(a)$ exists.

thm:four0 **Theorem 4.1.** *Suppose that $m \in \mathbb{N}$, $(a, m) = 1$ and $n \in \mathbb{N}$ is such that $a^n \equiv 1 \pmod{m}$. Then $\mathrm{ord}_m(a)|n$. In particular $\mathrm{ord}_m(a)|\phi(m)$.*

Proof. For concision let $t = \mathrm{ord}_m(a)$. Since t is minimal we have $t \leq n$. Thus by the division algorithm there are q and r with $0 \leq r < t$ such that $n = tq + r$. Hence

$$a^r \equiv (a^t)^q a^r = a^{qt+r} = a^n \equiv 1 \pmod{m}.$$

But $0 \leq r < t$. If we would have $r > 0$, then we would contradict the minimality of t. Hence $r = 0$. □

Here is an application we will make use of later.

thm:four00 **Theorem 4.2.** *Suppose that $d|p-1$. Then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.*

Proof. We have

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{d-p-2d} + \cdots + x^d + 1).$$

To see this just multiply out the right hand side and observe that the terms telescope. We know from Euler's theorem that there are exactly $p-1$ incongruent roots to the left hand side modulo p. On the other hand, by Lagrange's theorem, Theorem 3.13, the second factor has at most $p-1-d$ such roots, so the first factor must account for at least d. On the other hand, again by Lagrange's theorem, it has at most d. □

We have already seen that, when $(a,m) = 1$, a has order modulo m which divides $\phi(m)$. One question one can ask is, given any $d|\phi(m)$, are there elements of order d? In the special case $d = \phi(m)$ this would mean that $a, a^2, \ldots, a^{\phi(m)}$ are distinct modulo m, because otherwise we would have $a^u \equiv a^v \pmod{m}$ with $1 \leq u < v \leq \phi(m)$ and then $a^{v-u} \equiv 1 \pmod{m}$ and $1 \leq v - u < \phi(m)$ contradicting the assumption that $\mathrm{ord}_m(a) = \phi(m)$.

Example 4.1. $m = 7$.
$a = 1$, $\mathrm{ord}_7(1) = 1$.
$a = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1$. $\mathrm{ord}_7(2) = 3$.
$a = 3$, $3^2 = 9 \equiv 2$, $3^3 = 27 \equiv 6$, $3^4 \equiv 18 \equiv 4$,
$3^5 \equiv 12 \equiv 5$, $3^6 \equiv 1$, $\mathrm{ord}_7(3) = 6$.
$a = 4$, $4^2 \equiv 2$, $4^3 \equiv 2^6 \equiv 1$, $\mathrm{ord}_7(4) = 3$.
$a = 5$, $5^2 = 25 \equiv 4$, $5^3 \equiv 20 \equiv 6$, $5^4 \equiv 30 \equiv 2$,
$5^5 \equiv 10 \equiv 3$, $5^6 \equiv 1$, $\mathrm{ord}_7(5) = 6$.
$a = 6$, $6^2 = 36 \equiv 1$, $\mathrm{ord}_7(6) = 2$.
Thus there is one element of order 1*, one element of order* 2*, two of order* 3 *and two of order* 6*.*

Is it a fluke that for each $d|6 = \phi(7)$ *the number of elements of order* d *is* $\phi(d)$*?*

def:four1 **Definition 4.2.** *Suppose that* $m \in \mathbb{N}$ *and* $(a,m) = 1$*. If* $\mathrm{ord}_m(a) = \phi(m)$ *then we say that* a *is a primitive root modulo* m*.*

We know that we do not always have primitive roots. For example, any number a with $(a,8) = 1$ is odd and so $a^2 \equiv 1 \mod 8$, whereas $\phi(8) = 4$. There are primitive roots to some moduli. For example, modulo 7 the powers of 3 are successively $3, 2, 6, 4, 5, 1$.

Gauss determined precisely which moduli possess primitive roots. The first step is the case of prime modulus.

Theorem 4.3 (Gauss)**.** *Suppose that* p *is a prime number. Let* $d|p-1$ *then there are* $\phi(d)$ *residue classes* a *with* $\mathrm{ord}_p(a) = d$*. In particular there are* $\phi(p-1) = \phi(\phi(p))$ *primitive roots modulo* p*.*

Proof. We have already seen that the order of every reduced residue class modulo p divides $p-1$. For a given $d|p-1$ let $\psi(d)$ denote the number of reduced residues of order d modulo p. We know that the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions. Thus every solution has order dividing d. Moreover every reduced residue which has order dividing d must be a solution. Thus for each $d|p-1$ we have

$$\sum_{r|d} \psi(r) = d.$$

This is reminiscent of an earlier formula

$$\sum_{r|d} \phi(r) = d.$$

Let $1 = d_1 < d_2 < \ldots < d_k = p-1$ be the divisors of $p-1$ in order. We have a relationship

$$\sum_{r|d_j} \psi(r) = d_j$$

for each $j = 1, 2, \ldots$ and, of course, the sum is over a subset of the divisors of $p-1$. I claim that this determines $\psi(d_j)$ uniquely. We could prove this by observing that if N is the number of positive divisors of $p-1$, then we have N linear equations in the N unknowns $\psi(r)$ and we can we can write this in matrix notation $\boldsymbol{\psi}\mathcal{U} = \mathbf{d}$. Moreover $\mathcal{U}$ is an upper triangular matrix with non-zero entries on the diagonal and so is invertible. Hence the $\psi(d_j)$ are uniquely determined. But we already know a solution, namely $\psi = \phi$. If we wish to avoid the linear algebra we can prove this by induction on j. For the base case we have $\psi(1) = 1$. Suppose that $\psi(d_1), \ldots, \psi(d_j)$ are determined. Then we have

$$\sum_{r|d_{j+1}} \psi(r) = d_{j+1}.$$

Hence

$$\psi(d_{j+1}) = d_{j+1} - \sum_{\substack{r|d_{j+1} \\ r<d_{j+1}}} \psi(r)$$

and every term on the right hand side is already determined. Thus we can conclude there is only one solution to our system of equations. But we already know one solution, namely $\psi(r) = \phi(r)$. □

ex:fourx **Example 4.2.** *Here is the proof when $p = 13$, so we are concerned with the divisors of* 12.

$$\big(\psi(1), \psi(2), \psi(3), \psi(4), \psi(6), \psi(12)\big) \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = (1, 2, 3, 4, 6, 12)$$

How about higher powers of odd primes? We can use the idea of "lifting" which we already saw in connection with solutions of congruences.

Theorem 4.4 (Gauss)**.** *Suppose that p is an odd prime and $d|\phi(p^k) = p^{k-1}(p-1)$. Then there are $\phi(d)$ residue classes modulo p^k which have order d.*

Proof. We first prove the existence of a primitive root modulo p^k when $k > 1$. Let g be a primitive root modulo p. It is clear that a primitive root modulo p^k will also be one modulo p, so it makes sense to examine $g + jp$. We show that there is a j so that

$$(g + jp)^{p-1} = 1 + h_1 p$$

with $p \nmid h_1$. Observe that $g^{p-1} = 1 + lp$ for some l. Then, by the binomial expansion, for every j

$$\begin{aligned}(g + jp)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}jp \pmod{p^2} \\ &\equiv 1 + (l - g^{p-2}j)p \pmod{p^2}\end{aligned}$$

and we may choose j so that $p \nmid l - g^{p-2}j$.

Now we show that with this j, for every t there is an h_t such that

$$(g + jp)^{p^{t-1}(p-1)} = 1 + h_t p^t \quad (p \nmid h_t). \tag{4.1}$$ eq:four2

We do this by induction on t. We have already established the base case. Suppose we have already established the result for some t. Then

$$\begin{aligned}(g + jp)^{p^t(p-1)} &= (1 + h_t p^t)^p \\ &\equiv 1 + h_t p^{t+1} + \frac{p(p-1)}{2} h_t^2 p^{2t} \pmod{p^{3t}}.\end{aligned}$$

We have both $2t + 1 \geq t + 2$ and $3t \geq t + 2$. Hence we have

$$(g + jp)^{p^t(p-1)} \equiv 1 + h_t p^{t+1} \pmod{p^{t+2}}$$

and since $p \nmid h_t$ this gives the desired conclusion.

Now consider the number $g+jp$. We show that this is a primitive root modulo p^k, and we may suppose that $k \geq 2$. Let $d = \mathrm{ord}_{p^k}(g + jp)$. Then $d|\phi(p^k) = p^{k-1}(p-1)$. Hence $d = p^t v$ for some t and v with $0 \leq t \leq k-1$ and $v|p-1$. We have $p^t = (p - 1 + 1)^t \equiv 1 \pmod{p-1}$. Hence

$$\begin{aligned}1 &\equiv (g + jp)^d \equiv (g + jp)^{p^t v} \pmod{p^k} \\ &\equiv (g + jp)^v \pmod{p} \\ &\equiv g^v \pmod{p}\end{aligned}$$

and since g is a primitive root modulo p we have $v = p-1$. Now repeating the argument we have

$$\begin{aligned} 1 &\equiv (g+jp)^d \pmod{p^k} \\ &\equiv (g+jp)^{p^t(p-1)} \pmod{p^k} \\ &= 1 + h_{t+1}p^{t+1} \end{aligned}$$

by (4.1). Since $p \nmid h_{t+1}$ this can only be $\equiv 1 \pmod{p^k}$ if $t = k-1$.

Now suppose that $d|\phi(p^k)$ and g is a primitive root modulo p^k and consider the $\phi(d)$ residue classes

$$g^{b\phi(p^k)/d},$$

modulo p^k with $(b,d) = 1$ and $1 \le b \le d$. Since

$$\left(g^{b\phi(p^k)/d}\right)^d \equiv 1 \pmod{p^k}$$

they have order r dividing d. Moreover g would have order

$$\big(b\phi(p^k)r/d, \phi(p^k)\big) = (br,d)\phi(p^k)/d = \phi(p^k)r/d,$$

and so $r = d$. □

It is easy to see that 1 is a primitive root modulo 2 and 3 is a primitive root modulo 4, and we have already seen that there are no primitive roots modulo 8, and hence there are none modulo higher powers of 2. Thus we are half-way to proving the following theorem.

Theorem 4.5 (Gauss)**.** *We have primitive roots modulo m when $m = 2$, $m = 4$, $m = p^k$ and $m = 2p^k$ with p an odd prime and in no other cases.*

Proof. The one positive case left to settle is $m = 2p^k$. We have $\phi(2p^k) = \phi(p^k)$. Let g be a primitive root modulo p^k and let $G = g$ if g is odd and $G = g + p^k$ if g is even. Then G is odd and a primitive root modulo p^k. Hence, given x with $1 \le x \le 2p^k$ and $(x, 2p^k) = 1$ there is a y so that $G^y \equiv x \pmod{p^k}$ and (regardless of the value of y) $G^y \equiv x \pmod 2$. Hence $G^y \equiv x \pmod{2p^k}$.

It remains to show that for all other m there are no residue classes of order $\phi(m)$. We have already dealt with $m = 2^k$ with $k \ge 3$. Write $m = 2^k p_1^{k_1} \dots p_r^{k_r}$. We can suppose that (i) $k = 0$ or 1 and $r \ge 2$ or (ii) $k \ge 2$ and $r \ge 1$. The key to the proof is that given a with $(a,m) = 1$ the orders of a modulo 2^k, $p_j^{k_j}$ divides $\phi(2^k)$ and $\phi(p_j^{k_j})$ respectively. Thus the order of a modulo m divides the least common multiple of $\phi(2^k), \phi(p_1^{k_1}), \dots \phi(p_r^{k_r})$. That is

$$\mathrm{ord}_m(a) | [2^{k-1}, p_1^{k_1-1}(p_1-1), \dots, p_r^{k_r-1}(p_r-1)]$$

and this LCM is strictly smaller than $\phi(m)$ because 2 divides at least two terms. Thus in case (i) $[p_1^{k_1-1}(p_1-1), p_2^{k_2-1}(p_2-1)] = p_1^{k_1-1}p_2^{k_2-1}[p_1-1, p_2-1] \le \frac{1}{2}\phi(p_1^{k_1}p_2^{k_2})$. Likewise in case (ii) we have $[2^{k-1}, p_1^{k_1-1}(p_1-1)] = 2^{k-2}p_1^{k_1-1}[2, p_1-1] = 2^{k-2}p_1^{k_1-1}(p_1-1) < \phi(2^k p_1^{k_1})$. □

Example 4.3. *Primitive roots modulo* 7 *and* 7^2.

(i) Modulo 7. *Try* 2. *Divisors of* $\phi(7) = 6$ *are* $1, 2, 3, 6$ *and the order of* 2 *must be one of these.* $2^1 = 2 \not\equiv 1$, $2^2 = 4 \not\equiv 1$, $2^3 = 8 \equiv 1$ *so* 2 *not a primitive root.*

Try 3. $3^1 = 3 \not\equiv 1$, $3^2 = 9 \equiv 2 \not\equiv 1$, $3^3 = 27 \equiv 6 \not\equiv 1$. *Hence* 3 *has order* 6 *and so is a primitive root modulo* 7. *One can now find all primitive roots modulo* 7 *by considering* 3^x *with* $1 \le x \le 6$ *and* $(x, 6) = 1$. *The only choices for* x *are* 1 *and* 5, *so the only other primitive root modulo* 7 *is* $3^5 = 243 \equiv 5 \pmod 7$. *Thus* $3, 5$ *are the primitive roots modulo* 7.

By the way, this trial and error method is the best general method that we have. It is believed that in general one does not have to search very far, but we cannot prove it.

(ii) Modulo 7^2. *We know that a primitive root modulo* 7^2 *has to be one modulo* 7, *so we can start with* 3. *The divisors of* $\phi(7^2) = 6.7$ *are* $1, 2, 3, 6, 7, 14, 21, 42$. *We know that* $3^x \not\equiv 1 \pmod 7$ *when* $x = 1, 2, 3$ *and so* $3^x \not\equiv 1 \pmod{7^2}$ *in those cases. Also since* $3^7 \equiv 3 \pmod 7$, $3^{14} \equiv 3^2 \equiv 2 \pmod 7$ *and* $3^{21} \equiv 3^3 \equiv 6 \pmod 7$ *so* $3^x \not\equiv 1 \pmod{7^2}$ *in those cases either. Thus we only need check* $3^6 = 729 \equiv 43 \not\equiv 1 \pmod{7^2}$. *Thus* 3 *is also a primitive root modulo* 7^2.

We know from the Chinese Remainder Theorem that we can reduce a polynomial congruence modulo m when m is composite to its prime power constituents. However we were not able to treat the case $m = 2^k$ in general because when $k \ge 3$ primitive roots do not exist. Nevertheless we can usually apply the following theorem.

Theorem 4.6 (Gauss)**.** *Suppose that* $k \ge 3$. *Then the numbers* $(-1)^u 5^v$ *with* $u = 0, 1$ *and* $0 \le v < 2^{k-2}$ *form a set of reduced residues modulo* 2^k

Proof. We first prove that if $r \ge 3$, then

$$5^{2^{r-2}} = 1 + 2^r j_r \tag{4.2}$$

eq:four2k

with $2 \nmid j_r$. We prove this by induction on r. It is clear when $r = 3$, since $5^2 = 25 = 1 + 2^3 \cdot 3$. If (4.2) holds, then

$$5^{2^{r-1}} = 1 + 2^{r+1} j_r + 2^{2r} j_r^2$$

and $2 \nmid j_r + 2^{r-1} j_r^2$. We also know that $\mathrm{ord}_{2^k}(5) | \phi(2^k) = 2^{k-1}$, so $\mathrm{ord}_{2^k}(5) = 2^r$ for some $0 \le r \le k-1$. The relationship (4.2) shows that $r = k-2$. Hence the numbers

$$1, 5, 5^2, 5^3, \ldots, 5^{2^{k-2}-1}$$

are distinct modulo 2^k. Likewise the numbers

$$-1, -5, -5^2, -5^3, \ldots, -5^{2^{k-2}-1}$$

are distinct modulo 2^k. Moreover the numbers in the fist list are $\equiv 1 \pmod 4$ and those in the second one are $\equiv -1 \pmod 4$. Thus the members of the first list are all different modulo 2^k to those in the second. Thus the two lists together give a complete cover of the 2^{k-1} reduced residues modulo 2^k. □

In terms of group theory this says that the reduced residues modulo 2^k with $k \geq 3$, under multiplication form a direct product of a cyclic group of order 2 and one of order 2^{k-2}.

4.1.1 Exercises

1. Find all the primitive roots of 7, 14, 49.

2. First find a primitive root modulo 19 and then find all primitive roots modulo 19.

3. Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$ when $p - 1 \nmid k$ and is $\equiv -1 \pmod{p}$ when $p - 1 | k$.

4. Let g be a primitive root modulo p. Prove that no k exists satisfying $g^{k+2} \equiv g^{k+1} + 1 \equiv g^k + 2 \pmod{p}$.

5. Suppose that $p = 2^m + 1$ is a prime, $p \nmid a$ and a is a quadratic non-residue (i.e., $x^2 \equiv a \pmod{p}$ is insoluble) modulo p. Show that a is a primitive root modulo p.

6. [Gauss] Prove that for any prime number $p \neq 3$ the product of its primitive roots is $1 \pmod{p}$.

7. The Carmichael function $\lambda(m)$ is the smallest positive number such that $\mathrm{ord}_a(m) | \lambda(m)$ whenever $(a, m) = 1$. Prove that $\lambda(n) | \phi(n)$.

8. Prove that if a has order 3 modulo a prime p, then $1 + a + a^2 \equiv 0 \pmod{p}$, and $1 + a$ has order 6.

9. Suppose that $(10a, q) = 1$, and that k is the order of 10 modulo q. Show that the decimal expansion of the rational number a/q is periodic with least period k.

4.2 Binomial Congruences and Discrete Logarithms

As an application of this theory we can say something about the solution of congruences of the form

$$x^k \equiv a \pmod{p}$$

when p is odd. The case $a = 0$ is easy. The only solution is $x \equiv 0 \pmod{p}$. Suppose $a \not\equiv 0 \pmod{p}$. Then we can pick a primitive root g modulo p and then there will be a c so that $g^c \equiv a \pmod{p}$. Also, since any solution x will have $p \nmid x$ we can define y so that $g^y \equiv x \pmod{p}$. Thus our congruence becomes

$$g^{ky} \equiv g^c \pmod{p}.$$

Hence it follows that

$$ky \equiv c \pmod{p-1}.$$

We have turned a polynomial congruence into a linear one. This is a bit like using logarithms on real numbers. Sometimes the exponents c and y are referred to as the discrete

logarithms modulo p to the base g. Computing them numerically is hard and there is a protocol (Diffie-Hellman) which uses them to exchange secure keys and passwords. Our new congruence is soluble if and only if $(k, p-1)|c$, and when this holds the y which satisfy it lie in a residue class modulo $\frac{p-1}{(k,p-1)}$, i.e. $(k, p-1)$ different residue classes modulo $p-1$. Thus, when $a \not\equiv 0 \pmod{p}$ the original congruence is either insoluble or has $(k, p-1)$ solutions. Thus we just proved the following theorem.

Theorem 4.7. *Suppose p is an odd prime. When $p \nmid a$ the congruence $x^k \equiv a \pmod{p}$ has 0 or $(k, p-1)$ solutions, and the number of reduced residues a modulo p for which it is soluble is $\frac{p-1}{(k,p-1)}$.*

The above theorem suggests that we can use primitive roots to create the residue class equivalent of logarithms.

def:four2 **Definition 4.3.** *Given a primitive root g and a reduced residue class a modulo m we define the discrete logarithm $\operatorname{dlog}_g(a)$, or index $\operatorname{ind}_g(a)$ to be that unique residue class l modulo $\phi(m)$ such that $g^l \equiv a \pmod{m}$*

The notation $\operatorname{ind}_g(x)$ is more commonly used, but $\operatorname{dlog}_g(x)$ seems more natural.

ex:four4 **Example 4.4.** *Find a primitive root modulo 11 and construct a table of discrete logarithms. First we check 2. The divisors of $11-1=10$ are 1, 2, 5, 10 and $2^1 = 2 \not\equiv 1 \pmod{11}$, $2^2 = 4 \not\equiv 1 \pmod{11}$, $2^5 = 32 \equiv 10 \not\equiv 1 \pmod{11}$, so 2 is a primitive root modulo 11.*

Now we construct a table of powers of 2 modulo 11

y	1	2	3	4	5	6	7	8	9	10
$x \equiv 2^y$	2	4	8	5	10	9	7	3	6	1

Then we construct the "inverse" table

x	1	2	3	4	5	6	7	8	9	10
$y = \operatorname{dlog}_2(x)$	10	1	8	2	4	9	7	3	6	5

Note that while x is a residue modulo p (here $p = 11$), the y are residues modulo $p-1$ (here 10). The number y is the order, or exponent, to which 2 has to be raised to give x modulo p. In other words $x \equiv g^{\operatorname{dlog}_g(x)} \pmod{p}$.

ex:four5 **Example 4.5.** *We can use this to solve, if possible, the congruences,*

$$x^3 \equiv 6 \pmod{11},$$
$$x^5 \equiv 9 \pmod{11},$$
$$x^{65} \equiv 10 \pmod{11}$$

Consider the first one, $x^3 \equiv 6 \pmod{11}$. We can write $x \equiv 2^y \pmod{11}$, so that $x^3 = 2^{3y}$ and we see from the second table that $6 \equiv 2^9 \pmod{11}$. Thus what we need is that $3y$ and 9 match. This means that we need $3y \equiv 9 \pmod{10}$.

Recall that the modulus here is $p-1=10$ *since* $2^{10}\equiv 1 \pmod{11}$. *This has the unique solution*

$$y\equiv 3 \pmod{10}.$$

Going to the first table we find that $x\equiv 8 \pmod{11}$.

For the second congruence we find that $5y\equiv 6 \pmod{10}$ *and now we see that this has no solutions because* $(5,10)=5\nmid 6$.

In the third case we have $65y\equiv 5 \pmod{10}$ *and this is equivalent to* $13y\equiv 1 \pmod{2}$ *and this has one solution modulo* $y\equiv 1 \pmod{2}$, *and so* 5 *solutions modulo* 10 *given by* $y\equiv 1$, 3, 5, 7 *or* 9 *modulo* 10. *Hence the original congruence has five solutions given by*

$$x\equiv 2,\ 8,\ 10,\ 7,\ 6 \pmod{11}$$

4.2.1 Exercises

1. Show that 3 is a primitive root modulo 17 and draw up a table of discrete logarithms to this base modulo 17. Hence, or otherwise, find all solutions to the following congruences.
(i) $x^{12}\equiv 16 \pmod{17}$,
(ii) $x^{48}\equiv 9 \pmod{17}$,
(iii) $x^{20}\equiv 13 \pmod{17}$,
(iv) $x^{11}\equiv 9 \pmod{17}$.

2. (i) Find the orders of 2, 3 and 5 modulo 23.
(ii) Find a primitive root modulo 23, construct a table of discrete logarithms, and solve the congruence $x^6\equiv 4 \pmod{23}$.

3. Show that 2 is a primitive root modulo 13 and draw up a table of discrete logarithms to this base. Hence, or otherwise, find all solutions to the following congruences.
(i) $x^{16}\equiv 3 \pmod{13}$,
(ii) $x^{21}\equiv 3 \pmod{13}$,
(iii) $x^{31}\equiv 7 \pmod{13}$.

4. Show that 2 is a primitive root modulo 11 and draw up a table of discrete logarithms to this base modulo 11. Hence, or otherwise, find all solutions to the following congruences.
(i) $x^{6}\equiv 7 \pmod{11}$,
(ii) $x^{48}\equiv 9 \pmod{11}$,
(iii) $x^{7}\equiv 8 \pmod{11}$.

4.3 RSA

Rivest, Shamir and Adleman in 1978 rediscovered an idea which had already been described internally at GCHQ by Cocks in 1973 and then shared with NSA. This is sometimes described as a way of sharing information by public key encryption. The principle of the method is as follows. Let $n,d,e\in\mathbb{N}$ be such that

$$de\equiv 1 \pmod{\phi(n)}.$$

Given a message M encoded as a number, and suppose $M < n$. Compute

$$E \equiv M^e \pmod{n}$$

and transmit E. The recipient then computes

$$E^d \pmod{n}.$$

Then

$$E^d \equiv (M^e)^d = M^{de} \equiv M \pmod{n}$$

since $\phi(n)|de - 1$ and the recipient recovers the message. The sender has to know only n and e. The recipient only has to know n and d. The level of security depends only on the ease with which one can find d knowing n and e. The numbers n and e can be in the public domain.

The crucial question is the solubility of

$$de \equiv 1 \pmod{\phi(n)}$$

and this in turn requires the value of $\phi(n)$. Suppose that n is the product of two primes

$$n = pq.$$

If n can be factored then we have $\phi(n) = (p-1)(q-1)$. But this is a known hard problem, especially when the primes are roughly of the same size.

Of course if the value of $\phi(n)$ can be discovered not only is the message easily broken but n is easily factored since one has

$$p + q = pq + 1 - \phi(n) = n + 1 - \phi(n),$$

$$pq = n$$

and once can substitute for q and then solve the quadratic equation in p. In other words, knowing $\phi(n)$ is equivalent to factoring n.

4.3.1 Exercises

1. Given that n is a product of two primes p and q with $p < q$, prove that

$$p = \frac{n + 1 - \phi(n) - \sqrt{(n + 1 - \phi(n))^2 - 4n}}{2}.$$

If you have a good calculator use this to factorise n where $n = 19749361535894833$ and $\phi(n) = 19749361232517120$.

4.4 Notes

§1. The function $\mathrm{ord}_m(a)$ has its roots in work of Lagrange. Carmichael introduced his function in R. D. Carmichael (1910), "Note on a new number theory function". Bulletin of the American Mathematical Society. 16 (5), 232–238.

Euler invented the term *primitive root*, and Gauss (1801) was the first to prove that they exist modulo p for every prime p.

§2. For a description of the Diffie-Hellman key exchange see `https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange`

§3. There is an excellent wikipedia article on RSA at `https://en.wikipedia.org/wiki/RSA_(cryptosystem)`

Chapter 5

Quadratic Residues

ch:five

5.1 Quadratic Congruences

We can now apply the theory we have developed to study quadratic congruences, and especially

$$x^2 \equiv c \pmod{m}.$$

The structure here is especially rich and was thus subject to much work in the eighteenth century, culminating in a famous theorem of Gauss.

From the various theories we have developed we know that the first, or base, case we need to understand is that when the modulus is a prime p, and since the case $p = 2$ is rather easy we can suppose that $p > 2$. Then we are interested in

$$x^2 \equiv c \pmod{p}. \tag{5.1}$$

eq:five1

By the way, the apparently more general congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ (with $p \nmid a$ of course) can be reduced by "completion of the square" via $4a(ax^2 + bx + c) \equiv 0 \pmod{p}$ to $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$ and since $2ax + b$ ranges over a complete set of residues as x does this is equivalent to solving $x^2 \equiv b^2 - 4ac \pmod{p}$. Thus it suffices to know about the solubility of the congruence (5.1).

We know that (5.1) has at most two solutions, and that sometimes it is soluble and sometimes not

ex:five1

Example 5.1. $x^2 \equiv 6 \mod 7$ *has no solution (check* $x \equiv 0, 1, 2, 3 \pmod{7}$*), but*

$$x^2 \equiv 5 \pmod{11}$$

has the solutions

$$x \equiv 4, 7 \pmod{11}.$$

If $c \equiv 0 \pmod{p}$, then the only solution to (5.1) is $x \equiv 0 \pmod{p}$ (note that $p|x^2$ implies that $p|x$). If $c \not\equiv 0 \pmod{p}$ and the congruence has one solution, say $x \equiv x_0 \pmod{p}$, then $x \equiv p - x_0 \pmod{p}$ gives another.

The fundamental question here is can we characterise or classify those c for which the congruence (5.1) is soluble? Better still can we quickly determine, given c, whether (5.1) is soluble?

def:five1 **Definition 5.1.** *If $c \not\equiv 0 \pmod{p}$, and (5.1) has a solution, then we call c a quadratic residue which we abbreviate to QR. If it does not have a solution, then we call c a quadratic non-residue or QNR.*

Some authors also call 0 a quadratic residue. Others leave it undefined. We will follow the latter course. Zero does behave differently. Now we can prove the following simple, but surprisingly useful, theorem.

Theorem 5.1. *Let p be an odd prime number. The numbers*

$$1, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

are distinct modulo p and give a complete set of (non-zero) quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ quadratic residues modulo p and exactly $\frac{1}{2}(p-1)$ quadratic non-residues.

Proof. Suppose that $1 \leq x < y \leq \frac{1}{2}(p-1)$. If $p|y^2 - x^2 = (y-x)(y+x)$, then $p|y-x$ or $p|y+x$. But $0 < y - x < y + x < 2y \leq p - 1 < p$. Thus the numbers $1, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are distinct modulo p.

Now suppose that c is a quadratic residue modulo p. Then there is an x with $1 \leq x \leq p-1$ such that $x^2 \equiv c \pmod{p}$. If $x \leq \frac{1}{2}(p-1)$, then x^2 is in our list and represents c. If $\frac{1}{2}(p-1) < x \leq p-1$, then $(p-x)^2 \equiv x^2 \equiv c \pmod{p}$, $(p-x)^2$ represents c, and $1 \leq p - x \leq \frac{1}{2}(p-1)$. Moreover $(p-x)^2$ is in our list. Thus every QR is in our list and every member of our list is distinct and a QR. Hence there are exactly $\frac{1}{2}(p-1)$ QR. Moreover then the remaining $p - 1 - \frac{1}{2}(p-1) = \frac{1}{2}(p-1)$ non-zero residues have to be QNR. □

We can use this in various ways.

ex:five2 **Example 5.2.** *Find a complete set of quadratic residues r modulo 19 with $1 \leq r \leq 18$.*

We can solve this by first observing that $1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16, 5^2 = 25, 6^2 = 36, 7^2 = 49, 8^2 = 64, 9^2 = 81$ is a complete set of quadratic residues and then reduce them modulo 19 to give

$$1, 4, 9, 16, 6, 17, 11, 7, 5$$

which we can rearrange as

$$1, 4, 5, 6, 7, 9, 11, 16, 17.$$

To help us understand quadratic residues we make the following definition.

def:five2 **Definition 5.2.** *Given an odd prime number p and an integer c we define the Legendre symbol*

$$\left(\frac{c}{p}\right)_L = \begin{cases} 0 & c \equiv 0 \pmod{p}, \\ 1 & c \text{ a } QR \pmod{p}, \\ -1 & c \text{ a } QNR \pmod{p}, \end{cases} \tag{5.2}$$ eq:five2

The Legendre symbol is a remarkable function with lots of interesting properties.

ex:five3 **Example 5.3.** *One very important property is that it has the same value if one replaces c by $c + kp$ regardless of the value of k. Thus given p it is periodic in c with period p.*

ex:five4 **Example 5.4.** *Suppose that p is an odd prime and $a \not\equiv 0 \pmod{p}$. Then*

$$\sum_{x=1}^{p} \left(\frac{ax+b}{p}\right)_L = 0. \tag{5.3}$$ eq:five3

The proof of this is rather easy. The expression $ax + b$ runs through a complete set of residues as x does and so one of the terms is 0, half the rest are $+1$, and the remainder are -1.

ex:five5 **Example 5.5.** *The number of solutions of the congruence*

$$x^2 \equiv c \pmod{p}$$

is

$$1 + \left(\frac{c}{p}\right)_L.$$

We already know that the number of solutions is 1 when $p|c$, 2 when c is a QR, and 0 when c is a QNR and this matches the above exactly.

We can use this to count the solutions of more complicated congruences.

ex:five6 **Example 5.6.** *How many solutions does*

$$x^2 + y^2 \equiv c \pmod{p}$$

have in x and y? Denote the number by $N(p; c)$. We can rewrite the congruence as $z + w \equiv c \pmod{p}$, and then for each solution z, w ask for the number of solutions of $x^2 \equiv z \pmod{p}$ and $y^2 \equiv w \pmod{p}$. From above this is

$$\left(1 + \left(\frac{z}{p}\right)_L\right)\left(1 + \left(\frac{w}{p}\right)_L\right).$$

Also $w \equiv c - z \pmod{p}$*, thus the total number of solutions is*

$$N(p;c) = \sum_{z=1}^{p} \left(1 + \left(\frac{z}{p}\right)_L\right)\left(1 + \left(\frac{c-z}{p}\right)_L\right).$$

If we multiply this out we get

$$p + \sum_{z=1}^{p} \left(\frac{z}{p}\right)_L + \sum_{z=1}^{p} \left(\frac{c-z}{p}\right)_L + \sum_{z=1}^{p} \left(\frac{z}{p}\right)_L \left(\frac{c-z}{p}\right)_L.$$

By (5.3) the first and second sums are 0*, so that*

$$N(p;c) = p + \sum_{z=1}^{p} \left(\frac{z}{p}\right)_L \left(\frac{c-z}{p}\right)_L.$$

It is possible also to evaluate the sum here, but we need to know a little more about the Legendre symbol.

The Legendre symbol is a prototype for an important class of number theoretic functions called Dirichlet characters. A simple example would be to take an odd prime p and a primitive root modulo g modulo p, and then for a fixed h we can define $\chi(g^k) = e^{2\pi ihk/(p-1)}$ and $\chi(n) = 0$ if $p|n$. The Legendre symbol is the special case $h = \frac{p-1}{2}$. Dirichlet used them to prove that if $(a, m) = 1$, then there are infinitely many primes in the residue class a modulo m.

We can combine the definition of the Legendre symbol with a criterion first enunciated by Euler.

thm:five2 **Theorem 5.2** (Euler's Criterion)**.** *Suppose that p is an odd prime number. Then*

$$\left(\frac{c}{p}\right)_L \equiv c^{\frac{p-1}{2}} \pmod{p}$$

and the Legendre symbol, as a function of c, is totally multiplicative.

rem:five1 **Remark 5.1.** *By multiplicative we mean a function f which satisfies*

$$f(n_1 n_2) = f(n_1) f(n_2)$$

whenever $(n_1, n_2) = 1$. Totally multiplicative means that the condition $(n_1, n_2) = 1$ can be dropped.

rem:five2 **Remark 5.2.** *The totally multiplicative property means that if x and y are both QR, or both QNR, then their product is a QR, and their product can only be a QNR if one is a QR and the other is a QNR.*

Proof. If c is a quadratic residue, then there is an $x \not\equiv 0 \pmod{p}$ such that $x^2 \equiv c \pmod{p}$. Hence $c^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 = \left(\frac{c}{p}\right)_L \pmod{p}$. We know that the congruence

$$c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

has at most $\frac{p-1}{2}$ solutions and so we have just shown that it has exactly that many solutions. We also have

$$\left(c^{\frac{p-1}{2}} - 1\right)\left(c^{\frac{p-1}{2}} + 1\right) = c^{p-1} - 1$$

and we know that this has exactly $p-1$ roots modulo p. In particular every QNR is a solution, but cannot be a root of $c^{\frac{p-1}{2}} - 1$. Hence if c is a QNR, then $c^{\frac{p-1}{2}} \equiv -1 = \left(\frac{c}{p}\right)_L \pmod{p}$. This proves the first part of the theorem.

To prove the second part, we have to show that for any integers c_1, c_2 we have

$$\left(\frac{c_1 c_2}{p}\right)_L = \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$

If $c_1 \equiv 0 \pmod{p}$ or $c_2 \equiv 0 \pmod{p}$, then both sides are 0, so we can suppose that $c_1 c_2 \not\equiv 0 \pmod{p}$. Now

$$\begin{aligned}\left(\frac{c_1 c_2}{p}\right)_L &\equiv (c_1 c_2)^{\frac{p-1}{2}} \\ &\equiv c_1^{\frac{p-1}{2}} c_2^{\frac{p-1}{2}} \\ &\equiv \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L \pmod{p}.\end{aligned}$$

Thus p divides

$$\left(\frac{c_1 c_2}{p}\right)_L - \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$

But this is $-2, 0$ or 2 and so has to be 0 since $p > 2$ □

We can use this to evaluate the Legendre symbol in special cases.

ex:five7 **Example 5.7.** *Suppose that p is an odd prime. Then*

$$\left(\frac{-1}{p}\right)_L = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4}. \end{cases}$$

Observe that by Euler's criterion

$$\left(\frac{-1}{p}\right)_L \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Now the difference between the left and right hand sides is $-2, 0$ *or* 2 *and the same argument as above gives equality.*

This example has some interesting consequences.

1. Every odd prime divisor p *of the polynomial* $x^2 + 1$ *satisfies* $p \equiv 1 \pmod 4$.

2. There are infinitely many primes of the form $4k + 1$.

To see 1. one only has to observe that for any such prime factor -1 *has to be a quadratic residue, so its Legendre symbol is* 1. *To deduce 2., follow Euclid's argument by supposing there are only finitely many such, say* $p_1, \dots, p_r$, *and take* x *to be* $2p_1 \dots p_r$.

A famous question, first asked by I. M. Vinogradov in 1919, concerns the size $n_2(p)$ of the *least* positive QNR modulo p. One thing one can see straight away is that $n_2(p)$ has to be prime, since it must have a prime factor which is a QNR. He conjectured that for any fixed positive number $\varepsilon > 0$ we should have $n_2(p) < C(\varepsilon)p^{\varepsilon}$ and then proceeded to prove this at least when $\varepsilon > \frac{1}{2\sqrt{e}}$ where e is the base of the natural logarithm! In 1959 David Burgess, in his PhD thesis (!!) reduced this to any $\varepsilon > \frac{1}{4\sqrt{e}}$. Where on earth does the $\sqrt{e}$ come from? This was one of the things that got me interested in number theory when I was a student. Here is an easier result.

thm:five2a **Theorem 5.3.** *Suppose that* p *is an odd prime. Then*

$$n_2(p) \leq \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

Proof. Let k be the smallest k such that $p < kn_2(p)$. Since $n_2(p)$ cannot divide p we have $p < kn_2(p) < p + n_2(p)$. Thus $kn_2(p)$ is a QR, and so k is a QNR. Therefore $n_2(p) \leq k$ and so $n_2(p)^2 \leq p + n_2(p) - 1$. This can be rearranged as $n_2(p)^2 - n_2(p) \leq p - 1$, so $(n_2(p) - \frac{1}{2})^2 \leq p - \frac{3}{4}$. The theorem follows by taking the square. root. □

The multiplicative property of the Legendre symbol tells us that it suffices to understand

$$\left(\frac{q}{p}\right)_L$$

when p is an odd prime and q is prime. When q is also odd, Euler found a remarkable relationship between this Legendre symbol and

$$\left(\frac{p}{q}\right)_L$$

but no one in the eighteenth century was able to prove it. Gauss proved it when he was 19! The relationship enables one to imitate the Euclid algorithm and so rapidly evaluate the Legendre symbol.

5.1.1 Exercises

1. Find a complete set of quadratic residues r modulo 13 in the range $1 \leq r \leq 12$.

2. Find a complete set of quadratic residues r modulo 17 in the range $1 \leq r \leq 16$.

3. Find a complete set of quadratic residues r modulo 23 in the range $1 \leq r \leq 22$.

4. Find all solutions (if there are any) to each of the following congruences
(i) $x^2 \equiv -1 \pmod{7}$, (ii) $x^2 \equiv -1 \pmod{13}$, (iii) $x^5 + 4x \equiv 0 \pmod{5}$.

5. Suppose that p is an odd prime and g is a primitive root modulo p. Prove that g is a quadratic non-residue modulo p.

6. Prove that $7n^3 - 1$ can never be a perfect square.

7. Prove that if p is an odd prime, then

$$\sum_{x=1}^{p} \sum_{y=1}^{p} \left(\frac{xy+1}{p} \right)_L = p.$$

8. (i) Recall that for every reduced residue class r modulo p there is a unique reduced residue class s_r modulo p such that $1 \equiv rs_r \pmod{p}$, and that for every reduced residue class s modulo p there is a unique r such that $s_r \equiv s \pmod{p}$. Hence prove that if p is an odd prime, then

$$\sum_{r=1}^{p-1} \left(\frac{r(r+1)}{p} \right)_L = \sum_{s=1}^{p-1} \left(\frac{1+s}{p} \right)_L = -1.$$

(ii) Prove that if p is an odd prime, then the number of residues r modulo p for which both r and $r+1$ are quadratic residues is

$$\frac{p - (-1)^{\frac{p-1}{2}}}{4} - 1.$$

9. Let $N(p;c)$ be as in Example 5.6 so that

$$N(p;c) = p + \sum_{z=1}^{p} \left(\frac{z(c-z)}{p} \right)_L.$$

(i) Prove that if $c \equiv 0 \pmod{p}$, then

$$N(p;0) = p + (-1)^{\frac{p-1}{2}}(p-1).$$

(ii) Prove that if $c \not\equiv 0 \pmod{p}$, then

$$\sum_{z=1}^{p} \left(\frac{z(c-z)}{p} \right)_L = \sum_{z=1}^{p-1} \left(\frac{z^2(cs_z - 1)}{p} \right)_L = \sum_{s=1}^{p-1} \left(\frac{cs-1}{p} \right)_L = -(-1)^{\frac{p-1}{2}}.$$

(iii) Deduce that if $c \not\equiv 0 \pmod{p}$, then

$$N(p;c) = p - (-1)^{\frac{p-1}{2}}.$$

10. Let g be a primitive root modulo p. Prove that the quadratic residues are precisely the residue classes g^{2k} with $0 \le k < \frac{1}{2}(p-1)$. Show that the sum of the quadratic residues modulo p is the 0 residue.

11. Prove that every quadratic non-residue modulo p is a primitive root modulo p if and only if $p = 2^{2^n} + 1$ for some non-negative integer n.

12. Suppose that $p \nmid a$. Show that the number of solutions to $ax^2 + bx + c \equiv 0 \pmod{p}$ is $1 + \left(\frac{b^2-4ac}{p}\right)_L$.

13. Prove that $\sum_{x=1}^{p} \left(\frac{x}{p}\right)_L = 0$ and that if $p \nmid a$, then $\sum_{x=1}^{p} \left(\frac{ax+b}{p}\right)_L = 0$.

14. Let $S(p,a,b,c) = \sum_{x=1}^{p} \left(\frac{ax^2+bx+c}{p}\right)_L$.

(i) Show that $S(p,1,b,0) = \sum_{y=1}^{p-1} \left(\frac{1+by}{p}\right)_L$. (Hint: For each x with $1 \le x \le p-1$ let y denote the unique solution to $xy \equiv 1 \pmod{p}$, so that $x(x+b) \equiv x^2(1+by)$.) Deduce that $S(p,1,b,0) = p-1$ when $p|b$ and is -1 when $p \nmid b$.

(ii) Show that $S(p,1,0,c) = \sum_{y=1}^{p} \left(\frac{y+c}{p}\right)_L \left(1 + \left(\frac{y}{p}\right)_L\right)$. (Hint: Note that for each y with $1 \le y \le p$ the number of solutions in x to $x^2 \equiv y \pmod{p}$ is $1 + \left(\frac{y}{p}\right)_L$) Deduce that $S(p,1,0,c) = S(p,1,c,0) = p-1$ when $p|c$ and is -1 when $p \nmid c$.

(iii) Show that if $p \nmid a$, then $S(p,a,b,c) = \left(\frac{4a}{p}\right)_L S(p,1,0,4ac-b^2)$. Deduce that $S(p,a,b,c) = p\left(\frac{c}{p}\right)_L$ when $p|a$ and $p|b$, is 0 when $p|a$ and $p \nmid b$, and satisfies

$$S(p,a,b,c) = \begin{cases} \left(\frac{a}{p}\right)_L (p-1) & \text{when } p \nmid a \text{ and } p|b^2-4ac, \\ -\left(\frac{a}{p}\right)_L & \text{when } p \nmid a(b^2-4ac). \end{cases} \tag{5.4}$$ eq:five3a

5.2 Quadratic Reciprocity

What Euler spotted was a very curious relationship between the values of

$$\left(\frac{q}{p}\right)_L$$

when p and q are different odd primes, which only depended on their residue classes modulo 4. Of course, this was before the Legendre symbol was invented and he described the phenomenon in terms of quadratic residues and non-residues.

ex:fivea **Example 5.8.** *Here is a short table of values for primes out to* 29.

$p\backslash q$	3	5	7	11	13	17	19	23	29
3	0	−1	1	−1	1	−1	1	−1	−1
5	−1	0	−1	1	−1	−1	1	−1	1
7	−1	−1	0	1	−1	−1	−1	1	1
11	1	1	−1	0	−1	−1	−1	1	−1
13	1	−1	−1	−1	0	1	−1	1	1
17	−1	−1	−1	−1	1	0	−1	−1	−1
19	−1	1	1	1	−1	1	0	1	−1
23	1	−1	−1	−1	1	−1	−1	0	1
29	−1	1	1	−1	1	−1	−1	1	0

Table of $\left(\frac{q}{p}\right)_L$ for odd primes $p, q \le 23$.

Apparently if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{q}{p}\right)_L = \left(\frac{p}{q}\right)_L$, but if $p \equiv q \equiv 3 \pmod 4$, then $\left(\frac{q}{p}\right)_L \neq \left(\frac{p}{q}\right)_L$.

Gauss was fascinated by this and eventually found at least seven (!) different proofs. The first step in many of them is Gauss' Lemma.

Theorem 5.4 (Gauss' Lemma)**.** *Suppose that p is an odd prime and $(a, p) = 1$. Apply the division algorithm to write each of the $\frac{1}{2}(p-1)$ numbers ax with $1 \le x < \frac{1}{2}p$ as $ax = q_x p + r_x$ with $0 \le r_x < p$. Let m be the number of r_x with $\frac{1}{2}p < r_x < p$. Then we have*

$$\left(\frac{a}{p}\right)_L = (-1)^m$$

where

$$m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2.$$

This theorem enables us to evaluate quite a number of cases directly with some ease.

ex:five8 **Example 5.9.** *Take $a = 2$. Then we begin by considering the numbers $2x$ with $1 \le x < \frac{1}{2}p$. These numbers satisfy $2 \le 2x < p$. In view of the latter inequality, they are their own remainder, i.e. $r_x = 2x$, so we need to count the number of x with $\frac{1}{2}p < 2x < p$, that is $\frac{1}{4}p < x < \frac{1}{2}p$. Hence the number of such x is*

$$m = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor.$$

Now suppose that $p = 8k + 1$. Then $m = 4k - 2k$ is even. Likewise when $p = 8k + 7$ we have $m = 2k + 2$ is also even. It can be checked similarly that if $p \equiv 3$ or $5 \pmod 8$,

then m is odd. Thus

$$\left(\frac{2}{p}\right)_L = \begin{cases} 1 & (p \equiv \pm 1 \pmod 8), \\ -1 & (p \equiv \pm 3 \pmod 8). \end{cases} \tag{5.5}$$ eq:five4

One can check that another way of writing this is

$$\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}.$$

It is relatively easy to deal with the case $a = 3$ in a similar way.

Proof of Gauss' Lemma. The proof is combinatorial - a kind of counting argument. We consider the product

$$a^{\frac{p-1}{2}} \prod_{1 \le x < p/2} x = \prod_{1 \le x < p/2} ax.$$

This is

$$\equiv \prod_{1 \le x < p/2} r_x \pmod p.$$

Let $\mathcal{A}$ be the set of x with $p/2 < r_x < p$ and $\mathcal{B}$ the x with $1 \le r_x < p/2$. Then $\operatorname{card} \mathcal{A} = m$ and we can rearrange the product to give

$$a^{\frac{p-1}{2}} \prod_{1 \le x < p/2} x \equiv \left(\prod_{x \in \mathcal{A}} r_x\right) \prod_{x \in \mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x \in \mathcal{A}} (p - r_x)\right) \prod_{x \in \mathcal{B}} r_x \pmod p. \tag{5.6}$$ eq:five6

Since $|r_x - r_y| < p$ and $r_x - r_y \equiv a(x-y) \pmod p$ we have $r_x \ne r_y$ when $x \ne y$. Thus the r_x are distinct. Also since $p \nmid a$ and $1 \le x, y < p/2$ we have $p - r_x - r_y \equiv -a(x+y) \not\equiv 0 \pmod p$. Therefore the $p - r_x$ with $x \in \mathcal{A}$ are distinct from the r_y with $y \in \mathcal{B}$. Hence in the expression on the right in (5.6) the $\frac{1}{2}(p-1)$ numbers $p - r_x$ and r_x are just a permutation of the numbers z with $1 \le z \le \frac{1}{2}(p-1)$. Thus (5.6) becomes

$$a^{\frac{p-1}{2}} \prod_{1 \le x < p/2} x \equiv (-1)^m \prod_{1 \le x < p/2} x \pmod p$$

and so, by Euler's Criterion,

$$\left(\frac{a}{p}\right)_L \equiv a^{\frac{p-1}{2}} \equiv (-1)^m \pmod p.$$

Now we can complete the proof of the first formula in the theorem by our usual observation that the difference between the two sides is -2, 0 or 2.

For the final formula we note that

$$r_x = ax - p\left\lfloor \frac{ax}{p} \right\rfloor \tag{5.7}$$ eq:five7

so that $0 \leq r_x < p$. Now $0 < 2r_x/p < 2$ and so $\lfloor 2r_x/p \rfloor = 0$ or 1 and is 1 precisely when $p/2 < r_x < p$. Thus

$$m = \sum_{1 \leq x < p/2} \lfloor 2r_x/p \rfloor.$$

Moreover, by (5.7)

$$\begin{aligned} \lfloor 2r_x/p \rfloor &= \left\lfloor \frac{2ax}{p} - 2\left\lfloor \frac{ax}{p} \right\rfloor \right\rfloor \\ &= \left\lfloor \frac{2ax}{p} \right\rfloor - 2\left\lfloor \frac{ax}{p} \right\rfloor \\ &\equiv \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2 \end{aligned}$$

and the final formula follows. □

If we restrict our attention to odd a there is a useful variant of this.

Theorem 5.5. *Suppose that p is an odd prime and $(a, 2p) = 1$. Then*

$$\left(\frac{a}{p}\right)_L = (-1)^n$$

where

$$n = \sum_{1 \leq x < p/2} \left\lfloor \frac{ax}{p} \right\rfloor.$$

We also have

$$\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}.$$

Proof. We have

$$\begin{aligned} \left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L &= \left(\frac{2}{p}\right)_L \left(\frac{a+p}{p}\right)_L \\ &= \left(\frac{4}{p}\right)_L \left(\frac{(a+p)/2}{p}\right)_L \\ &= \left(\frac{(a+p)/2}{p}\right)_L \\ &= (-1)^l \end{aligned}$$

where

$$\begin{aligned} l &= \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{(a+p)x}{p} \right\rfloor \\ &= \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{ax}{p} + x \right\rfloor \\ &= \sum_{x=1}^{(p-1)/2} \left(\left\lfloor \frac{ax}{p} \right\rfloor + x \right) \\ &= n + \frac{p^2-1}{8}. \end{aligned}$$

If we take $a = 1$, then we have recovered the stated formula for

$$\left(\frac{2}{p}\right)_L.$$

Then factoring out the formula for this give the result for

$$\left(\frac{a}{p}\right)_L.$$

□

Now we come to the big one. This is the Law of Quadratic Reciprocity. Gauss called it "Theorema Aureum", the Golden Theorem.

Theorem 5.6 (The Law of Quadratic Reciprocity)**.** *Suppose that p and q are odd prime numbers. Then*

$$\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

or equivalently

$$\left(\frac{q}{p}\right)_L = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)_L,$$

We can use this to compute rapidly Legendre symbols.

ex:five8a **Example 5.10.**

$$\left(\frac{11}{23}\right)_L = (-1)^{\frac{11-1}{2}\cdot\frac{23-1}{2}} \left(\frac{23}{11}\right)_L = (-1)^{55} \left(\frac{1}{11}\right)_L = (-1)\cdot 1 = -1.$$

ex:five8b **Example 5.11.**

$$\begin{aligned} \left(\frac{101}{107}\right)_L &= (-1)^{50\cdot 53} \left(\frac{107}{101}\right)_L = 1 \cdot \left(\frac{6}{101}\right)_L = \left(\frac{2}{101}\right)_L \left(\frac{3}{101}\right) \\ &= (-1)^{\frac{(101)^2-1}{8}} (-1)^{50\cdot 1} \left(\frac{101}{3}\right)_L (-1)^{1275} \left(\frac{2}{3}\right)_L = (-1)(-1) = 1. \end{aligned}$$

ex:five9 **Example 5.12.** *Is* $x^2 \equiv 951 \pmod{2017}$ *soluble?* 2017 *is prime but* $951 = 3 \times 317$. *Thus*

$$\left(\frac{951}{2017}\right)_L = \left(\frac{3}{2017}\right)_L \left(\frac{317}{2017}\right)_L.$$

Now by the law, since $2017 \equiv 1 \pmod{4}$,

$$\left(\frac{3}{2017}\right)_L = \left(\frac{2017}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1$$

and

$$\left(\frac{317}{2017}\right)_L = \left(\frac{2017}{317}\right)_L = \left(\frac{115}{317}\right)_L = \left(\frac{5}{317}\right)_L \left(\frac{23}{317}\right)_L.$$

Again applying the law, we have

$$\left(\frac{5}{317}\right)_L = \left(\frac{317}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1$$

and

$$\left(\frac{23}{317}\right)_L = \left(\frac{317}{23}\right)_L = \left(\frac{18}{23}\right)_L = \left(\frac{2}{23}\right)_L = 1$$

so that

$$\left(\frac{317}{2017}\right)_L = -1$$

and thus

$$\left(\frac{951}{2017}\right)_L = -1.$$

Thus the congruence is insoluble.

We can also use the law to obtain general rules, like that for $2 \pmod{p}$.

ex:five10 **Example 5.13.** *Let* $p > 3$ *be an odd prime. Then*

$$\left(\frac{3}{p}\right)_L = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)_L.$$

Now p *is a QR modulo 3 iff* $p \equiv 1 \pmod{3}$. *Thus*

$$\left(\frac{3}{p}\right)_L = \begin{cases} (-1)^{\frac{p-1}{2}} & \big(p \equiv 1 \pmod{3}\big) \\ -(-1)^{\frac{p-1}{2}} & \big(p \equiv 2 \pmod{3}\big). \end{cases}$$

We can also combine this with the formula in the case of $-1 \pmod{p}$ *which follows from the Euler Criterion. Thus*

$$\left(\frac{-3}{p}\right)_L = \begin{cases} 1 & \big(p \equiv 1 \pmod{3}\big) \\ -1 & \big(p \equiv 2 \pmod{3}\big). \end{cases}$$

We now turn to the proof of the law.

Proof of the Law of Quadratic Reciprocity. We start from two applications of the previous theorem. Thus

$$\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$$

where

$$u = \sum_{1 \le x < p/2} \left\lfloor \frac{qx}{p} \right\rfloor$$

and

$$v = \sum_{1 \le y < q/2} \left\lfloor \frac{py}{q} \right\rfloor .$$

Observe that $\left\lfloor \frac{qx}{p} \right\rfloor$ is the number of positive integers y with $1 \le y \le qx/p$. Thus the first sum is the number of ordered pairs x, y with $1 \le x < p/2$ and $1 \le y < qx/p$. Likewise $\sum_{1 \le y < q/2} \left\lfloor \frac{py}{q} \right\rfloor$ is the number of ordered pairs x, y with $1 \le y < q/2$ and $1 \le x < py/q$, that is with $1 \le x < p/2$ and $xq/p < y < q/2$. Hence $u + v$ is the number of ordered pairs x, y with $1 \le x < p/2$ and $1 \le y < q/2$. This is

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

and completes the proof. This argument is due to Eisenstein. □

5.2.1 Exercises

1. Evaluate the following Legendre symbols.
   (i) $\left(\frac{2}{127}\right)_L$,
   (ii) $\left(\frac{-1}{127}\right)_L$,
   (iii) $\left(\frac{5}{127}\right)_L$,
   (iv) $\left(\frac{11}{127}\right)_L$.

2. (i) Prove that 3 is a QR modulo p when $p \equiv \pm 1 \pmod{12}$ and is a QNR when $p \equiv \pm 5 \pmod{12}$.

   (ii) Prove that -3 is a QR modulo p for primes p with $p \equiv 1 \pmod 6$ and is a QNR for primes $p \equiv -1 \pmod 6$.

   (iii) By considering $4x^2 + 3$ show that there are infinitely many primes in the residue class $1 \pmod 6$.

3. Show that for every prime p the congruence

$$x^6 - 11x^4 + 36x^2 - 36 \equiv 0 \pmod{p}$$

is always soluble.

4. Find the number of solutions of the congruence (i) $x^2 \equiv 226 \pmod{563}$, (ii) $x^2 \equiv 429 \pmod{563}$.

5. Decide whether $x^2 \equiv 150 \pmod{1009}$ is soluble or not.

6. Find all primes p such that $x^2 \equiv 13 \pmod{p}$ has a solution.

7. Show that $(x^2 - 2)/(2y^2 + 3)$ is never an integer when x and y are integers.

5.3 The Jacobi symbol

In Example 5.12, there were several occasions when we needed to factorise the a in $\left(\frac{a}{p}\right)_L$. Jacobi introduced an extension of the Legendre symbol which avoids this.

def:five3 **Definition 5.3.** *Suppose that m is an odd positive integer and a is an integer. Let $m = p_1^{r_1} \dots p_s^{r_s}$ be the canonical decomposition of m. Then we define the Jacobi symbol by*

$$\left(\frac{a}{m}\right)_J = \prod_{j=1}^{s} \left(\frac{a}{p_j}\right)_L^{r_j}.$$

Note that interpreting 1 as being an "empty product of primes" means that

$$\left(\frac{a}{1}\right)_J = 1.$$

Remarkably the Jacobi symbol has exactly the same properties as the Legendre symbol, except for one. That is, for a general odd modulus m it does not tell us about the solubility of $x^2 \equiv a \pmod{m}$.

ex:five11 **Example 5.14.** *We have*

$$\left(\frac{2}{15}\right)_J = \left(\frac{2}{3}\right)_L \left(\frac{2}{5}\right)_L = (-1)^2 = 1,$$

but $x^2 \equiv 2 \pmod{15}$ is insoluble because any solution would also be a solution of $x^2 \equiv 2 \pmod{3}$ which we know is insoluble.

Properties of the Jacobi symbol

1. Suppose that m is odd. Then
$$\left(\frac{a_1 a_2}{m}\right)_J = \left(\frac{a_1}{m}\right)_J \left(\frac{a_2}{m}\right)_J.$$
2. Suppose that the m_j are odd. Then
$$\left(\frac{a}{m_1 m_2}\right)_J = \left(\frac{a}{m_1}\right)_J \left(\frac{a}{m_2}\right)_J.$$
3. Suppose that m is odd and $a_1 \equiv a_2 \pmod{m}$. Then
$$\left(\frac{a_1}{m}\right)_J = \left(\frac{a_2}{m}\right)_J.$$
4. Suppose that m is odd. Then
$$\left(\frac{-1}{m}\right)_J = (-1)^{\frac{m-1}{2}}.$$
5. Suppose that m is odd. Then
$$\left(\frac{2}{m}\right)_J = (-1)^{\frac{m^2-1}{8}}.$$
6. Suppose that m and n are odd and $(m,n) = 1$. Then
$$\left(\frac{n}{m}\right)_J \left(\frac{m}{n}\right)_J = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

The first three of these follow easily from the definition. The rest depend on algebraic identities combined with inductions on the number of prime factors, but proving them is tiresome. For 4. we need to know that

$$\frac{m_1 - 1}{2} + \frac{m_2 - 1}{2} \equiv \frac{m_1 m_2 - 1}{2} \pmod{2},$$

5. depends on

$$\frac{m_1^2 - 1}{8} + \frac{m_2^2 - 1}{8} \equiv \frac{m_1^2 m_2^2 - 1}{8} \pmod{2}.$$

6. Finally here one needs

$$\frac{l-1}{2}\cdot\frac{m-1}{2} + \frac{n-1}{2}\cdot\frac{m-1}{2} \equiv \frac{ln-1}{2}\cdot\frac{m-1}{2} \pmod{2}.$$

ex:five12 **Example 5.15.** *Return to Example 5.12, where we evaluated* $\left(\frac{951}{2017}\right)_L$. *Now we don't have to factor* 951. *By the Jacobi version of the law*

$$\begin{aligned}\left(\frac{951}{2017}\right)_L &= \left(\frac{2017}{951}\right)_J = \left(\frac{115}{951}\right)_J = -\left(\frac{951}{115}\right)_J \\ &= -\left(\frac{31}{115}\right)_J = \left(\frac{115}{31}\right)_J = \left(\frac{22}{31}\right)_J \\ &= -\left(\frac{31}{11}\right)_J = -\left(\frac{9}{11}\right)_J = -1.\end{aligned}$$

Note that we can process this like the Euclidean algorithm. Suppose we are interested in

$$\left(\frac{n}{m}\right)_L$$

where n and m are odd. Follow the Euclidean algorithm and obtain

$$\begin{aligned} n &= q_1 m + r_1, \\ m &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\vdots \quad \vdots \end{aligned}$$

Then provided that the m, n, r_1, r_2 are all odd, for suitable exponents $t_1, t_2, \ldots$ we obtain

$$\begin{aligned}\left(\frac{n}{m}\right)_J &= \left(\frac{r_1}{m}\right)_J = (-1)^{t_1}\left(\frac{m}{r_1}\right)_J \\ &= (-1)^{t_1}\left(\frac{r_2}{r_1}\right)_J = (-1)^{t_2}\left(\frac{r_1}{r_2}\right)_J \\ &= (-1)^{t_2}\left(\frac{r_3}{r_2}\right)_J = (-1)^{t_3}\left(\frac{r_2}{r_3}\right)_J \\ &\vdots \qquad\qquad \vdots \qquad\qquad \vdots\end{aligned}$$

If any of the r_j should be even, then we adjust things by taking out the highest power of 2.

5.3.1 Exercises

1. Let $n \in \mathbb{Z}$ and let $n = (-1)^u 2^v p_1^{v_1} \ldots p_r^{v_r}$ be the canonical decomposition of n with $u = 0$ or 1, $v \geq 0$, and each $v_j > 0$ when $r \geq 1$.

(i) If v is odd, then let $n_0 = |n|2^{-v}$ and choose $m \in \mathbb{N}$ so that $m \equiv 5 \pmod 8$ and $m \equiv 1 \pmod{n_0}$. Prove that

$$\left(\frac{n}{m}\right)_J = -1.$$

(ii) If v is even, but there is a j for which v_j is odd, let $n_j = |n|2^{-v}p_j^{-v_j}$ and choose $m \in \mathbb{N}$ so that $m \equiv 1 \pmod{(4n_j)}$ and m is a QNR modulo p_j. Prove that

$$\left(\frac{n}{m}\right)_J = -1.$$

(iii) If v is even, v_j is even for every j and $u = 1$, choose $m \in \mathbb{N}$ so that $m \equiv 3 \pmod 4$. Prove that

$$\left(\frac{n}{m}\right)_J = -1.$$

(iv) Prove that if n is not a perfect square, then there is an odd prime number p such that

$$\left(\frac{n}{p}\right)_L = -1.$$

(v) Prove that if n is a QR for every odd prime number p not dividing n, then n is a perfect square.

This is an example of the "local to global" principle.

2. Decide the solubility of
(i) $x^2 \equiv 219 \pmod{383}$,
(ii) $x^2 \equiv 226 \pmod{562}$,
(iii) $x^2 \equiv 429 \pmod{563}$,
(iv) $x^2 \equiv 105 \pmod{317}$.

5.4 Other questions

There are many interesting problems associated with quadratic residues and the Legendre and Jacobi symbols.

1. How many consecutive quadratic residues are there, that is how many x with $1 \le x \le p-2$ have the property that x and $x+1$ are both quadratic residues modulo p? This number is

$$\sum_{x=1}^{p-2} \frac{1}{4}\left(1+\left(\frac{x}{p}\right)_L\right)\left(1+\left(\frac{x+1}{p}\right)_L\right).$$

The method of exercise 5.1.1.13 is useful here. How about the number of triples $x, x+1, x+2$, or how about a fixed sequence of QR and QNR?

2. Given an N with $0 \le N \le p$, how small can you make M, regardless of the value of N, and ensure that the interval $(N, N+M]$ contains a quadratic non-residue?

3. Let m be an odd positive integer, and for brevity write $\chi(x)$ for the Jacobi symbol $\left(\frac{x}{m}\right)_J$. For a complex number z define

$$L(z;\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^z}.$$

This converges for $\Re z > 0$. There is a Riemann hypothesis for this function but we cannot prove it. Also $L(1,\chi)$ has some interesting values. For example if $m = 3$, then

$$L(1,\chi) = \frac{\pi}{3\sqrt{3}}.$$

4. The Gauss sum

$$\tau_p = \sum_{x=1}^{p} \left(\frac{x}{p}\right)_L e^{2\pi i x/p}$$

was studied by Gauss in connection with several of his proofs of the law of quadratic reciprocity. He showed that

$$\tau_p = \begin{cases} \sqrt{p} & (p \equiv 1 \pmod 4) \\ i\sqrt{p} & (p \equiv 3 \pmod 4). \end{cases}$$

5.4.1 Exercises

1. (i) Prove that if $\chi_1(n) = (-1)^{(n-1)/2}$ when n is odd and $\chi_1(n) = 0$ when n is even, then $L(1,\chi_1) = \frac{\pi}{4}$

(ii) Prove that if $\chi(n) = \left(\frac{n}{3}\right)_L$, then $L(1,\chi) = \frac{\pi}{3\sqrt{3}}$

(iii) Prove that if $\chi(n) = \left(\frac{n}{5}\right)_L$, then $L(1,\chi) = \frac{1}{\sqrt{5}} \log \frac{3+\sqrt{5}}{2}$

2. Let $c_n \in \mathbb{C}$ $(n = 1, 2, \ldots, p)$. Prove that

$$\sum_{a=1}^{p} \left| \sum_{n=1}^{p} c_n e^{2\pi i a n/p} \right|^2 = p \sum_{n=1}^{p} |c_n|^2.$$

3. For an odd prime p define

$$S(p,a) = \sum_{y=1}^{p} e^{2\pi i a y^2/p}$$

(i) Prove that if $p \nmid a$, then

$$\begin{aligned} S(p,a) &= \sum_{x=1}^{p} \left(1 + \left(\frac{x}{p}\right)_L\right) e^{2\pi i a x/p} \\ &= \sum_{x=1}^{p} \left(\frac{x}{p}\right)_L e^{2\pi i a x/p} \\ &= \left(\frac{a}{p}\right)_L \tau_p. \end{aligned}$$

(ii) Prove that

$$\sum_{a=1}^{p} |S(p,a)|^2 = p(2p-1).$$

(iii) Prove that

$$\begin{aligned}(p-1)|\tau_p|^2 &= \sum_{a=1}^{p-1} \left| \left(\frac{a}{p}\right)_L \tau_p \right|^2 \\ &= \sum_{a=1}^{p-1} |S(p,a)|^2 \\ &= p(p-1),\end{aligned}$$

whence $|\tau_p| = \sqrt{p}$.

5.5 Computing Solutions to Quadratic Congruences

The first algorithm computes the Jacobi symbol

$$\left(\frac{m}{n}\right)_J$$

for a given positive odd integer n and integer m, and is just an immediate application of the law of quadratic reciprocity together with the removal of any powers of 2 at each stage and an evaluation of the corresponding

$$\left(\frac{2}{n}\right)_J.$$

alg:LJ **Algorithm 5.1 (LJ).** *Given an integer m and a positive integer n, compute $\left(\frac{m}{n}\right)_J$.*
1. *Reduction loops.*

1.1. *Compute $m \equiv m \pmod{n}$, so the new m satisfies $0 \le m < n$. Put $t = 1$.*

1.2. *While $m \neq 0$*

1.2.1. *While m is even*

put $m = m/2$ and, if $n \equiv 3$ or $5 \pmod 8$, then put $t = -t$.

1.2.2. *Interchange m and n.*

1.2.3. *If $m \equiv n \equiv 3 \pmod 4$, then put $t = -t$.*

1.2.4. *Compute $m \equiv m \pmod{n}$, so that the new $m < n$.*

2. *Output.*

2.1. *If $n = 1$, then return t.*

2.2. *Else return 0.*

Generally we will refer to the second and third algorithms here as **QC**. They are often attributed to Shanks (1973) and Tonelli (1891), but in one form or another they in principle go back to Euler, Legendre and Gauss.

The second algorithm computes a solution x to

$$x^2 \equiv a \pmod{p}$$

when p is an odd prime $p \not\equiv 1 \pmod 8$.

alg:QC357/8

Algorithm 5.2 (QC357/8). *Given a prime $p \equiv 3, 5, 7 \pmod 8$ and an a with $\left(\frac{a}{p}\right)_L = 1$, compute a solution to $x^2 \equiv a \pmod p$.*

1. *If $p \equiv 3$ or $7 \pmod 8$, then compute $x \equiv a^{(p+1)/4} \pmod p$. Return x.*

2. *If $p \equiv 5 \pmod 8$, then compute $x \equiv a^{(p+3)/8} \pmod p$. Compute $x^2 \pmod p$.*

2.1. *If $x^2 \equiv a \pmod p$, then return x.*

2.2. *If $x^2 \not\equiv a \pmod p$, then compute $x \equiv x2^{(p-1)/4} \pmod p$. Return x.*

Proof. The proof that this gives a solution is relatively easy. When $p \equiv 3 \pmod 4$ we have $\frac{p+1}{4} \in \mathbb{N}$, so

$$x \equiv a^{(p+1)/4} \pmod p$$

makes sense and then

$$x^2 \equiv a^{(p+1)/2} = a^{1+\frac{p-1}{2}} \equiv a\left(\frac{a}{p}\right)_L = a \pmod p$$

by Euler's criterion.

When $p \equiv 5 \pmod 8$, the only case at issue is when $a^{(p+3)/4} \not\equiv a \pmod p$, so that $a^{(p-1)/4} \not\equiv 1 \pmod p$. But by Euler's criterion $a^{(p-1)/2} \equiv 1 \pmod p$, so $a^{(p-1)/4} \equiv \pm 1 \pmod p$, and hence $a^{(p-1)/4} \equiv -1 \pmod p$. Thus the new choice of x gives

$$x^2 \equiv a^{(p+3)/4}2^{(p-1)/2} \equiv (-a)\left(\frac{2}{p}\right)_L = (-a)(-1)^{(p^2-1)/8} = (-a)(-1) = a \pmod p.$$

□

The final algorithm deals with the trickier case $p \equiv 1 \pmod 8$. This algorithm will work for any odd prime, but the previous algorithm is faster for $p \not\equiv 1 \pmod 8$.

alg:QC1/8

Algorithm 5.3 (QC1/8). *Given a prime $p \equiv 1 \pmod 8$ and an a with $\left(\frac{a}{p}\right)_L = 1$, compute a solution to $x^2 \equiv a \pmod p$.*

1. *Compute a random integer b with $\left(\frac{b}{p}\right)_L = -1$. In practice checking successively the primes $b = 2, 3, 5, \ldots$, or even crudely just the integers $b = 2, 3, 4, \ldots$, will find such a b quickly.*

2. *Factor out the powers of 2 in $p - 1$, so that $p - 1 = 2^s u$ with u odd. Compute $d \equiv a^u \pmod p$. Compute $f \equiv b^u \pmod p$.*

3. *Compute an m so that $df^m \equiv 1 \pmod p$ as follows.*

3.1. *Initialise* $m_0 = 0$.

3.2. *For each* $i = 0, 1, \ldots, s-1$ *compute* $g \equiv (df^{m_i})^{2^{s-1-i}} \pmod{p}$. *If* $g \equiv -1 \pmod{p}$, *then put* $m_{i+1} = m_i + 2^i$. *Otherwise take* $m_{i+1} = m_i$

3.3. *Return* $m = m_s$. *This will satisfy*

$$df^m \equiv 1 \pmod{p}, \text{ and } m \text{ will be even.} \tag{5.8}$$ eq:five8

4. *Compute* $x \equiv a^{(u+1)/2} f^{m_s/2} \pmod{p}$. *Return* x.

Proof. The proof that this works is a little more involved than the previous algorithms. That x is a solution follows because

$$\left(a^{\frac{u+1}{2}} f^{\frac{m}{2}}\right)^2 = a^{u+1} f^m = adf^m \equiv a \pmod{p}.$$

The crucial thing is (5.8). To prove this we first make some observations. We have

$$d^{2^{s-1}} \equiv a^{2^{s-1}u} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

by Euler's criterion. Hence $\mathrm{ord}_p(d) | 2^{s-1}$. Also

$$f^{2^{s-1}} \equiv b^{2^{s-1}u} = b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

by Euler's criterion. Moreover

$$f^{2s} \equiv b^{p-1} \equiv 1 \pmod{p},$$

so $\mathrm{ord}_p(f) = 2^s$.

Now we prove by induction on i for $0 \leq i \leq s$ that

$$(df^{m_i})^{2^{s-i}} \equiv 1 \pmod{p}.$$

For the base case $i = 0$ we have $m_0 = 0$ so that

$$(df^{m_0})^{2^s} = d^{2^s} \equiv 1 \pmod{p}.$$

For the inductive step suppose that for some i with $0 \leq i \leq s-1$ we have

$$(df^{m_i})^{2^{s-i}} \equiv 1 \pmod{p}.$$

Then

$$(df^{m_i})^{2^{s-1-i}} \equiv \pm 1 \pmod{p}.$$

If

$$(df^{m_i})^{2^{s-1-i}} \equiv 1 \pmod{p},$$

then $m_{i+1} = m_i$ and so

$$(df^{m_{i+1}})^{2^{s-1-i}} \equiv 1 \pmod{p}$$

as required. If

$$(df^{m_i})^{2^{s-1-i}} \equiv -1 \pmod{p},$$

then $m_{i+1} = m_i + 2^i$ and so

$$\begin{aligned}(df^{m_{i+1}})^{2^{s-1-i}} &\equiv (df^{2^i+m_i})^{2^{s-1-i}} \\ &= (df^{m_i})^{2^{s-1-i}} f^{2^{s-1}} \\ &\equiv -b^{\frac{p-1}{2}} \\ &\equiv 1 \pmod{p}\end{aligned}$$

once more, by Euler's criterion. □

5.5.1 Exercises

1. Write a computer program to implement (LJ), and use it evaluate the Legendre symbols

$$\text{(i)} \left(\frac{40000000003}{100000000019}\right)_L, \quad \text{(ii)} \left(\frac{100000000057}{40000000031}\right)_L, \text{(iii)} \quad \left(\frac{40000000003}{100000000091}\right)_L.$$

2. Write an algorithm (QC) to find the solutions to $x^2 \equiv a \pmod{p}$ where a are the quadratic residues and p are the corresponding primes occurring in question 1. above. 3.

Consider the numbers

$$a_1 = 23456789023456787,$$

$$a_2 = 23456789023456789,$$

$$m_1 = 77778888999911107,$$

$$m_2 = 55556666777711111.$$

Use (LJ) to evaluate

$$\left(\frac{a_1}{m_1}\right)_J, \quad \left(\frac{a_2}{m_1}\right)_J, \quad \left(\frac{a_1}{m_2}\right)_J, \quad \left(\frac{a_2}{m_2}\right)_J.$$

Assuming that the m_j are prime, for those a_i for which the Legendre symbol is $+1$ solve (QC)

$$x^2 \equiv a_i \pmod{m_j}.$$

5.6 Notes

sec:five5

§1. Fermat and Euler had studied questions which in modern terminology can be described in terms of the solubility of quadratic congruences. A. M. Legendre's eponymous symbol was introduced by him in "Essai sur la théorie des nombres", Paris, 1798, p. 186. I. M. Vinogradov made his conjecture on the least quadratic non-residue in "On the distribution of quadratic residues and non-residues", Zh. Fiz,-Mt. Obshch. Univ. Perm 2, 1-16, 1919. The estimate of D. A. Burgess's result is in "The distribution of quadratic residues and non-residues", Mathematika 4(1957), 106-112.

Assuming the Riemann Hypothesis associated with the Dirichlet L-function $L(s;\chi)$ where χ is the Legendre symbol, Ankeny showed that $n_2(p) = O\big((\log p)^2\big)$. For an account of this see H. L. Montgomery, "Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis", American Mathematical Society, 1994, p. 176. ISBN 0-8218-0737-4.

Yu. V. Linnik "A remark on the least quadratic non-residue, Doklady Akad. Nauk URSS (N.S.) 36(1942), 119–120, showed that if there are any primes for which $n_2(p)$ is unexpectedly large, then they are rare. In particular he showed that if $c > 0$ is fixed, then the number of primes p with $2 < p \le x$ such that $n_2(p) > (\log p)^c$ is at most

$$x^{2/c+f(x)}$$

where $f(x) \to 0$ as $x \to \infty$, and that if $\delta > 0$ is fixed, then the number of primes p with $2 < p \le x$ for which $n_2(p) > p^\delta$ is at most

$$C(\delta) \log\log x$$

where $C(\delta)$ is a positive number which depends only on δ.

§2. Euler in 1783 had formulated a conjecture that if we take the primes p in the residue class r modulo $4m$, then the residue class m modulo p is always a QR modulo p or always a QNR modulo p and moreover $4m - r$ is the same. That is, when $p \nmid 4m$,

$$\left(\frac{m}{p}\right)_L$$

depends only on the residue class r in which p lies modulo $4m$, and is the same for primes in the residue class $4m-r$. This follows at once from the LQR in our modern formulation. The first correct proof is due to Gauss (1796). This was before Legendre invented his symbol and Gauss used the much clumsier notation aRp and aNp to indicate whether a was a quadratic residue modulo p or a quadratic non-residue.

§3. Jacobi defined his symbol in C. G. J. Jacobi (1837), "Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie", Bericht Ak. Wiss. Berlin, 127–136.

§4. The investigation of the distribution of patterns of k consecutive QR and QNR is intimately connected with questions concerning the zeros of the zeta function of curves $y^2 = f(x)$ over finite fields. See the article on "Quadratic residue patterns modulo a prime" by Keith Conrad at `https://kconrad.math.uconn.edu/blurbs/`

Exercise 5.5.3 shows that the sum

$$S(p,a) = \sum_{x=1}^{p} e(ax^2/p)$$

is closely related to τ_p. Gauss showed that $\tau_p = \sqrt{p}$ when $p \equiv 1 \pmod 4$ and $\tau_p = i\sqrt{p}$ when $p \equiv 3 \pmod 4$ and used this as the basis of one of his proofs of LQR.

We know less about the sums

$$S_k(a,p) = \sum_{x=1}^{p} e(ax^k/p).$$

We do know that if $p \nmid a$, then

$$|S_k(p,a)| \leq \big((k,p-1)-1\big)\sqrt{p}.$$

but in general we do not know how

$$p^{-1/2}S_k(p,a)$$

is distributed. In a few cases, especially the cubic case when $p \equiv 1 \pmod 3$ it is known that the argument is "uniformly distributed". See D. R. Heath-Brown, "Kummer's conjecture for cubic Gauss sums", Israeli. J. Math. 120(2000), 97–124 and the reference to the earlier paper of Heath-Brown and Patterson.

Chapter 6

Primality and Probability

6.1 Miller-Rabin

In its simplest form the Miller-Rabin test is a test for composites, although with some compromises it is also an effective test for primality.

thm:six1 **Theorem 6.1.** *Let $n \in \mathbb{N}$ be odd, $n > 1$ and take out the powers of 2 from $n-1$ so that*

$$n - 1 = 2^u v$$

where v is odd. Choose $a \in \{2, 3, \ldots, n-2\}$. If

$$a^v \not\equiv 1 \pmod{n} \text{ and } a^{2^w v} \not\equiv -1 \pmod{n} \text{ for } 1 \leq w \leq u-1, \tag{6.1}$$ eq:six2

then n is composite and a is a **witness**.

Proof. If $(a, n) > 1$, then (6.1) will hold and n will be composite. Suppose that $(a, n) = 1$ and n were to be prime. Then by Fermat-Euler we have

$$n | a^{n-1} - 1 = a^{2^u v} - 1 = (a^v - 1)(a^v + 1)(a^{2v} + 1) \ldots (a^{2^{u-1} v} + 1) \tag{6.2}$$ eq:six3

and n would have to divide one of the factors on the right, contradicting (6.1). □

If we can find a witness, then we have certainty that n is composite. There are some observations that one can make in association with this. It is a good idea to check a couple of things before applying the test since they can be checked very rapidly.

A. Check n for small prime factors p for, say, $p \leq \log n$.

B. Check that n is not a prime power, $n = p^k$. One can do this by checking to see if

$$n^{1/k} = \lfloor n^{1/k} \rfloor$$

for $2 \leq k \leq \frac{\log n}{\log 2}$. These remarks combined with the next theorem show that witnesses always exist.

thm:six2 **Theorem 6.2.** *If n is odd and has at least two different prime factors p and q, then they can be chosen so that*

$$p-1=2^j l,\ q-1=2^k m, j\le k,$$

and then there are a with $(a,n)=1$ and

$$\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)>0$$

and such an a is a witness.

As it stands this theorem only proves the existence of witnesses. Since we do not expect to have found numerical values for p or q, it does not tell us how to find the a. However it can be used to show that we do not have to search very far. By the way, this process reminds me that much of mathematical research, indeed much of scientific research, is forensic in nature. We are currently studying the pathology of factorisation.

When $(a,n)=1$, the expression

$$\frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)$$

is 0 or 1, and when it is 1, a is a witness. Thus the number of witnesses for n is at least

$$\sum_{\substack{a=1\\(a,n)=1}}^{n}\frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right).$$

Moreover

$$\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{p}\right)_L=\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{q}\right)_L=\sum_{\substack{a=1\\(a,n)=1}}^{n}\left(\frac{a}{pq}\right)_J=0$$

(see Exercise 6.1.1). Thus

$$\sum_{\substack{a=1\\(a,n)=1}}^{n}\frac{1}{4}\left(1+\left(\frac{a}{p}\right)_L\right)\left(1-\left(\frac{a}{q}\right)_L\right)=\frac{\phi(n)}{4}.$$

Therefore at least a quarter of all reduced residues modulo n act as witness. Hence we can proceed by picking N values of a at random. Then the probability that none of them are witnesses is at most $(3/4)^N$. Therefore if we pick, say, at least $10\log n$ numbers a at random, then we can be practically certain of finding a witness.

If we want some kind of absolute certainty, then we can assume the truth of the Riemann hypothesis for the three functions

$$L(s;\chi)=\sum_{m=1}^{\infty}\frac{\chi(m)}{m^s}$$

with

$$\chi(m) = \left(\frac{m}{p}\right)_L, \ \chi(m) = \left(\frac{m}{q}\right)_L, \ \chi(m) = \left(\frac{m}{pq}\right)_J, \tag{6.3}$$ eq:six5

which in practice means that we have to assume it for every Jacobi symbol modulo n since in principal we do not know the numerical values of p and q. This hypothesis implies that if n is large, then for $N = 2(\log n)^2$ we have

$$\sum_{\substack{r \le N \\ r \text{ prime}}} (1 - r/N)\left(1 + \left(\frac{r}{p}\right)_L\right)\left(1 - \left(\frac{r}{q}\right)_L\right)(\log r) > 0. \tag{6.4}$$ eq:six6

In turn, this tells us that not only is there a witness $a \le 2(\log n)^2$, but we can suppose that it is prime.

Proof of Theorem 6.2. Let p and q be as in the hypothesis and suppose they divide n to order d and e respectively. If we choose any QR x modulo p, any QNR y modulo q, and any z with $(z, np^{-d}q^{-e}) = 1$, then by the Chinese Remainder Theorem, Theorem 3.12, it follows that there are $a \equiv x \pmod{p}$, $\equiv y \pmod{q}$ and $\equiv z \pmod{np^{-d}q^{-e}}$ which satisfy the hypothesis. If $a^{n-1} \not\equiv 1 \pmod{n}$, then none of the factors on the right of (6.2) can be divisible by n, so any such a will be a witness. Thus we can suppose that we have $a^{n-1} \equiv 1 \pmod{n}$.

Let u and v be as in Theorem 6.1 so that $n - 1 = 2^u v$ with v odd. For $0 \le w \le u - 1$ we have

$$a^{2^w v} + 1 = (a^v - 1 + 1)^{2^w} + 1 \equiv 2 \pmod{a^v - 1}.$$

Hence

$$\left(a^v - 1, a^{2^w v} + 1\right) | 2.$$

Likewise when $0 \le w < x \le u - 1$ we have

$$a^{2^x v} + 1 = (a^{2^w v} + 1 - 1)^{2^{x-w}} + 1 \equiv 2 \pmod{a^{2^w v} = 1}$$

and so

$$\left(a^{2^w v} + 1, a^{2^x v} + 1\right) | 2.$$

Thus p and q, and *a fortiori* n cannot divide two different factors in (6.2).

Thus it remains to just consider the case when n divides exactly one of the factors $a^v - 1$, $a^{2^w u} + 1$. The hypothesis implies that

$$\left(\frac{a}{p}\right)_L = 1, \ \left(\frac{a}{q}\right)_L = -1.$$

Hence, by Euler's Criterion, Theorem 5.2,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \ a^{\frac{q-1}{2}} \equiv -1 \pmod{q}.$$

Let $e = \mathrm{ord}_p(a)$ and $f = \mathrm{ord}_q(a)$. Then

$$e \left| \frac{p-1}{2} \right. , \; f | q-1, \; f \nmid \frac{q-1}{2}.$$

Recall that the hypothesis also states that

$$p - 1 = 2^j l, \; q - 1 = 2^k m, j \leq k.$$

Hence

$$e = 2^i l', \; f = 2^k m' \text{ with } 0 \leq i \leq j-1, \; l' | l, \; m' | m.$$

In particular

$$0 \leq i < j \leq k. \tag{6.5}$$ eq:six4

Recall n divides exactly one of the expressions

$$a^v - 1, \; a^v + 1, \ldots, a^{2^{u-1}v} + 1.$$

Consider the different possibilities. If $n | a^v - 1$, then $a^v \equiv 1 \pmod{q}$ and $f | v$. But f is even and v is odd, so this is impossible.

If $n | a^{2^s v} + 1$ for some s with $0 \leq s \leq u-1$, then

$$a^{2^{s+1}v} \equiv 1 \pmod{n}, \; a^{2^s v} \equiv -1 \pmod{n}.$$

Thus

$$e | 2^{s+1} v, e \nmid 2^s v,$$

and since $e = 2^i l'$ we have $l' | v, i = s+1$. Moreover

$$f | 2^{s+1} v, f = 2^k m', 2^k m' | 2^{s+1} v, m' | v, k \leq s+1.$$

Thus $k \leq i$ which contradicts (6.5). Hence a is a witness. □

Note that the previous theorem depends on the theory of quadratic residues and non-residues. Thus it should be no surprise that showing that there is a small witness is similar to showing that there are small quadratic non-residues. Thus the best bound for a leads to questions which have a similar provenance to that concerning the least quadratic non-residue $n_2(p)$ discussed in Theorem 5.3 and its preamble, and in §5.6. In particular Linnik's work quoted there suggests that any composite n with no small witnesses would be incredibly rare.

Since no-one has ever come close to disproving the Riemann Hypothesis I am going to suggest the second approach, which I outline in the following algorithm.

alg:MillRab **Algorithm 6.1 (Miller Rabin).** *Assume that n is odd.*

1. *Check n for small factors not exceeding $\log n$.*

2. *Check that n is not a prime power.*

3. *Take out the powers of 2 in $n-1$ so that*

$$n-1 = 2^u v$$

with v odd.

4. *For each a with $2 \leq a \leq \min\left\{2(\log n)^2, n-2\right\}$ check the statements*

$$n|a^v - 1,\ n|a^v + 1, \ldots, n|a^{2^{u-1}v} + 1.$$

5. *If a is such that they are all false, stop and declare that n is composite and a is a witness.*

6. *If no witness a is found with $a \leq \min\left\{2(\log n)^2, n-2\right\}$, then declare that n is prime.*

There are a couple of further wrinkles that can be tried in this process. Before doing the divisibility checks in 4, check that $(a,n) = 1$ because if $(a,n) > 1$, then one has a proper divisor of n and not only is n composite but one has found a factor. With regard to the construction of a in the proof of Theorem 6.2, we see that a is a QNR with respect to one of the prime factors of n, and we observed in Section §5.1 that the least QNR modulo a prime is itself a prime. Thus it is no surprise that in the use of the Riemann Hypothesis mentioned above the $a \leq 2(\log n)^2$ which arises is in fact prime. Thus we can restrict our attention to prime values of a.

In this form the test obviously runs in polynomial time.

ex:six1 **Example 6.1.** *Let $n = 133$. Then*

$$n - 1 = 2^2 \times 33$$

and

$$2^{33} \equiv 50 \pmod{133},\ 2^{66} \equiv 106 \pmod{133}$$

so

$$n \nmid 2^{33} - 1,\ n \nmid 2^{33} + 1,\ n \nmid 2^{66} + 1$$

Thus n is composite and 2 is a witness.

To establish primality in a non-trivial case involves quite a lot of calculation and is best left to a computer program. However to illustrate the method here is a trivial example.

ex:six2 **Example 6.2.** *Let $n = 11$. Then $n - 1 = 2 \times 5$ and we have the following*

$$\begin{aligned}
2^5 &= 32 \equiv -1 \pmod{11} \\
3^5 &= 243 \equiv 1 \pmod{11} \\
4^5 &\equiv (2^5)^2 \equiv 1 \pmod{11} \\
5^5 &= 3125 \equiv 1 \pmod{11} \\
6^5 &= (-5)^5 \equiv -1 \pmod{11} \\
7^5 &= (-4)^5 \equiv -1 \pmod{11} \\
8^5 &= (-3)^5 \equiv -1 \pmod{11} \\
9^5 &= (3^5)^2 \equiv 1 \pmod{11}
\end{aligned}$$

There is no witness, so n is prime. Of course we knew that! Even for a number like 211 this would be heavy handed and is one of the reasons for an initial range of trial division. For large n one will only need to consider a relatively small range of a.

6.1.1 Exercises

exs:six1.1 1. Prove that if n is odd and p and q are different prime factors of n, then

$$\sum_{\substack{m=1 \\ (m,n)=1}}^{n} \left(\frac{m}{p}\right)_L = \sum_{\substack{m=1 \\ (m,n)=1}}^{n} \left(\frac{m}{q}\right)_L = \sum_{\substack{m=1 \\ (m,n)=1}}^{n} \left(\frac{m}{pq}\right)_J = 0.$$

2. Write a programme to implement the Miller–Rabin test in its deterministic form in which one assumes the Generalized Riemann Hypothesis, and use it to test the following six numbers. The output from your programme should read, for each number, either "n is composite. a is a witness." where n is the number being tested and a is the value of the witness, or "n is prime". The run time on each of these numbers should not exceed a minute or so.

(a) 3215031751,
(b) 341550071728321,
(c) 1234567891234567919,
(d) 3825123056546413051,
(e) 129600198716501564336903237 1289,
(f) 59545797598759584957498579859585984759457948579595794859456799501.

3. Write a computer program to implement (LJ), the evaluation of the Jacobi symbol, and use it

(i) to find the primes p with $83 \leq p \leq 113$ for which $a = 73$ is a quadratic residue modulo p,

(ii) to find the least quadratic residue $a > 1$ and least positive quadratic non–residue b modulo p of whichever of 370370384407407431 and 370370384407407539 is prime p. You

might like to use your previous implementation of the Miller–Rabin test to find which, if any, of these numbers is prime.

4. Consider the numbers

$$a_1 = 2345678902345678992345678992345456677888990189,$$

$$a_2 = 2345678902345678992345678992345456677888990190,$$

$$m_1 = 24479520371121008474792131183260228434377050031262 89,$$

$$m_2 = 595457975987595849574985798595859847594579485795957948594567995 01.$$

Use (LJ) to evaluate

$$\left(\frac{a_1}{m_1}\right)_J, \quad \left(\frac{a_2}{m_1}\right)_J, \quad \left(\frac{a_1}{m_2}\right)_J, \quad \left(\frac{a_2}{m_2}\right)_J.$$

For those m_j which are prime (Miller-Rabin is useful here) and those a_i for which the Legendre symbol is $+1$ solve (QC)

$$x^2 \equiv a_i \pmod{m_j}.$$

6.2 Probability

We have already used the term "probabilistic" informally in the previous section without saying precisely what we mean.

def:six1 **Definition 6.1.** *Suppose that we have a finite set $\mathcal{A}$ of cardinality M, and a subset $\mathcal{B}$ of cardinality N. In general we will suppose that the elements of $\mathcal{B}$ have some special property that marks them out from those in the complement of $\mathcal{B}$ with respect to $\mathcal{A}$. If we pick an element of $a \in \mathcal{A}$ without fear or favour, then we define the probability that $a \in \mathcal{B}$ as*

$$\frac{N}{M}.$$

It is also possible to define probability for elements of infinite sets, but then we have to be concerned with how we measure the size of the sets, and this involves the much more sophisticated subject of measure theory. Fortunately we have no need of that here.

ex:six3 **Example 6.3.** *Let $\mathcal{A} = \{1, 2, \ldots, M\}$, let $q \in \mathbb{N}$ and $0 \leq r < q$ and let*

$$\mathcal{B}(q, r) = \{a \in \mathcal{A} : a \equiv r \pmod{q}\}.$$

Then

$$N = \operatorname{card} \mathcal{B}(q, r) = 1 + \left\lfloor \frac{M - r}{q} \right\rfloor.$$

Now

$$\frac{M-r}{q} - 1 < \lfloor \frac{M-r}{q} \rfloor \leq \frac{M-r}{q}$$

and so

$$-1 < -\frac{r}{q} < N - \frac{M}{q} \leq 1 - \frac{r}{q} < 1.$$

Therefore

$$-\frac{1}{M} + \frac{1}{q} < \frac{N}{M} < \frac{1}{q} + \frac{1}{M}.$$

Thus if M is large compared with q we can see that the probability that an element of a is in $\mathcal{B}$ is close to

$$\frac{1}{q}$$

Well, that seemed pretty straightforward. But consider the following. Suppose we have a class of with s students. What are the chances that there are two with the same birthday? For simplicity assume there are no leap years. Well in the population at large there are 365^2 pairs of birthdays and of those pairs only 365 will be the same. Thus if you pick a random pair of people you might conclude that only one in 365 pairs have the same birthday so the class will have to be really large, with getting on for at least 365 members.

Well look at it this way, The number of possible configurations of birthdays for s people is 365^s - each person can have any one of 365 possibilities. Let $\mathcal{A}$ be the set of all such configurations. One can think of the elements as being s-tuples $(d_1, d_2, \ldots, d_s)$ with each entry in the s-tuple being a number d_j in the range $\{1, 2, \ldots, 365\}$. Then $M = \operatorname{card} \mathcal{A} = 365^s$

In how many of those s-tuples could all the entries (birthdays) be different? Let $\mathcal{B}$ the corresponding subset of $\mathcal{A}$. Then we are interested in the $N = \operatorname{card} \mathcal{B}$. Well

$$N = 365(365-1)\ldots(365-s+1) \tag{6.6}$$ eq:six7

Think of it this way. The first person's birthday has 365 possibilities, i.e. the number of choices for d_1 is 365. The second person's birthday d_2 then only has 364 choices, and so on. Thus the number of ways in which all the birthdays are different is the number of s-tuples in which the entries are different and this is (6.6). Thus the probability that an arbitrary member of $\mathcal{A}$ is in $\mathcal{B}$ is

$$\rho(s) = \frac{N}{M} = \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\ldots\left(1 - \frac{s-1}{365}\right).$$

Thus the probability that at least two members of the class share a birthday is

$$1 - \rho(s) = 1 - \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\ldots\left(1 - \frac{s-1}{365}\right).$$

s	$\rho(s)$	s	$\rho(s)$
21	.5563...	22	.5243...
23	.4927...	24	.4616...
25	.4313...	26	.4017...
27	.3731...	28	.3455...
29	.3190...	30	.2936...
31	.2695...	32	.2466...
33	.2250...	34	.2046...
35	.1856...	36	.1678...
37	.1512...	38	.1359...
39	.1217...	40	.1087...
41	.0968...	42	.0859...
43	.0760...	44	.0671...
45	.0590...	46	.0517...
47	.0452...	48	.0394...
49	.0342...	50	.0296...

The probability $\rho(s)$ that a class of size s does not have two birthdays the same.

This shows that if the class has 23 members, then it is more likely than not that there will be two people sharing a birthday. This class has 48 members so it is practically certain that two members will have the same birthday. This is the *birthday paradox* and its generalization plays an important rôle in establishing coincidences in computations.

We need to generalize this. Let D be the number of possible values for each entry in the s-tuple - so we are now supposing that our year has D days! Then $M = \operatorname{card} A = D^s$ and $N = \operatorname{card} B$ is

$$N = D(D-1)\dots(D-N+1)$$

so that the probability that there are no coincidences in the entries in an arbitrary s-tuple is

$$\frac{N}{M} = \left(1 - \frac{1}{D}\right)\left(1 - \frac{2}{D}\right)\dots\left(1 - \frac{s-1}{D}\right).$$

Thus if this number is smaller than 0.5 we could conclude that amongst all the s-tuples it is more likely that at least one s-tuple will have two entries the same than that all s-tuples will have all entries different. In a particular case we might ask how large s has to be in terms of D that this probability is smaller than some number σ where $0 < \sigma < 1$, so that

$$\rho(s) = \prod_{k=1}^{s-1}\left(1 - \frac{k}{D}\right) < \sigma.$$

Since it is easier to work with sums than products, we can rewrite this as

$$\log\frac{1}{\rho(s)} = \sum_{k=1}^{s-1}\log\frac{1}{1-\frac{k}{D}} > \log\frac{1}{\sigma}.$$

Of course it makes sense to suppose that s is somewhat smaller than D, and so we can use the expansion for the logarithmic factor to obtain

$$\log \frac{1}{\rho(s)} = \sum_{k=1}^{s-1} \sum_{h=1}^{\infty} \frac{k^h}{hD^h} > \log \frac{1}{\sigma}. \tag{6.7}$$ eq:six8

We can rewrite the double sum over k and h as

$$= \sum_{h=1}^{\infty} \sum_{k=1}^{s-1} \frac{k^h}{hD^h}.$$

When $h = 1$ the sum over k is

$$\frac{s(s-1)}{2D}$$

and when $h \geq 2$ all the terms are positive and the h-th one is at most

$$\frac{(s-1)^{h+1}}{hD^h}.$$

Thus if we suppose that

$$\sum_{k=1}^{s-1} \frac{k}{D} > \log \frac{1}{\sigma}, \tag{6.8}$$ eq:six8a

then by (6.7)

$$\log \frac{1}{\rho(s)} > \log \frac{1}{\sigma} \tag{6.9}$$ eq:six8b

will certainly hold.

Summing the series in (6.8) gives

$$\frac{s(s-1)}{2D} > \log \frac{1}{\sigma}. \tag{6.10}$$ eq:six9

If we suppose also that D is large and s is smaller than $D^{2/3}$, then the contribution from the terms on the left of (6.7) with $h \geq 2$ will be small and we will not lose much by supposing the last inequality. Nevertheless we always have

$$\log \frac{1}{\rho(s)} > \frac{s(s-1)}{2D}$$

Thus we see that, once s gets somewhat larger than $\sqrt{D}$, when we pick an s-tuple at random we are quite likely to find two entries the same. Even for a number as small as $D = 365$ this quite crude approximation shows that $\rho(s) < \frac{1}{2}$ when $s = 23$.

The inequality (6.10) can be rearranged to give

$$\exp\left(-\frac{s(s-1)}{2D^2}\right) < \sigma \tag{6.11}$$ eq:six10

and so if that holds, then we have

$$\rho(s) < \sigma. \tag{6.12}$$ eq:six11

This reveals that the probability is dropping off quadratically in the exponent, and once s gets past $\sqrt{2D}$ drops off incredibly rapidly. Thus even if σ is taken to be quite small one does not have to take s much bigger than $\sqrt{D}$ to achieve the desired result. In other words, if s is large compared with $\sqrt{D}$, then it will be almost certain that there will be coincidences. By the way, some attacks on security systems take advantage of this and we will make use of it later in one of the factoring attacks.

6.2.1 Exercises

1. The Martian year is approximately 668 Martian days. Compute the probability $\rho(s)$ for a class of s Martian students when $21 \leq s \leq 50$. For which size class of Martians is one more likely than not to have two Martians with the same birthday?

For a Mercurian the solar day appears to be longer than the solar year, so sadly on Mercury the human concept of birthday does not make sense.

6.3 Notes

§1. There are excellent discussions of the Miller-Rabin test at `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf` and `https://en.wikipedia.org/wiki/Miller-Rabin_primality_test`. For example the former shows by a more sophisticated argument than the one we present that at least $\frac{3}{4}$ of all reduced residues modulo n are witnesses when n is composite. This is due independently to G. L. Miller, "Riemann's Hypothesis and tests for primality", J. Computer and System Sciences 13(1976), 300–317 and L. Monier, "Evaluation and comparison of two efficient probabilistic primality testing algorithms", Theoretical Computer Science 12(1980), 97–108. See also M. O. Rabin, "Probabilistic algorithm for testing primality", J. Number Theory 12(1980), 128–138.

The advantage of the Miller-Rabin test is simplicity. The disadvantage is that it is either probabilistic or depends for certainty on an unproved hypothesis. There are more sophisticated tests, such as the Elliptic curve primality test which gives certainty but for which the worst case runtime is not known or the Baillie-PSW primality test which is probabilistic. There are some claims that the latter is deterministic but as far as I am aware there is no published worst case runtime. For an overview of this subject see `https://en.wikipedia.org/wiki/Primality_test`. It seems clear from the discussion there that the only test which is deterministic and runs in reasonable time for very large n is the Miller-Rabin test under the Riemann Hypothesis for Jacobi (and Legendre) symbols. I have much greater confidence that this form of the Riemann hypothesis holds than that there are no counterexamples to the other tests. I would add that even if the hypothesis turned out to be false, Linnik's theorems suggest that any counterexamples to Miller-Rabin would be incredibly rare.

H. L. Montgomery, "Topics in Multiplicative Number Theory", Lecture Notes in Mathematics, Springer, vol. 227, 1971", pages 123-125, shows for a more general class of functions χ than the χ in (6.3) that on the Riemann Hypothesis for each χ we have

$$\sum_{\substack{m \le N \\ m \text{ prime}}} (1 - m/M)\chi(m) \log m < C_1 N^{1/2} \log r$$

where r is the modulus of χ, so $2 = p$ or q or pq in our cases. He also observes that if $\chi(m) = 1$ for all $m \le N$, then the sum is $> C_2 N$. The C_1 and C_2 are positive constants, so it follows that there is a prime $m < C(\log r)^2$ with $\chi(m) \ne 1$ where C is another positive constant. There is also an account of this on page 179 of H. L. Montgomery, "Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis", American Mathematical Society, 1994, p. 176. ISBN 0-8218-0737-4. Explicit values for the constants are given by E. Bach, "Explicit bounds for primality testing and related problems", Mathematics of Computation, 55(191)(1990), 355–380.

It seems quite likely that (6.4) holds for N as small as $C(\log N) \log\log N$.

§2 It is believed that the birthday paradox was first discovered by H. Davenport in 1927 and first published by R. Von Mises, "Über Aufteilungs- und Besetzungswahrscheinlichkeiten", Revue de la faculté des sciences de l'Université d'Istanbul 4(1939), 145-163, reprinted in P. Frank, S. Goldstein, M. Kac, W. Prager, G. Szegö, G. Birkhoff, eds. Selected Papers of Richard von Mises. Vol. 2. Providence, Rhode Island: Amer. Math. Soc. pp. (1964), 313–334.

Chapter 7

Pollard's Methods

7.1 Pollard rho

John Pollard, in the 1970s, created a number of different techniques for factoring large integers. The Pollard rho is named for a way of representing the iterative process which looks like the Greek lower case rho, ρ. Suppose you start from some object P_0, and successively compute $P_1, P_2, P_3, \ldots$ and that sooner or later you find some pair $j < k$ so that $P_j = P_k$. Then $P_{j+1} = P_{k+1}$ and so on. That is the sequence just repeats itself with period $k - j$. We can represent this as a ρ, where P_0 is at the base of the tail, and P_j is where the tail meets the loop.

How this works to factorize n in the case of Pollard rho is that one chooses some polynomial, normally irreducible over $\mathbb{Q}$, like

$$f(x) = x^2 + 1,$$

pick an x_0 at random and successively compute

$$\begin{aligned} x_1 &= f(x_0) \pmod{n}, \\ x_2 &= f(x_1) \pmod{n}, \\ x_3 &= f(x_2) \pmod{n}, \\ &\vdots \quad \vdots \qquad \vdots \end{aligned}$$

Since there are only n residue classes, sooner or later there has to be a repetition. We then check

$$GCD(x_i - x_j, n)$$

for each pair i, j and hope to find a non-trivial factor of n. There is no guarantee of finding one quickly, but sometimes one is found. The usual procedure is to stop after a certain amount of time and try a different polynomial f.

What is the theory? Suppose d is a proper divisor of n. For every i let $y_i \equiv x_i \pmod{d}$. Then $y_j \equiv x_j \equiv f(x_{j-1}) \equiv f(y_{j-1}) \pmod{d}$. Thus sooner or later $y_j = y_k$

for some j, k with $j \neq k$. Then $x_j \equiv y_j \equiv y_k \equiv x_k \pmod{d}$. Probably, and hopefully, $x_j \neq x_k$ so $d|GCD(x_j - x_k, n)$ and the GCD will differ from n.

How far should we expect to go before finding a solution? Given a prime $p < \sqrt{n}$ with $p|n$ we are seeking different numbers in the same residue class modulo p. If we have $x_1, x_2, \ldots, x_s$ created at random, this is akin to the birthday paradox with a year that has p days and a class size of s. Thus we can expect that with s not much bigger than $\sqrt{p} < n^{1/4}$ we will find a solution.

ex:seven1 **Example 7.1.** *Let* $n = 1133$ *and* $f(x) = x^2 + 1$. *Of course* $11|1133$.

Take $x_0 = 2$. *Then* $x_1 = 5$, $x_2 = 26$, $x_3 = 677$, $x_4 = 598$. *Now*

$$\begin{aligned}(x_1 - x_0, n) &= (3, 1133) = 1,\\ (x_2 - x_0, n) &= (24, 1133) = 1,\\ (x_3 - x_0, n) &= (675, 1133) = 1,\\ (x_4 - x_0, n) &= (596, 1133) = 1,\\ (x_2 - x_1, n) &= (21, 1133) = 1,\\ (x_3 - x_1, n) &= (672, 1133) = 1,\\ (x_4 - x_1, n) &= (593, 1133) = 1,\\ (x_3 - x_2, n) &= (651, 1133) = 1,\\ (x_4 - x_2, n) &= (572, 1133) = 11.\end{aligned}$$

Not very efficient, but it illustrates the idea.

The method can be speeded up as follows by an idea due to Floyd. We want to know when we have reached the loop. Think of this as a race with two runners. If one is running twice as fast as the other, the point at which the faster one comes round the loop to overtake the slower one is the place where the tail meets the loop. With this in mind, let $z_0 = x_0$ and then at the j-th step compute x_j as above and

$$z_{j+1} \equiv f(f(z_j)) \pmod{n}.$$

Then

$$z_j = x_{2j},$$

so we are computing x_j and x_{2j} simultaneously. If x_j and x_k with $j < k$ are the smallest pair with $x_j \equiv x_k \pmod{d}$, let $l = k - j$. Then

$$x_i \equiv x_{i+rl} \pmod{d}$$

for every $i \geq j$ and every $r \geq 0$.

Take $i = l\lceil j/l \rceil$ so that $i \geq j$ and $r = \lceil j/l \rceil$. Then $rl = i$ and so

$$x_i \equiv x_{2i} \equiv z_i \pmod{d}.$$

Thus we only need check

$$GCD(z_i - x_i, n) = GCD$$

and this really speeds up the computations. In the previous example.

ex:seven2 **Example 7.2.** *Let* $n = 1133$*,* $f(x) = x^2 + 1$ *and* $x_0 = 2$*.*
Then we compute

$$x_1 = 5, z_1 = 26,\ (z_1 - x_1, n) = (21, 1133) = 1,$$
$$x_2 = 26, z_2 = 598,\ (z_2 - x_2, n) = (572, 1133) = 11.$$

That is more like it!
A less obvious example

ex:seven2a **Example 7.3.** *Let* $n = 713$*,* $f(x) = x^2 + 1$ *and* $x_0 = 2$*.*
Then we compute

$$x_1 = 5, z_1 = 26,\ (z_1 - x_1, n) = (21, 713) = 1,$$
$$x_2 = 26, z_2 = 584\,(z_2 - x_2, n) = (558, 713) = 31.$$

There are a number of more sophisticated variants of this which are designed to speed the algorithm up. Generally there is no rigorous proof but it is believed that the run time is normally proportional to $\sqrt{p}$ where p is the smallest prime factor of n and so in the worst case, for a composite number the run time is proportional to $n^{1/4}$.

sec:seven1.1

7.1.1 Exercises

1. Write a programme or script to implement Pollard's "ρ" (in Pari the exponentiation, gcd and mod algorithms are already programmed in, although for large exponents it is necessary to use the "binary expansion / successive squaring" method) and use it to factorise $1231331, 9912409831, 950161333249$.

7.2 Pollard p-1

Here we take a fairly large number K and hope that n has a prime factor p such that none of the prime factors of $p - 1$ exceed K. To explain the method we will assume a little more, namely that

$$p - 1 | K!$$

Obviously we do not want to compute and store $K!$, which will be huge. Thus for some a coprime with n we define $x_0 = a$ and successively compute

$$x_k \equiv x_{k-1}^k \pmod{n} \text{ and } GCD(x_k - 1, n) \quad (k = 1, 2, 3, \ldots, K),$$

stopping if the GCD reveals a proper factor of n. Since n is large we can expect that $x_k \not\equiv 1 \pmod{n}$, but if $p|n$ and $p - 1|k!$, so that $k! = m(p-1)$ for some m, then we have

$$x_k \equiv a^{k!} = (a^{p-1})^m \equiv 1 \pmod{p}.$$

ex:seven3 **Example 7.4.** *Consider our old friend 1133. Let $a = 2$. Thus*

$$x_0 = 2, x_1 = 2^2 = 4, x_2 = 4^3 = 64,$$

$$x_3 = 64^4 = 16777216 \equiv 719 \pmod{1133}, (718, 1133) = 1,$$

$$x_4 = 719^5 = 192,151,797,699,599 \equiv 1101 \pmod{1133}, (1100, 1133) = 11.$$

Now look at the less obvious example we considered above

ex:seven4 **Example 7.5.** *Let $n = 713$, and $a = 2$. Thus*

$$x_0 = 2, x_1 = 2^2 = 4, x_2 = 4^3 = 64,$$

$$x_3 = 64^4 = 16777216 \equiv 326 \pmod{713}, (325, 713) = 1,$$

$$x_4 = 326^5 = 3,682,035,745,376 \equiv 311 \pmod{713}, (310, 713) = 31.$$

In practice for large numbers the elliptic curve method is faster and the Pollard $p-1$ has largely disappeared. It uses the group structure of the powers of a modulo n. The elliptic curve method is based on a similar basic idea but takes advantage of the richer underlying group structure of elliptic curves.

7.2.1 Exercises

sec:seven2.1

1. Write a programme or script to implement Pollard's "$p-1$" (in Pari the exponentiation, gcd and mod algorithms are already programmed in, although for large exponents it is necessary to use the "binary expansion / successive squaring" method) and use it to factorise 1231331 and 950161333249.

Chapter 8

The Quadratic Sieve

ch:eight

8.1 Prolegomenon

sec:eight1

There have been many factorization algorithms developed with the intent of finding t, x, y so that

$$tn = x^2 - y^2, \tag{8.1}$$

eq:eight1

going back to Fermat in the case $t = 1$ and Legendre for general t. One of the lines of attack was through the use of continued fractions. It seems to have been periodically rediscovered, for example by Kraitchik and, most notably, by Lehmer and Powers in 1931 and then developed further by Morrison and Brillhart in 1975 who showed that the advent of modern computers made it a practical method. The idea is to consider the continued fraction of $\sqrt{tn}$

$$\sqrt{tn} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

This expansion is actually periodic, and truncating the expansion after k terms produces an approximation

$$\frac{A_k}{B_k} \tag{8.2}$$

eq:eight2

to $\sqrt{tn}$. In particular

$$A_k^2 - tnB_k^2 = (-1)^{k-1}R_k \tag{8.3}$$

eq:eight3

where R_k is relatively small. By the way the approximation (8.2) turns out to be exactly the approximation that would arise from an application of Dirichlet's theorem, Theorem 2.2. Thus we have a solution to

$$A_k^2 \equiv (-1)^{k-1}R_k \pmod{n}.$$

Having computed $(-1)^{k-1}R_k$ for $k = 0, \ldots K$ one looks for a subset $\mathcal{K}$ of the k such that the product

$$\prod_{k \in \mathcal{K}} (-1)^{k-1}R_k$$

is a perfect square. Then for

$$R \equiv \prod_{k \in \mathcal{K}} (-1)^{k-1} R_k \pmod{n},\ A \equiv \prod_{k \in \mathcal{K}} A_k \pmod{n}$$

one has

$$A^2 \equiv R^2 \pmod{n}$$

and hopefully $GCD(A \pm R, n)$ provides a proper factor of n.

Things then developed very rapidly culminating in 1981 with what we now know as the Quadratic Sieve (QS).

The expression in (8.3) on the left can be thought of as an indefinite binary quadratic form

$$x^2 - tny^2.$$

Gauss had already studied such forms and had introduced the idea of "composition" of forms. This lead Shanks to bring such ideas to the party, and gave arise to an alternative version of the method usually known as SQUFOF (SQUareFOrmsFactorization). This has a worse case runtime proportional to $n^{1/4}$, so does not compete in that regard to the other methods described here. However SQUFOF is sufficiently simple that it can be implemented on a pocket calculator and the instructor of this course has a version on his mobile phone.

8.2 The Quadratic Sieve

sec:eight2

Recall that in Lehman's method the aim is to find x, t so that

$$x^2 - 4tn$$

is a perfect square. In the discussion above of the continued fraction approach we saw that an alternative way to achieve this is to find $x_1, \ldots, x_r$ and $y_1, \ldots, y_r$ such that

$$y_i \equiv x_i^2 \pmod{n}$$

and

$$(x_1 \ldots x_r)^2 \equiv y_1 \ldots y_r = z^2 \pmod{n}.$$

However we want something better than trial and error.

Idea. Initially we consider

$$x^2 - n$$

although eventually we may have to consider other polynomials. The data we garner from this will ultimately enable us to find t, x such that $x^2 - tn$ is a perfect square. Suppose that each of the y_j has only small prime factors, say we have $p \leq B$ for every $p | y_j$. For

example take $B = 7$ and suppose we found $y_1 = 6, y_2 = 15, y_3 = 21, y_4 = 35$. Then we would have

$$y_1 = 2^1 3^1 5^0 7^0, y_2 = 2^0 3^1 5^1 7^0, y_3 = 2^0 3^1 5^0 7^1, y_4 = 2^0 3^0 5^1 7^1$$

so we can associate with these the four vectors

$$\mathbf{v}_1 = \langle 1, 1, 0, 0\rangle, \mathbf{v}_2 = \langle 0, 1, 1, 0\rangle, \mathbf{v}_3 = \langle 0, 1, 0, 1\rangle, \mathbf{v}_4 = \langle 0, 0, 1, 1\rangle.$$

Then we want to find integers $e_j = 0$ or 1 so that

$$e_1\mathbf{v}_1 + e_2\mathbf{v}_2 + e_3\mathbf{v}_3 + e_4\mathbf{v}_4 \equiv \mathbf{0} \pmod 2$$

where $\mathbf{0} = \langle 0, 0, 0, 0\rangle$. Thus $e_1 = 0$, $e_2 = e_3 = e_4 = 1$ will do and

$$y_1^0 y_2^1 y_3^1 y_4^1 = 15.21.35 = (3.5.7)^2 = (105)^2.$$

Thus we can find perfect squares by vector addition. In other words solving linear equations. In practice this in turn means Gaussian elimination.

def:eight1 **Definition 8.1.** *Given a positive real number B we say that an integer z is B-factorable when every prime factor p of z satisfies $p \le B$. To emphasise the fact that in our situation only certain primes (but also -1) may occur we will also use the term $\mathcal{P}$-factorable where $\mathcal{P}$ is a set of primes, probably augmented by -1.*

Note that the term B-smooth is commonly used instead. The word "smooth" has many better uses in mathematics.

alg:QS **Algorithm 8.1 (QS.).** *We are given an odd number n which we know to be composite and not a perfect power. The objective is to find a non–trivial factor of n by first finding x and y so that $x^2 \equiv y^2 \pmod n$ and then checking $\gcd(x \pm y, n)$..*

1. Initialization.

1.1. *Pick a number B as the upper bound for the primes in the factor base $\mathcal{P}$. Theory says take $B = \lceil L(n)^{1/2} \rceil$ where $L(n) = \exp(\sqrt{\log n \log\log n})$, but in practice a B somewhat smaller works well. Also, adding extra primes suggested by the sieving process can be useful and if one uses the wrinkle in 5.3 below, then the prime p is adjoined to the factor base $\mathcal{P}$.*

1.2. *Set $p_0 = -1$, $p_1 = 2$ and find the odd primes $p_2 < p_3 < \ldots < p_K \le B$ such that $\left(\frac{n}{p_k}\right)_L = 1$. Then $\mathcal{P} = \{p_0, p_1, \ldots, p_K\}$ and $\operatorname{card}\mathcal{P} = K + 1$ The Algorithm 5.1* **LJ** *is useful here.*

1.3. *For $k = 2, \ldots, K$ find the solutions $\pm t_{p_k}$ to $x^2 \equiv n \pmod{p_k}$ by using Algorithms 5.2 and 5.3,* **QC357/8, QC1/8**.

2. Sieving.

2.1. *Let $N = \lceil \sqrt{n} \rceil$. Sieve the sequence $x^2 - n$ with $x = N + j$, $j = 0, \pm 1, \pm 2, \ldots$ until one has obtained a list of at least $J \geq K + 2$ B-factorable $x^2 - n$ and their factorizations ($K + 2$ is somewhat arbitrary and can be increased if necessary but in the first example below is $K + 1$ instead). This could be done by using a matrix, with initially B^2 columns (B^2 is somewhat arbitrary and can be increased if necessary) so that each column is a $K + 3$ dimensional vector in which the first entry is x, the second is $x^2 - n$, and the $k + 3$–rd entry will be the exponent of p_k in $x^2 - n$.*

2.2. *For each prime p_k in the factor base divide out all the prime factors p_k in each entry $x^2 - n$ with $x \equiv \pm t_{p_k} \pmod{p_k}$, recording the exponent in the $k + 3$-rd entry in the associated j-th vector. Once the primes start to grow this speeds things up significantly.*

2.3. *If the second entry in a column vector has reduced to 1, then $x^2 - n$ is B–factorable. If it has not completely factored then one can discard that column, or at least put it aside in case one needs to extend the factor base later. Theory tells us that we will need at least $K + 1$, and generally somewhat more, say J, completely factored, which is the reason for taking so many columns in the first place.*

3. Linear Algebra.

3.1. *Form a $(K + 1) \times J$ matrix $\mathcal{M}$ with the rows being formed by the 3–rd through $K+3$–rd entries of the row vectors arising in 2.2, but with the entries reduced modulo 2. It is convenient to label columns as $j = 1$ through J and the corresponding x as x_1 through x_J.*

3.2. *Use linear algebra (Gaussian elimination, for example) to solve*

$$\mathcal{M}\mathbf{e} = \mathbf{0} \pmod{2}$$

where $\mathbf{e}$ is a J dimensional vector of 0s and 1s (not all 0!). It is likely that one will need more than one solution before finding a factorization of n. Gaussian elimination or standard linear algebra packages should give a basis for the space of all solutions.

4. Factorization.

4.1. *Compute $x = x_1^{e_1} x_2^{e_2} \ldots x_{K+2}^{e_J}$ modulo n and*

$$y = \sqrt{(x_1^2 - n)^{e_1} (x_2^2 - n)^{e_2} \ldots (x_J^2 - n)^{e_J}}$$

modulo n. The value of x can be computed by using the first entries in the column vectors in the original matrix and the square root in the definition of y should be computed using the factorizations in the body of that matrix. Note

that all multiplications should be performed modulo n so nothing bigger than n^2 will occur.

4.2. *Compute $l = \gcd(x - y, n)$, $m = \gcd(x + y, n)$.*

4.3. *Return l, m.* **4.4.** *If necessary repeat for all solutions* **e** *until a non-trivial factor found.*

5. Aftermath.

5.1. *If no proper factor of n found, try one or more of the following.*

5.2. *Extend the sieving in 2.1 to obtain more* **e** *and pairs x, y. As a matter of policy the original sieving probably should be conducted so as to obtain K' pairs with K' somewhat more than $K + 2$.*

5.3. *Use another polynomial in place of $x^2 - n$, or rather, be a bit more cunning about the choice of the x in 2.1. Choose a large prime p for which $b^2 - n \equiv 0 \pmod{p}$ is soluble, and compute b. Then $(px+b)^2 - n \equiv 0 \pmod{p}$ and x can be chosen so that $f(x) = ((px + b)^2 - n)/p$ is comparatively small since p is large, so the sieving proceeds relatively speedily, there is a better chance of a complete factorization of $f(x)$, and we only have to augment the factor base with the prime p.*

The most time consuming part of this algorithm is the sieving. Note that just restricting the x to $x \equiv \pm t_k$ already speeds it up considerably but this is still usually the slowest part. The linear algebra can also be speeded up by various techniques, especially those developed for dealing with sparse matrices.

Although the numbers in the following example are much smaller than would occur in a practice the example does illustrate the complexity of the basic quadratic sieve.

ex:eight1 **Example 8.1.** *Let $n = 9487$ and take the sieving limit $B = 30$. We first need to check which primes $p \leq 30$ will occur in the method. Thus for each odd prime $p \leq 30$ we need to ascertain whether n is a QR or a QNR modulo p.*

$$\left(\frac{9487}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1, \left(\frac{9487}{13}\right)_L = \left(\frac{10}{13}\right)_L = \left(\frac{36}{13}\right)_L = 1,$$
$$\left(\frac{9487}{5}\right)_L = \left(\frac{2}{5}\right)_L = -1, \left(\frac{9487}{17}\right)_L = \left(\frac{1}{17}\right) = 1,$$
$$\left(\frac{9487}{7}\right)_L = \left(\frac{2}{7}\right)_L = 1, \left(\frac{9487}{19}\right)_L = \left(\frac{6}{19}\right)_L = \left(\frac{25}{19}\right)_L = 1,$$
$$\left(\frac{9487}{11}\right)_L = \left(\frac{5}{11}\right)_L = 1, \left(\frac{9487}{23}\right)_L = \left(\frac{11}{23}\right)_L = -\left(\frac{23}{11}\right)_L = -1,$$
$$\left(\frac{9487}{29}\right)_L = \left(\frac{4}{29}\right)_L = 1.$$

Thus we will take our set of primes to be $\mathcal{P} = \{-1, 2, 3, 7, 11, 13, 17, 19, 29\}$. *Then we can compute*

$$t_3 = \pm 1, t_7 = \pm 3, t_{11} = \pm 4, t_{13} = \pm 5, t_{17} = \pm 1, t_{19} = \pm 5, t_{29} = \pm 2.$$

Now for a range of values of x near $\sqrt{n} \approx 97$ we factorise $f(x) = x^2 - n$. At this stage we throw away the x which do not completely factor in our factor base.

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
x	81	84	85	89	95	97	98	100	101	103
$f(x)$	-2926	-2431	-2262	-1566	-462	-78	117	513	714	1122
-1	2926,1	2431,1	2262,1	1566,1	462,1	78,1	117,0	513,0	714,0	1122,0
2	1463,1	2431,0	1131,1	783,1	231,1	39,1	117,0	513,0	357,1	561,1
3	1463,0	2431,0	377,1	29,3	77,1	13,1	13,2	19,3	119,1	187,1
7	209,1	2431,0	377,0	29,0	11,1	13,0	13,0	19,0	17,1	187,0
11	19,1	221,1	377,0	29,0	1,1	13,0	13,0	19,0	17,1	17,1
13	19,0	17,1	29,1	29,0	1,0	1,1	1,1	19,0	17,0	17,0
17	19,0	1,1	29,0	29,0	1,0	1,0	1,0	19,0	1,1	1,1
19	1,1	1,0	29,0	29,0	1,0	1,0	1,0	1,1	1,0	1,0
29	1,0	1,0	1,1	1,1	1,0	1,0	1,0	1,0	1,0	1,0

In the table above, in the column below each prime I have included the exponent of the prime which occurs in the factorisation and the residual factor after that prime has been factored out. It might also be handy to include a column beween the first and second ones which contains the values of t_{p_j}.

I have included one such value, $x = 82$, below, so that you can see what happens. If n is proving awkward to factorise, one might go back and check to see if there are primes outside the factor base which occur in multiple places and then add them to the factor base. For example, $f(92)$ and $f(94)$ would completely factorise if we included the prime 31 in the factor base.

x	82	92	94
$f(x)$	-2763	-1023	-651
-1	2763,1	2763,0	651,1
2	2763,0	1023,1	651,0
3	307,2	341,1	217,1
7	307,0	341,0	31,1
11	307,0	31,0	31,0
13	307,0	31,0	31,0
17	307,0	31,0	31,0
19	307,0	31,0	31,0
29	307,0	31,0	31,0

Let $\mathbf{v}(x)$ denote the vector of exponents in the factorization of $f(x)$, so that

$$\begin{aligned}\mathbf{v}(85) &= \langle 1,1,1,0,0,1,0,0,1\rangle,\\ \mathbf{v}(89) &= \langle 1,1,3,0,0,0,0,0,1\rangle,\\ \mathbf{v}(98) &= \langle 0,0,2,0,0,1,0,0,0\rangle,\end{aligned}$$

Then

$$\mathbf{v}(85)+\mathbf{v}(89)+\mathbf{v}(98) = \langle 2,2,6,0,0,2,0,0,2\rangle.$$

and the entries in this are all even. Thus

$$\begin{aligned}85^2\times 89^2\times 98^2 &\equiv (85^2-n)(89^2-n)(98^2-n) \pmod{9487}\\ 741370^2 &\equiv (-1\times 2\times 3^3\times 13\times 29)^2 = 20358^2 \pmod{9487}.\end{aligned}$$

Unfortunately

$$\begin{aligned}(741370+20358, 9487) &= 1,\\ (741370-20358, 9487) &= 9487.\end{aligned}$$

We also have

$$\mathbf{v}(81)+\mathbf{v}(95)+\mathbf{v}(100) = \langle 2,2,4,2,2,0,0,2,0\rangle,$$

so that

$$81^2\times 95^2\times 100^2 \equiv (-1\times 2\times 3^2\times 7\times 11\times 19)^2 \pmod{9487}$$

which gives

$$769500^2 \equiv 26334^2 \pmod{9487}$$

and

$$\begin{aligned}(769500+26334, 9487) &= 179,\\ (769500-26334, 9487) &= 53.\end{aligned}$$

There is a lot to take away from this.

1. We need to use the theory of quadratic residues, via the Legendre symbol and quadratic reciprocity to see which primes to include in the factor base.

2. We then need to sieve out the x, i.e remove those x for which $f(x)$ does not completely factor in the factor base, and then to store the vector of exponents for each x which survives. This can take a lot of memory.

3. Whilst not apparent in the simple example above, we will need to work hard to find linear combinations of the vectors of exponents in which all the entries are even. This will involve some form of Gaussian elimination. The complexity is somewhat reduced by the fact that we only need to do this modulo 2, but it will still also require quite a lot of memory.

Going back to the table

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
x	81	84	85	89	95	97	98	100	101	103
$f(x)$	-2926	-2431	-2262	-1566	-462	-78	117	513	714	1122
-1	2926,1	2431,1	2262,1	1566,1	462,1	78,1	117,0	513,0	714,0	1122,0
2	1463,1	2431,0	1131,1	783,1	231,1	39,1	117,0	513,0	357,1	561,1
3	1463,0	2431,0	377,1	29,3	77,1	13,1	13,2	19,3	119,1	187,1
7	209,1	2431,0	377,0	29,0	11,1	13,0	13,0	19,0	17,1	187,0
11	19,1	221,1	377,0	29,0	1,1	13,0	13,0	19,0	17,1	17,1
13	19,0	17,1	29,1	29,0	1,0	1,1	1,1	19,0	17,0	17,0
17	19,0	1,1	29,0	29,0	1,0	1,0	1,0	19,0	1,1	1,1
19	1,1	1,0	29,0	29,0	1,0	1,0	1,0	1,1	1,0	1,0
29	1,0	1,0	1,1	1,1	1,0	1,0	1,0	1,0	1,0	1,0

we can extract the exponents of each prime thus

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 3 & 1 & 1 & 2 & 3 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then we wish to find solutions to

$$\mathcal{M}\mathbf{e} \equiv \mathbf{0} \pmod 2.$$

other than $\mathbf{0}$. In other words we want the exponents in the prime factorisation of

$$f(x_1)^{e_1} \dots f(x_K)^{e_K}$$

to be even in a non-trivial way. The standard way of doing this is through Gaussian elimination, and it suffices to perform it modulo 2. Below I have listed the successive row operations, beginning with using the first row to eliminate the first entries in the other rows, and then using successive rows to eliminate the entries in the column corresponding to their leading entry.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 3 & 1 & 1 & 2 & 3 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1&1&1&1&1&1&0&0&0&0\\ 0&1&0&0&0&0&0&0&1&1\\ 0&0&1&1&1&1&0&1&1&1\\ 0&0&1&1&0&1&0&0&0&1\\ 0&0&1&1&0&1&0&0&1&1\\ 0&0&1&0&0&1&1&0&1&1\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&1&1&1&1&0&1&1&1\\ 0&0&1&1&0&0&0&0&0&0 \end{pmatrix}, \quad \begin{pmatrix} 1&1&1&1&1&1&0&0&0&0\\ 0&1&0&0&0&0&0&0&1&1\\ 0&0&1&1&1&1&0&1&1&1\\ 0&0&0&0&1&0&0&1&1&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&1&1&0&1&1&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&1&0&1&1&1 \end{pmatrix}$$

$$\begin{pmatrix} 1&1&1&1&1&1&0&0&0&0\\ 0&1&0&0&0&0&0&0&1&1\\ 0&0&1&1&1&1&0&1&1&1\\ 0&0&0&0&1&0&0&1&1&0\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&1&1&0&1&1&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0&0&1 \end{pmatrix}.$$

It is then arranged into echelon form and the leading entries used successively to remove any entries above

$$\begin{pmatrix} 1&1&1&1&1&1&0&0&0&0\\ 0&1&0&0&0&0&0&0&1&1\\ 0&0&1&1&1&1&0&1&1&1\\ 0&0&0&1&1&0&1&1&0&0\\ 0&0&0&0&1&0&0&1&1&0\\ 0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix}, \quad \begin{pmatrix} 1&1&1&1&1&1&0&0&0&0\\ 0&1&0&0&0&0&0&0&0&1\\ 0&0&1&1&1&1&0&1&0&1\\ 0&0&0&1&1&0&1&1&0&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix}$$

$$\begin{pmatrix} 1&1&1&1&1&0&0&0&0&1\\ 0&1&0&0&0&0&0&0&0&1\\ 0&0&1&1&1&0&0&1&0&0\\ 0&0&0&1&1&0&1&1&0&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix}, \quad \begin{pmatrix} 1&1&1&1&0&0&0&1&0&1\\ 0&1&0&0&0&0&0&0&0&1\\ 0&0&1&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&1&0&0&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix}$$

$$\begin{pmatrix} 1&1&1&0&0&0&1&1&0&1\\ 0&1&0&0&0&0&0&0&0&1\\ 0&0&1&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&1&0&0&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix}, \begin{pmatrix} 1&1&0&0&0&0&0&1&0&1\\ 0&1&0&0&0&0&0&0&0&1\\ 0&0&1&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&1&0&0&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix}$$

$$\begin{pmatrix} 1&0&0&0&0&0&0&1&0&0\\ 0&1&0&0&0&0&0&0&0&1\\ 0&0&1&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&1&0&0&0\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0 \end{pmatrix}$$

Thus we find that

$$\begin{aligned} e_1 + e_8 &\equiv 0 \pmod 2,\\ e_2 + e_{10} &\equiv 0 \pmod 2,\\ e_3 + e_7 &\equiv 0 \pmod 2,\\ e_4 + e_7 &\equiv 0 \pmod 2,\\ e_5 + e_8 &\equiv 0 \pmod 2,\\ e_6 + e_{10} &\equiv 0 \pmod 2,\\ e_9 &\equiv 0 \pmod 2. \end{aligned}$$

Thus taking e_7, e_8 and e_{10} as the independent variables we see that

$$\big(f(x_3)f(x_4)f(x_7)\big)^{e_7}\big(f(x_1)f(x_5)f(x_8)\big)^{e_8}\big(f(x_2)f(x_6)f(x_{10})\big)^{e_{10}}$$

is always a perfect square. The choices $e_7 = 1, e_8 = e_{10} = 0$ and $e_8 = 1, e_7 = e_{10} = 0$ correspond to the solutions used above. The solution $e_{10} = 1, e_7 = e_8 = 0$ does not give a factorization. The reader is welcome to explore other choices.

Here is another example with a somewhat larger n.

ex:eight3 **Example 8.2.** *Let $n = 5479879$ and take the sieving limit $B = 50$. We first need to check which primes $p \le 50$ will occur in the method. Thus for each odd prime $p \le 50$ we need to ascertain whether n is a QR or a QNR modulo p. Running the algorithm* **LJ** *we obtain a factor base*

$$\mathcal{P} = \{-1, 2, 3, 5, 11, 31, 47\}.$$

We have $\sqrt{n} \approx 2340$, but for larger numbers such as n it is harder to obtain complete factorisations of $f(x) = x^2 - n$. Either the range for x has to be increased, or alternatively extend the factor base $\mathcal{P}$.

	x_1	x_2	x_3	x_4	x_5	x_6
x	2198	2225	2252	2373	2383	2477
$f(x)$	−648675	−529254	−408375	151250	198810	655650
−1	1	1	1	0	0	0
2	0	1	0	1	1	1
3	3	7	3	0	2	2
5	2	0	3	4	1	2
11	0	2	2	2	0	0
31	2	0	0	0	0	1
47	0	0	0	0	2	1

Now we extract the parity of the exponents for each prime and form the matrix

$$\mathcal{M} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We now apply Gaussian elimination and obtain

$$\mathcal{M} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus we find that

$$\begin{aligned} e_1 + e_4 &\equiv 0 \pmod 2, \\ e_2 + e_4 + e_5 &\equiv 0 \pmod 2, \\ e_3 + e_5 &\equiv 0 \pmod 2, \\ e_6 &\equiv 0 \pmod 2, \end{aligned}$$

Thus taking e_4 and e_5 as the independent variables we see that

$$\begin{aligned} e_1 &\equiv e_4 \pmod 2, \\ e_2 &\equiv e_4 + e_5 \pmod 2, \\ e_3 &\equiv e_5 \pmod 2, \\ e_6 &\equiv 0 \pmod 2, \end{aligned}$$

and so each of

$$\begin{aligned} &f(x_1)f(x_2)f(x_4), \\ &f(x_2)f(x_3)f(x_5), \end{aligned}$$

is a perfect square. We have

$$x_1 \times x_2 \times x_4 = 2198 \times 2225 \times 2373 = 11605275150$$

and

$$f(x_1)f(x_2)f(x_4) = (-1)^2 \times 2^2 \times 3^{10} \times 5^6 \times 11^4 \times 31^2 = (2 \times 3^5 \times 5^3 \times 11^2 \times 31)^2 = 227873250^2$$

Now

$$\begin{aligned} 11605275150 - 227873250 &= 11377401900, \\ 1105275150 + 227873250 &= 11833148400, \end{aligned}$$

$$(11377401900, n) = (11377401900, 5479879) = 5431$$

and

$$(11833148400, 5479879) = 1009.$$

We can also check to see what happens with the second relationship. We have

$$x_2 \times x_3 \times x_5 = 2225 \times 2252 \times 2383 = 11940498100$$

and

$$f(x_2)f(x_3)f(x_5) = (-1)^2 \times 2^2 \times 3^{12} \times 5^4 \times 11^4 \times 47^2 = (2 \times 3^6 \times 5^2 \times 11^2 \times 47)^2 = 207291150^2$$

Then

$$\begin{aligned} 11940498100 - 207291150 &= 11733206950, \\ 11940498100 + 207291150 &= 12147789250, \end{aligned}$$

$$(11733206950, 5479879) = 1009$$

and

$$(12147789250, 5479879) = 5431.$$

8.3 Note on Gaussian Elimination

eight3

As part of the quadratic sieve we need to solve systems of linear congruences of the kind

$$\begin{aligned} a_{11}e_1 + a_{12}e_2 + \cdots + a_{1m}e_m &\equiv 0 \pmod 2, \\ a_{21}e_1 + a_{22}e_2 + \cdots + a_{2m}e_m &\equiv 0 \pmod 2, \\ \vdots \qquad\qquad & \qquad \vdots \\ a_{l1}e_1 + a_{l2}e_2 + \cdots + a_{lm}e_m &\equiv 0 \pmod 2. \end{aligned} \tag{8.4}$$

eq:eight10

In our situation the a_{jk} can be taken to be 1 or 0 which simplifies computation. When n, the number to be factored, is large the matrices will be sparse, i.e. the majority of the entries will be 0 and then there are more efficient methods than Gaussian elimination. However, for the purposes of the exposition in this chapter Gaussian elimination is adequate, and has the merit of being straightforward.

We can write this more succinctly in matrix notation as

$$\mathcal{A}\mathbf{e} = \mathbf{0}$$

where

$$\mathcal{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{pmatrix}$$

and

$$\mathbf{e} = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}$$

and

$$\mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

The first observation that can be made is that it is immaterial as to the order in which we write the equations so at any state we can interchange them if it is convenient to do so. Clearly if we have a row of zeros, then we can remove that row and make the matrix smaller. Likewise if any column is all zeros we can remove that column and give any value we like to the corresponding variable, that is treat it as a free variable. Thus we can suppose initially that every column has a non-zero entry. We can then rearrange the rows so that $a_{11} = 1$. This is sometimes called a *pivot*.

Our second observation is that in (8.4) we can take one equation and subtract it from another. This is equivalent to taking the corresponding row in the matrix and subtracting it from the second corresponding row. When Gaussian elimination is applied generally in the real world one can even take real multiples of one row from another, but in this world we have the much simple environment of having only zeros and ones. Note that if subtraction gives -1 this is the same as 1.

We now take the first row and subtract it from every row with $a_{1k} = 1$. Thus the new matrix will have $a_{11} = 1$ and all the entries below it 0.

Now consider the

$$\begin{pmatrix} 1 & a_{12} & \cdots & a_{1m} \\ 0 & a_{22} & \cdots & a_{2m} \\ 0 & \vdots & & \vdots \\ 0 & a_{l2} & \cdots & a_{lm} \end{pmatrix}.$$

If all the a_{j2} with $2 \leq j \leq l$ are 0, then we move on to the next column. If at least one of the a_{j2} is 1 we move that row to the second row and then subtract it from all the other rows with $a_{j2} = 1$ and $j \geq 2$. We continue in this way until we have reduced the matrix to *echelon* form

$$\begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} & \cdots & a_{1m} \\ 0 & 1 & a_{23} & a_{24} & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

Note that the matrix might well have zeros on the diagonal from some point on. If so some of the rows at the bottom of the matrix are likely to consist of all zeros.

The first 1 in a row is sometimes called a *pivot*. Starting from the bottom of the matrix we now use these pivots to remove any non-zero entry above the pivot. Thus the last matrix would take on the shape

$$\begin{pmatrix} 1 & 0 & a_{13} & 0 & \cdots & a_{1m} \\ 0 & 1 & a_{23} & 0 & \cdots & a_{2m} \\ 0 & 0 & 0 & 1 & \cdots & a_{3m} \\ 0 & 0 & 0 & 0 & \cdots & \vdots \\ & & \vdots & & & \vdots \end{pmatrix}.$$

This is called *reduced echelon* form.

What we see now is that if a_{jk} is a pivot, then the variable e_j only occurs in the j-th row, since all the entries above and below are 0. Thus e_j is determined uniquely by the other (non-pivot) variables, so can be considered as dependent variables. In other words we can take the non-pivot variables, which can be considered independent variables, to be anything we please (0 or 1) and the pivot variables will be determined by them.

Thus in Example 8.1 above we see that the reduced echelon form is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and e_1, e_2, e_3, e_4, e_5, e_6 and e_9 are dependent variables and the rest can be chosen at random.

8.4 Notes

sec:eight4

§1. The history of factorization methods related to searching for t, x, y with $x^2 - y^2 = tn$ is complicated. Apart from Legendre in the eighteenth century there is F. W. Lawrence, "Factorisation of numbers", Messenger of Math., 24(1895), 100-109 and Kraitchik in the 1920s. Continued fraction expansions seemed to have been used explicitly first by D. H. Lehmer and R. E. Powers, "On Factoring Large Numbers", Bull. A. M. S. 37(1931), 770–776, but further developments had to await the widespread use of electronic computers. For a further analysis of the continued fraction method see J. Brillhart and M. A. Morrison, "A Method of Factoring and the Factorization of F_7", Mathematics of Computation, 29(1975), 183-205. Lehman's method described in §2.3 seems to have been discovered independently and is similar ro Lawrence's method listed above, and avoids continued fraction expansions. As noted in §2.3 the theoretical underpinning can be made to depend instead on Dirichlet's theorem on diophantine approximation.

Schroeppel noticed, but did not publish, that the Brillhart-Morrison method had a sub-exponential run time and that it could be improved by introducing sieving ideas in place of continued fraction expansions. Then in 1981 J. D. Dixon, "Asymptotically fast factorization of integers", Math. Comp. 36 (153)(1981), 255–260 created the prototype quadratic sieve using a factor base, and in 1982 Pomerance moulded it in to the form which we examine here. See C. Pomerance, "A Tale of Two Sieves", Notices of the AMS, 43(12)(1996), 1473–1485. It was also in the 1970s that Shanks explored in a different direction. There is a full analysis of SQUFOF in J. E. Gowers and S. S. Wagstaff, "Square Form Factorization", Mathematics of Computation, 77(2008), 551-588. Just to illustrate the long history of rediscovery in this area, apparently in 1858 V. Šimerka had used a method similar to SQUFOF to obtain the factorization

$$11111111111111111 = 2071723 \times 5363222357.$$

§2 The barbarism B-smooth is commonly used to mean B-factorable.

Chapter 9

Arithmetical Functions

9.1 Introduction

sec:nin1

A major consideration in assessing factorisation and primality testing algorithms is the ability to judge and compare possible run times. Underpinning this is some knowledge of the growth patterns of common arithmetic functions and a familiarity with the basic techniques used to elucidate the way in which primes are distributed under various constraints.

It is convenient to make the following definition.

def:nine1 **Definition 9.1.** *Let $\mathcal{A}$ denote the set of arithmetical functions, that is the functions defined by*

$$\mathcal{A} = \{f : \mathbb{N} \to \mathbb{C}\}.$$

Of course the range of any particular function might well be a subset of $\mathbb{C}$, such as $\mathbb{R}$ or $\mathbb{Z}$. There are quite a number of important arithmetical functions. Some examples are

def:nine2 **Definition 9.2 (The divisor function).** *The number of positive divisors of n.*

$$d(n) = \sum_{m|n} 1.$$

def:nine3 **Definition 9.3 (The Möbius function).** *This is a more peculiar function. It is defined by*

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes,} \\ 0 & \text{if there is a prime } p \text{ such that } p^2|n. \end{cases}$$

It is also convenient to introduce three very boring functions.

def:nine4 **Definition 9.4 (The Unit).**

$$e(n) = \begin{cases} 1 & (n = 1), \\ 0 & (n > 1). \end{cases}$$

def:nine5 **Definition 9.5 (The One).**

$$\mathbf{1}(n) = 1 \text{ for every } n.$$

def:nine6 **Definition 9.6 (The Identity).**

$$N(n) = n.$$

Two other functions which have interesting structures but which we will say less about at this stage are

def:nine7 **Definition 9.7 (The primitive character modulo 4).** *We define*

$$\chi_1(n) = \begin{cases} (-1)^{\frac{n-1}{2}} & 2 \nmid n, \\ 0 & 2|n. \end{cases}$$

Similar functions we have already met are Euler's function ϕ, the Legendre symbol and its generalization the Jacobi symbol

$$\left(\frac{n}{m}\right)_J.$$

Here we think of it as a function of n, keeping m fixed, but we could also think of it as a function of m keeping n fixed.

def:nine8 **Definition 9.8 (Sums of two squares).** *We define $r(n)$ to be the number of ways of writing n as the sum of two squares of integers.*

ex:ninesq **Example 9.1.** *For example, $1 = 0^2 + (\pm 1)^2 = (\pm 1)^2 + 0^2$, so $r(1) = 4$, $r(3) = r(6) = r(7) = 0$, $r(9) = 4$, $65 = (\pm 1)^2 + (\pm 8)^2 = (\pm 4)^2 + (\pm 7)^2$ so $r(65) = 16$.*

The functions d, ϕ, e, $\mathbf{1}$, N, χ_1, $\left(\frac{\cdot}{m}\right)_J$ have an important property. That is that they are multiplicative. We already discussed this in connection with Euler's function and the Legendre and Jacobi symbols. Here is a reminder.

def:nine9 **Definition 9.9.** *An arithmetical function f which is not identically 0 is* **multiplicative** *when it satisfies*

$$f(mn) = f(m)f(n) \tag{9.1}$$ eq:ninemult

whenever $(m, n) = 1$. Let $\mathcal{M}$ denote the set of multiplicative functions. If (9.1) holds for **all** *m and n, then we say that f is* **totally multiplicative**.

The function $r(n)$ is not multiplicative, since $r(65) = 16$ but $r(5) = r(13) = 8$. Indeed the fact that $r(1) \neq 1$ would contradict the next theorem. However it is true that $r(n)/4$ is multiplicative, but this is a little trickier to prove.

Theorem 9.1. *Suppose that $f \in \mathcal{M}$. Then $f(1) = 1$.*

Proof. Since f is not identically 0 there is an n such that $f(n) \neq 0$. Hence $f(n) = f(n \times 1) = f(n)f(1)$, and the conclusion follows. □

It is pretty obvious that e, $\mathbf{1}$ and N are in $\mathcal{M}$, and it is actually quite easy to show

thm:nine2 **Theorem 9.2.** *We have $\mu \in \mathcal{M}$.*

Proof. Suppose that $(m, n) = 1$. If $p^2|mn$, then $p^2|m$ or $p^2|n$, so $\mu(mn) = 0 = \mu(m)\mu(n)$. If

$$m = p_1 \dots p_k, \quad n = p_1' \dots p_l'$$

with the p_i, p_j' distinct, then

$$\mu(mn) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(m)\mu(n).$$

□

The following is very useful.

thm:zero5 **Theorem 9.3.** *Suppose the $f \in \mathcal{M}$, $g \in \mathcal{M}$ and h is defined for each n by*

$$h(n) = \sum_{m|n} f(m)g(n/m).$$

Then $h \in \mathcal{M}$.

Proof. Suppose $(n_1, n_2) = 1$. Then a typical divisor m of n_1n_2 is uniquely of the form m_1m_2 with $m_1|n_1$ and $m_2|n_2$. Hence

$$\begin{aligned} h(n_1n_2) &= \sum_{m_1|n_1} \sum_{m_2|n_2} f(m_1m_2)g(n_1n_2/(m_1m_2)) \\ &= \sum_{m_1|n_1} f(m_1)g(n_1/m_1) \sum_{m_2|n_2} f(m_2)g(n_2/m_2). \end{aligned}$$

□

This enables us to establish an interesting property of the Möbius function.

Theorem 9.4. *We have*

$$\sum_{m|n} \mu(m) = e(n).$$

Proof. By the definition of $\mathbf{1}$ the sum here is

$$\sum_{m|n} \mu(m)\mathbf{1}(n/m)$$

and so by the previous theorem it is in $\mathcal{M}$. Moreover if $k \geq 1$, then

$$\sum_{m|p^k} \mu(m) = \mu(1) + \mu(p) = 1 - 1 = 0$$

□

9.1.1 Exercises

1. Show that

$$\left(\sum_{m|n} d(m)\right)^2 = \sum_{m|n} d(m)^3.$$

2. (i) Show that

$$\sum_{l|(m,n)} \mu(l)$$

is 1 when $(m,n)=1$ and is 0 otherwise.

(ii) Prove that

$$\sum_{\substack{m=1 \\ (m,n)=1}}^{n} m = \frac{1}{2} n\phi(n) \quad \text{when} \quad n > 1.$$

(iii) Suppose that $n \geq 2$ and n has the distinct prime factors $p_1, p_2, \ldots, p_r$. Show that

$$\sum_{\substack{m=1 \\ (m,n)=1}}^{n} m^2 = \frac{1}{3}\phi(n)n^2 + \frac{1}{6}(-1)^r \phi(n) p_1 p_2 \ldots p_r.$$

3. A *squarefree* number is one which has no square other than 1 dividing it. Let $s(n)$ denote the characteristic function of the squarefree numbers.

(i) Prove that

$$s(n) = \sum_{m^2|n} \mu(m).$$

(ii) Prove that $s(n)$ is multiplicative.

4. A positive integer n is perfect when $\sigma(n) = 2n$.

(i) (Euclid) Prove that if $2^{(l+1)} - 1$ is prime, then $2^l(2^{l+1} - 1)$ is perfect.

(ii)(Euler) Suppose that $n = 2^l m$, m odd, is an even perfect number. Prove that $\sigma(m) = m + \frac{m}{2^{l+1}-1}$. Prove that m has exactly two positive divisors and so is prime, and that $m = 2^{l+1} - 1$.

(iii) Prove that there is no squarefree perfect number apart from 6.

5. Show that the only totally multiplicative function f for which $\sum_{m|n} f(m)$ is totally multiplicative is the unit e.

6. Prove that for every positive integer n,

$$\sum_{m|n} \mu(m)d(m) = (-1)^{\omega(n)},$$

where $\omega(n)$ is the number of different prime factors of n, as defined in §7.5.

7. Show that the sum of all the primitive roots modulo p lies in the residue class $\mu(p-1)$ modulo p.

8. Let $k \in \mathbb{N}$. Prove that there are infinitely many n such that $\mu(n+1) = \mu(n+2) = \cdots = \mu(n+k)$.

9. (i) Prove that there is an arithmetic function f such that for every natural number n we have $\mu(n) = \sum_{m|n} f(m)$.

(ii) Prove that f multiplicative, and give a formula for $f(p^k)$ when p is prime.

10. Show that every odd number n can be written as the difference of two squares, $n = x^2 - y^2$. How many different choices for the integers x and y are there?

11. Show that if n is a natural number, then

$$\prod_{m|n} m = n^{\frac{1}{2}d(n)}.$$

12. Suppose that $f : \mathbb{N} \to \mathbb{Z}$ is a totally multiplicative function with $f(n) = 0$ or ± 1. Prove that

$$\sum_{m|n} f(m) \geq 0$$

and

$$\sum_{m|n^2} f(m) \geq 1.$$

13. (a) Prove that if $x \geq 1$, then

$$\sum_{n \leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1.$$

Here $\lfloor * \rfloor$ is defined in Definition 1.5.
(b) Prove that

$$-1 + 1/x \leq \sum_{n \leq x} \frac{\mu(n)}{n} \leq 1 + 1/x.$$

In fact we know that

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0,$$

but this is equivalent to the prime number theorem in the sense that if follows from the prime number theorem and there is a relatively simple proof that it implies the prime number theorem.

14.[Schneider] Suppose that $|x| < 1$. (i) Prove that

$$-\sum_{k=1}^{\infty} \frac{\phi(k)}{k} \log(1 - x^k) = \frac{x}{1-x}.$$

(ii) Prove that

$$-\sum_{k=1}^{\infty}\frac{\mu(k)}{k}\log(1-x^k)=x.$$

(iii) Prove that if $\omega=\frac{\sqrt{5}-1}{2}$, so that $1/\omega$ is the *golden ratio*, then

$$\sum_{k=1}^{\infty}\frac{\mu(k)-\phi(k)}{k}\log(1-\omega^k)=1.$$

15. Prove that

$$\sum_{m|n}(-1)^m\phi(n/m)=\begin{cases}-n & (n \text{ odd}),\\ 0 & (n \text{ even}).\end{cases}$$

9.2 Dirichlet Convolution

labelsec:nine2
Theorem 9.3 suggests a general way of defining new functions.

def:nine10 **Definition 9.10.** *Given two arithmetical functions f and g we define the* **Dirichlet convolution** *$f*g$ to be the function defined by*

$$(f*g)(n)=\sum_{m|n}f(m)g(n/m).$$

Note that this operation is commutative because

$$f*g(n)=\sum_{m|n}f(m)g(n/m)=\sum_{m|n}g(n/m)f(m)$$

and the mapping $m\leftrightarrow n/m$ is a bijection.

It is also quite easy to see that the relation is associative

$$(f*g)*h=f*(g*h).$$

To see this write the left hand side as

$$\sum_{m|n}\left(\sum_{l|m}f(l)g(m/l)\right)h(n/m)$$

and interchange the order of summation and replace m by kl, so that $kl|n$, i.e $l|n$ and $k|n/l$. Thus the above is

$$\sum_{l|n}f(l)\sum_{k|n/l}g(k)h\big((n/l)/k\big)=f*(g*h)(n).$$

Dirichlet convolution has some interesting properties.
1. $f * e = e * f = f$ for any $f \in \mathcal{A}$, so e is really acting as a unit.
2. $\mu * \mathbf{1} = \mathbf{1} * \mu = e$, so μ is the inverse of $\mathbf{1}$, and *vice versa*.
3. Theorem 9.3 tells us that if $f \in \mathcal{M}$ and $g \in \mathcal{M}$, then $f * g \in \mathcal{M}$.
4. Theorem 3.2 says that $\phi * \mathbf{1} = N$.
5. $d = \mathbf{1} * \mathbf{1}$, so $d \in \mathcal{M}$. Hence
6. $d(p^k) = k + 1$ and $d(p_1^{k_1} \dots p_r^{k_r}) = (k_1 + 1) \dots (k_r + 1)$.

thm:nine5 **Theorem 9.5** (Möbius inversion I)**.** *Suppose that $f \in \mathcal{A}$ and $g = f * \mathbf{1}$. Then $f = g * \mu$.*

Proof. We have

$$g * \mu = (f * \mathbf{1}) * \mu = f * (\mathbf{1} * \mu) = f * e = f.$$

□

Theorem 9.6 (Möbius inversion II)**.** *Suppose that $g \in \mathcal{A}$ and $f = g * \mu$, then $g = f * \mathbf{1}$.*

The proof is similar.

Theorem 9.7. *We have $\phi = \mu * N$ and $\phi \in \mathcal{M}$. Moreover*

$$\phi(n) = n \sum_{m|n} \frac{\mu(m)}{m} = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

This gives new proofs of Corollary 3.6 and Theorem 3.7.

Proof. By property 4. and Theorem 9.5 we have

$$\phi = N * \mu = \mu * N.$$

Therefore, by property 3 and Theorem 9.2, $\phi \in \mathcal{M}$. Moreover $\phi(p^k) = p^k - p^{k-1}$ and we are done. □

Theorem 9.8. *Let $\mathcal{D} = \{f \in \mathcal{A} : f(1) \neq 0\}$. Then $\langle \mathcal{D}, * \rangle$ is an abelian group.*

Proof. Of course e is the unit, and closure is obvious. We already checked commutativity and associativity. It remains, given $f \in \mathcal{D}$, to construct an inverse. Define g iteratively by

$$\begin{aligned} g(1) &= 1/f(1) \\ g(n) &= -\sum_{\substack{m|n \\ m>1}} f(m)g(n/m)/f(1) \end{aligned}$$

and it is clear that $f * g = e$. □

9.2.1 Exercises

1. We define $\sigma(n)$ for $n \in \mathbb{N}$ to be the sum of the divisors of n,

$$\sigma(n) = \sum_{m|n} m.$$

(i) Prove that σ is a multiplicative function.
(ii) Evaluate $\sigma(1050)$.
(iii) Prove that

$$\sum_{m|n} \phi(m)\sigma(n/m) = nd(n).$$

(iv) Show that if $\sigma(n)$ is odd, then n is a square or twice a square.
(v) Prove that

$$\sum_{m|n} \mu(m)\sigma(n/m) = n.$$

(vi) Prove that

$$\sum_{m|n} \mu(n/m) \sum_{l|m} \mu(l)\sigma(m/l) = \phi(n).$$

2. (cf Hille (1937)) Suppose that $f(x)$ and $F(x)$ are complex-valued functions defined on $[1, \infty)$. Prove that

$$F(x) = \sum_{n \le x} f(x/n)$$

for all x if and only if

$$f(x) = \sum_{n \le x} \mu(n) F(x/n)$$

for all x.

3. Show for each positive integer k that there is a unique arithmetic function ϕ_k such that $\sum_{m|n} \phi_k(m) = n^k$. Obtain a formula for $\phi_k(n)$ and show that $\phi_k(n)$ is multiplicative.

4. Evaluate $h(n) = \sum_{m|n} (-1)^m \mu(n/m)$.

5. Suppose that the arithmetical function $\eta(n)$ satisfies $\sum_{m|n} \eta(m) = \phi(n)$. Show that $\eta(n)$ is multiplicative and evaluate $\eta(p^k)$.

6. Let $g(n)$ denote the number of ordered k-tuples of integers $x_1, x_2, \ldots, x_k$ such that $1 \le x_j \le n$ $(j = 1, 2 \ldots, k)$ and

$$(x_1, x_2, \ldots, x_k, n) = 1,$$

and let $G(n) = \sum_{m|n} g(m)$. Prove that $G(n) = n^k$ and that

$$g(n) = n^k \prod_{p|n} \left(1 - p^{-k}\right).$$

7. This question investigates whether there exists an arithmetic function θ such that $\theta * \theta = \mu$ and $\theta(1) \geq 0$.

(i) Prove that θ exists and is uniquely determined.

(ii) Prove that

$$\theta(p^k) = (-1)^k \binom{\frac{1}{2}}{k}.$$

This is the coefficient of z^k in the Taylor expansion of $(1-z)^{1/2}$ centred at 0. It is easily checked that

$$\theta(p^k) = -\frac{(2k)!}{2^{2k}(k!)^2} = -\frac{1}{2^{2k}}\binom{2k}{k}.$$

(iii) By considering the function $\theta_1(n) = \prod_{p^k \| n} \theta(p^k)$, or otherwise, show that $\theta \in \mathcal{M}$.

8. Let $s \in \mathbb{N}$. Generalise the results of question 7 to the situation $\theta * \theta * \cdots * \theta = \mu$ where on the left one has the s-fold product.

9. Prove that

$$\sum_{m|n} (-1)^{m-1} \mu(n/m) = \begin{cases} 1 & (n=1), \\ -2 & (n=2), \\ 0 & (n>2). \end{cases}$$

9.3 Averages of Arithmetical Functions

sec:nine3

One of the most powerful techniques we have is to take an average.

eq:nine2 **Example 9.2.** *Suppose we have an arithmetical function f and we would like to know that is it often non-zero. If we could show, for example, that for each large X we have*

$$\sum_{n \leq X} f(n)^2 > C_1 X^{5/3}$$

and

$$|f(n)| < C_2 X^{1/3} \quad (n \leq X),$$

where C_1 and C_2 are positive constants, then it follows that

$$C_1 X^{5/3} < \sum_{n \leq X} f(n)^2 \leq (C_2 X^{1/3})^2 \operatorname{card}\{n \leq X : f(n) \neq 0\}$$

and so

$$\operatorname{card}\{n \leq X : f(n) \neq 0\} > C_1 C_2^{-2} X.$$

A more sophisticated version of this would be that if one could show that

$$\sum_{X < n \leq 2X} \big(f(n) - C_3 n^{1/3}\big)^2 < C_4 X^{4/3},$$

then it would follow that for most n the function $f(n)$ is about $n^{1/3}$.

This technique has been used to show that "almost all" even numbers are the sum of two primes.

We are going to need some notation which avoids the continual use of $C_1, C_2, \ldots$, etc., to denote unspecified constants.

Given functions f and g defined on some domain $\mathcal{X}$ with $g(x) \geq 0$ for all $x \in \mathcal{X}$ we write

$$f(x) = O\big(g(x)\big) \tag{9.2}$$ eq:bigoh

to mean that there is some constant C such that

$$|f(x)| \leq Cg(x)$$

for every $x \in \mathcal{X}$. We also use

$$f(x) = o\big(g(x)\big)$$

to mean that if there is some limiting operation, such as $x \to \infty$, then

$$\frac{f(x)}{g(x)} \to 0$$

and

$$f(x) \sim g(x)$$

to mean

$$\frac{f(x)}{g(x)} \to 1.$$

The symbol O was introduced by Bachmann in 1894, and the symbol o by Landau in 1909. The O-symbol can be a bit clumsy for complicated expressions and we will often instead use the Vinogradov symbols, which I. M. Vinogradov introduced about 1934. Thus we will use

$$f \ll g \tag{9.3}$$ eq:vin

to mean (9.2). This also has the advantage that we can write strings of inequalities in the form

$$f_1 \ll f_2 \ll f_3 \ll \ldots.$$

Also if f is also non-negative we may use

$$g \gg f$$

to mean (9.3).

Our first theorem on averages concerns the function $r(n)$ and is due to Gauss. The proof illustrates a rather general principle.

thm:nine11 **Theorem 9.9** (Gauss)**.** *Let $X \geq 1$ and $G(X)$ denote the number of lattice points in the disc centre 0 of radius $\sqrt{X}$, i.e. the number of ordered pairs of integers x, y with $x^2 + y^2 \leq X$. Then*

$$G(X) = \sum_{n \leq X} r(n)$$

and

$$G(X) = \pi X + O(X^{1/2}).$$

Let

$$E(X) = G(X) - \pi X.$$

The question of the actual size of $E(X)$ is one of the classic problems of analytic number theory.

Proof. The first part of this is immediate from the definition of $r(n)$.

To prove the second part we associate with each lattice point (x, y) the unit square $S(x, y) = [x, x + 1) \times [y, y + 1)$ and this gives a partition of the plane. The squares with $x^2 + y^2 \leq X$ are contained in the disc centred at 0 of radius $\sqrt{X} + \sqrt{2}$ (apply Pythagorus's theorem). On the other hand their union contains the disc centered at 0 of radius $\sqrt{X} - \sqrt{2}$. Moreover their area is $G(X)$ and it lies between the areas of the two discs, so

$$\pi(\sqrt{X} - \sqrt{2})^2 \leq G(X) \leq \pi(\sqrt{X} + \sqrt{2})^2,$$

i.e.

$$\pi X - \pi 2\sqrt{2}\sqrt{X} + 2 < G(X) \leq \pi X + \pi 2\sqrt{2}\sqrt{X} + 2\pi,$$

Hence $|G(X) - \pi X| \leq \pi 2\sqrt{2}\sqrt{X} + 3\pi \ll \sqrt{X}$. □

The general principle involved in the above proof is that if one has some finite convex region in the plane and one expands it homothetically, then the number of lattice points in the region is approximately the area of the region with an error of order the length of the boundary. Thus in the theorem above the unit disc centered at the origin has its linear dimensions blown up by a factor of $\sqrt{X}$ (its radius) and the number of lattice points is approximately its area, πX with an error of order the length of the boundary $2\pi\sqrt{X}$.

Before proceeding to look further at some of the arithmetical functions we have defined above, consider the important sum

$$S(X) = \sum_{n \leq X} \frac{1}{n} \tag{9.4}$$ eq:nineE

where $X \geq 1$. This crops up in many places. We already saw it in Chapter 1 in Euler's proof of the infinitude of primes, Theorem 1.3. We observed that the sum $S(X)$ behaves a bit like the integral so is a bit like $\log X$ which tends to infinity with X. In fact there is something more precise which one can say, which was discovered by Euler.

thm:nineE **Theorem 9.10** (Euler)**.** *When $X \geq 1$ the sum $S(X)$ satisfies*

$$S(X) = \log X + C_0 + O\left(\frac{1}{X}\right)$$

where $C_0 = 0.577\ldots$ is Euler's constant

$$C_0 = 1 - \int_1^\infty \frac{t - \lfloor t \rfloor}{t^2} dt$$

where $\lfloor * \rfloor$ is defined in Definition 1.5.

Proof. We have

$$\begin{aligned} S(X) &= \sum_{n \leq X} \left(\frac{1}{X} + \int_n^X \frac{dt}{t^2} \right) = \frac{\lfloor X \rfloor}{X} + \int_1^X \frac{\lfloor t \rfloor}{t^2} dt \\ &= \int_1^X \frac{dt}{t} + 1 - \int_1^X \frac{t - \lfloor t \rfloor}{t^2} dt - \frac{X - \lfloor X \rfloor}{X} \\ &= \log X + C_0 + \int_X^\infty \frac{t - \lfloor t \rfloor}{t^2} dt - \frac{X - \lfloor X \rfloor}{X}. \end{aligned}$$

□

Euler computed C_0 to 19 decimal places (by hand of course). Actually that is not so hard.

One of the more famous theorems concerning averages of arithmetical functions is

thm:nine10 **Theorem 9.11** (Dirichlet)**.** *Suppose that $X \in \mathbb{R}$ and $X \geq 2$. Then*

$$\sum_{n \leq X} d(n) = X \log X + (2C_0 - 1)X + O(X^{1/2}).$$

Let

$$\Delta(X) = \sum_{n \leq X} d(n) - X \log X - (2C_0 - 1)X.$$

As with the similar question for the Gauss lattice point problem one can ask "how does $\Delta(X)$ really behave?"

Proof. The divisor function $d(n)$ can be thought of as the number of ordered pairs of positive integers m, l such that $ml = n$. Thus when we sum over $n \leq X$ we are just counting the number of ordered pairs m, l such that $ml \leq X$. In other words we are counting the number of *lattice points* m, l under the rectangular hyperbola

$$xy = X.$$

The method that Gauss employed for his lattice point problem fails here, because the area under the rectangular hyperbola is infinite, and so is the boundary. Nevertheless the number of lattice points under the curve is finite.

We follow Dirichlet's ingenious proof method, which has become known as the *method of the hyperbola*. We *could* just crudely count, given $m \leq X$, the number of choices for l, namely

$$\left\lfloor \frac{X}{m} \right\rfloor$$

and obtain

$$\sum_{m \leq X} \frac{X}{m} + O(X)$$

and then apply Euler's estimate for $S(X)$, but this gives a much weaker error term.

Dirichlet's idea is to divide the region under the hyperbola into two parts. That with

$$m \leq \sqrt{X},\ l \leq \frac{X}{m}$$

and that with

$$l \leq \sqrt{X},\ m \leq \frac{X}{l}.$$

Clearly each region has the same number of lattice points. However the points m, l with $m \leq \sqrt{X}$ and $l \leq \sqrt{X}$ are counted in both regions. Thus we obtain

$$\begin{aligned} \sum_{n \leq X} d(n) &= 2 \sum_{m \leq \sqrt{X}} \left\lfloor \frac{X}{m} \right\rfloor - \lfloor \sqrt{X} \rfloor^2 \\ &= 2 \sum_{m \leq \sqrt{X}} \frac{X}{m} - X + O(X^{1/2}) \\ &= 2X\big(\log(\sqrt{X}) + C_0\big) - X + O(X^{1/2}). \end{aligned}$$

where in the last line we used Euler's estimate. □

One can also compute an average for Euler's function

thm:nine12 **Theorem 9.12.** *Suppose that $x \in \mathbb{R}$ and $x \geq 2$. Then*

$$\sum_{n \leq x} \phi(n) = \frac{x^2}{2} \sum_{m=1}^{\infty} \frac{\mu(m)}{m^2} + O(x \log x).$$

We remark that the infinite series here is "well known" to be $\frac{6}{\pi^2}$.

Proof. We have $\phi = \mu * N$. Thus

$$\sum_{n \leq x} \phi(n) = \sum_{n \leq x} n \sum_{m \mid n} \frac{\mu(m)}{m} = \sum_{m \leq x} \mu(m) \sum_{l \leq x/m} l.$$

We want a good approximation to the inner sum. This is just the sum of an arithmetic progression of $\lfloor x/m \rfloor$ terms with first term 1 and last term $\lfloor x/m \rfloor$. Thus the sum is

$$\frac{1}{2}\left\lfloor \frac{x}{m} \right\rfloor \left(1 + \left\lfloor \frac{x}{m} \right\rfloor\right) = \frac{1}{2}\left(\frac{x}{m}\right)^2 + O\left(\frac{x}{m}\right).$$

Inserting this in the formula above gives

$$\sum_{n\le x} \phi(n) = \frac{x^2}{2} \sum_{m\le x} \frac{\mu(m)}{m^2} + O\left(\sum_{m\le x} \frac{x}{m}\right).$$

The error term is $\ll x \log x$ by Euler's bound applied to the sum. The main term is

$$\frac{x^2}{2} \sum_{m=1}^{\infty} \frac{\mu(n)}{m^2} + O\left(\sum_{m>x} \frac{x^2}{m^2}\right)$$

The error term here, by the monotonicity of the general term is

$$\ll x^2 \int_x^{\infty} \frac{dy}{y^2} \ll x.$$

Collecting together our bounds gives the theorem. □

There is a curious application of this.

thm:nine12a **Theorem 9.13.** *The probability that two positive integers are coprime is $\frac{6}{\pi^2}$. In other words*

$$\frac{1}{x^2} \operatorname{card}\{m, n : m, n \le x, (m, n) = 1\} \to \frac{6}{\pi^2} \text{ as } x \to \infty.$$

Proof. We have

$$\begin{aligned}\sum_{n\le x} \phi(n) &= \sum_{n\le x} \sum_{\substack{m\le n \\ (m,n)=1}} 1 \\ &= \frac{1}{2} \operatorname{card}\{m, n : m \le n \le x, (m, n) = 1\} \\ &= \frac{1}{2} \operatorname{card}\{m, n : m, n \le x, (m, n) = 1\} + \frac{1}{2}.\end{aligned}$$

since if $m > 1$, then $(m, m) = m > 1$. Thus

$$\frac{1}{x^2} \operatorname{card}\{m, n : m, n \le x, (m, n) = 1\} = -\frac{1}{x^2} + \frac{2}{x^2} \sum_{n\le x} \phi(n).$$

and the result follows from the previous theorem. □

9.3.1 Exercises

1. Prove that for any positive fixed real numbers C and ε we have $(\log n)^C \ll n^\varepsilon$.

2. Suppose that $f(x)$ is differentiable on $[1, X]$ with a continuous derivative on $[1, X]$.
(i) Prove that

$$\sum_{n\le X} f(n) = \lfloor X\rfloor f(X) - \int_1^X \lfloor t\rfloor f'(t)dt$$

$$= \int_1^X f(t)dt + f(1) - (X - \lfloor X\rfloor)f(X) + \int_1^X (t - \lfloor t\rfloor)f'(t)dt.$$

(ii) Suppose further that f is differentiable on $[1, \infty)$ with a continuous derivative on $[1, \infty)$ and that

$$\int_0^\infty |f'(t)|dt$$

converges. Prove that

$$\sum_{n\le X} f(n) = \int_1^X f(t)dt + C - (X - \lfloor X\rfloor)f(X) - \int_X^\infty (t - \lfloor t\rfloor)f'(t)dt$$

where

$$C = f(1) + \int_1^\infty (t - \lfloor t\rfloor)f'(t)dt.$$

3. Prove that $\sum_{n\le x} \frac{\sigma(n)}{n} = \frac{\pi^2}{6}x + O(\log x)$ for $x \ge 2$.

4. Let $D(x) = \sum_{n\le x} d(n)$.
(i) Prove that

$$\sum_{n\le x} \frac{d(n)}{n} = \frac{D(x)}{x} + \int_1^x \frac{D(u)}{u^2}du.$$

(ii) Prove that

$$\sum_{n\le x} \frac{d(n)}{n} = \frac{1}{2}(\log x)^2 + O(\log x).$$

5. A number $n \in \mathbb{N}$ is *squarefree* when it has no repeated prime factors. For $X \in \mathbb{R}$, $X \ge 1$ let $Q(X)$ denote the number of squarefree numbers not exceeding X.
(i) Prove that

$$Q(X) = \frac{6}{\pi^2}X + O\left(\sqrt{X}\right).$$

(ii) Prove that if $n \in \mathbb{N}$, then

$$Q(n) \ge n - \sum_p \left[\frac{n}{p^2}\right].$$

(iii) Prove that

$$\sum_p \frac{1}{p^2} < \frac{1}{4} + \sum_{k=1}^{\infty} \frac{1}{(2k+1)^2} < \frac{1}{4} + \sum_{k=1}^{\infty} \frac{1}{4k(k+1)} = \frac{1}{2}.$$

(iv) Prove that $Q(n) > n/2$ for all $n \in \mathbb{N}$.

(v) Prove that every integer $n > 1$ is a sum of two squarefree numbers.

6. Let $f(n)$ denote the number of solutions of $x^3 + y^3 = n$ in natural numbers x, y. Show that

$$\sum_{n \le X} f(n) = AX^{2/3} + O\left(X^{1/3}\right) \quad \text{where} \quad A = \int_0^1 (1-\alpha^3)^{1/3} d\alpha.$$

Note that $A = \frac{1}{3}B(4/3, 1/3) = \frac{\Gamma(4/3)^2}{\Gamma(5/3)} = \frac{1}{\pi} 3^{3/2} \Gamma(4/3)^3$. Here $B(\alpha, \beta)$ is the Beta function.

7. Show that the number $N(X)$ of different natural numbers of the form $2^r 3^s$ with $r \in \mathbb{N}$, $s \in \mathbb{N}$ and $2^r 3^s \le X$ satisfies

$$N(X) = \frac{(\log X)^2}{2(\log 2)(\log 3)} + O(\log X)$$

as $X \to \infty$. Hint: Note that the condition $2^r 3^s \le X$ is equivalent to $r \log 2 + s \log 3 \le \log X$.

8. Let $M(X)$ denote the number of ordered pairs (m, n) with $m \ne n$, $m \le X$ and $n \le X$ such that $\gcd(m, n) = 1$. Prove that

$$M(X) = 2 \sum_{2 \le n \le X} \phi(n) = \frac{6}{\pi^2} X^2 + O(X \log X),$$

that is, the probability that two different integers chosen at random from $[1, X]$ are coprime is $\frac{6}{\pi^2}$.

9. Let Let

$$d_k(n) = \sum_{\substack{m_1, m_2, \ldots, m_k \\ m_1 m_2 \ldots m_k = n}} 1.$$

Prove that

$$\sum_{n \le X} d_k(n) \sim X \frac{(\log X)^{k-1}}{(k-1)!} \quad \text{as} \quad X \to \infty.$$

10. (i) Prove that $d(mn) \le d(m)d(n)$

(ii) Prove that

$$\sum_{n \le x} d(n)^2 \ll x(\log x)^3.$$

(iii) Let k be a fixed positive integer. Prove that

$$\sum_{n \le x} d(n)^k \ll x(\log x)^{2^k - 1}.$$

9.4 Orders of Magnitude of Arithmetical Functions.

sec:nine4

It is sometimes useful to know something about the way that an arithmetical function grows. Multiplicative functions tend to oscillate quite a bit in size. For example $d(p) = 2$ but if we take n to be the product of the first k primes where k is large, then

$$d(n) = 2^k.$$

The function $d(n)$ also arises in comparisons, for example in deciding the convergence of certain important series. Thus it is useful to have a simple universal upper bound.

thm:nine14 **Theorem 9.14.** *Let $\varepsilon > 0$. Then there is a positive number C which depends at most on ε such that for every $n \in \mathbb{N}$ we have*

$$d(n) < Cn^{\varepsilon}.$$

Note, such a statement is often written as

$$d(n) = O_{\varepsilon}(n^{\varepsilon})$$

or

$$d(n) \ll_{\varepsilon} n^{\varepsilon}.$$

Proof. It suffices to prove the theorem when

$$\varepsilon \leq \frac{1}{\log 2}.$$

Write $n = p_1^{k_1} \dots p_r^{k_r}$ where the p_j are distinct. Recall that

$$d(n) = (k_1 + 1) \dots (k_r + 1).$$

Thus

$$\frac{d(n)}{n^{\varepsilon}} = \prod_{j=1}^{r} \frac{k_j + 1}{p_j^{\varepsilon k_j}}.$$

Since we are only interested in an upper bound the terms for which $p_j^{\varepsilon} > 2$ can be thrown away since $2^k \geq k + 1$. However there are only $\leq 2^{1/\varepsilon}$ primes p_j for which

$$p_j^{\varepsilon} \leq 2.$$

Morever for any such prime we have

$$\begin{aligned} p_j^{\varepsilon k_j} &\geq 2^{\varepsilon k_j} \\ &= \exp(\varepsilon k_j \log 2) \\ &\geq 1 + \varepsilon k_j \log 2 \\ &\geq (k_j + 1)\varepsilon \log 2. \end{aligned}$$

Thus

$$\frac{d(n)}{n^\varepsilon} \le \left(\frac{1}{\varepsilon \log 2}\right)^{2^{1/\varepsilon}}. \tag{9.5}$$ eq:nine30

□

The above can be refined.

thm:nine15 **Theorem 9.15.** *Let $\varepsilon > 0$. Then for every $n \in \mathbb{N}$ we have*

$$d(n) \ll \exp\left(\frac{(\log 2 + \varepsilon)\log n}{\log\log n}\right)$$

In Theorem 9.23 we will show that this is essentially best possible.

Proof. We may suppose that n is larger than some function of ε. In (9.5) replace the ε of that inequality by

$$\frac{\log 2 + \frac{\varepsilon}{2}}{\log\log n}.$$

The n^ε becomes

$$\exp\left(\frac{\left(\log 2 + \frac{\varepsilon}{2}\right)\log n}{\log\log n},\right)$$

and the right hand side becomes

$$\begin{aligned}\exp\left(2^{\frac{\log\log n}{\log 2+\varepsilon/2}} \log\frac{\log\log n}{(\log 2+\varepsilon/2)\log 2}\right) &= \exp\left((\log n)^{1-\frac{\varepsilon/2}{\log 2+\varepsilon/2}} \log\frac{\log\log n}{(\log 2+\varepsilon/2)\log 2}\right)\\ &\ll \exp\left(\frac{\varepsilon\log n}{2\log\log n}\right).\end{aligned}$$

□

The product

$$\prod_{p\mid n}\left(1-\frac{1}{p}\right),$$

or similar such objects, can arise in many contexts. Crudely,

$$(1-1/p)^{-1} \le 2 = d(p) \le d(p^k).$$

Thus

$$\prod_{p\mid n}\left(1-\frac{1}{p}\right) \ge \frac{1}{d(n)} \gg n^{-\varepsilon}.$$

Thus

$$n\exp\left(-(\log 2+\varepsilon)\frac{\log n}{\log\log n}\right) \le \phi(n) < n.$$

In Chapter 8 we will do much better than this.

9.4.1 Exercises

1. Let

$$d_k(n) = \sum_{\substack{m_1,m_2,\ldots,m_k \\ m_1m_2\ldots m_k=n}} 1.$$

(i) Prove that $d_k \in \mathcal{M}$.
(ii) Prove that for any fixed $\varepsilon > 0$ we have

$$d_k(n) \ll n^{\varepsilon}.$$

9.5 Euler and Primes

sec:nine5

There is a function which we have already seen in Definition 1.5, but we have only used so far as a form of shorthand. This is the floor function. It is not an arithmetical function - it is defined on $\mathbb{R}$, not $\mathbb{Z}$. There is a variant of this which is also useful.

def:nine11 **Definition 9.11.** *Occasionally it is also useful to define the* **ceiling function** $\lceil \alpha \rceil$ *for real numbers* α *as the smallest integer* u *such that* $\alpha \leq u$.

The difference $\alpha - \lfloor \alpha \rfloor$ is often called **the fractional part** of α and is sometimes denoted by $\{\alpha\}$.

ex:nine1 **Example 9.3.** $\lfloor \pi \rfloor = 3$, $\lceil \pi \rceil = 4$, $\lfloor \sqrt{2} \rfloor = 1$, $\lfloor -\sqrt{2} \rfloor = -2$, $\lceil -\sqrt{2} \rceil = -1$.

Another related function which is very useful in some parts of number theory, although we will not use it here is $\|x\|$, *the distance of* x *from a nearest integer*,

$$\|x\| = \min_{n \in \mathbb{Z}} |x - n| = \min(x - \lfloor x \rfloor, \lceil x \rceil - x).$$

We already explored the properties of the floor function in Theorem 1.10. Here is another useful property. The floor function has some useful properties.

thm:eight1 **Theorem 9.16.** *For* $x \in \mathbb{R}$ *define* $b(x) = \lfloor x \rfloor - 2\lfloor x/2 \rfloor$. *Then* $b(x)$ *is periodic with period* 2 *and* $b(x) = 0$ *when* $0 \leq x < 1$ *and* 1 *when* $1 \leq x < 2$.

Proof. For $x \in \mathbb{R}$ define $b(x) = \lfloor x \rfloor - 2\lfloor x/2 \rfloor$. Then $b(x)$ is periodic with period 2 and $b(x) = 0$ when $0 \leq x < 1$ and 1 when $1 \leq x < 2$.

The periodicity is easy, since for any $k \in \mathbb{Z}$ we have

$$\begin{aligned} b(x + 2k) &= \lfloor x \rfloor + 2k - 2\lfloor (x/2) + k \rfloor \\ &= \lfloor x \rfloor + 2k - 2\lfloor (x/2) \rfloor - 2k \\ &= b(x). \end{aligned}$$

Hence we only have to evaluate it when $0 \leq x < 2$. It is pretty clear that $b(x) = 0$ when $0 \leq x < 1$ and $= 1$ when $1 \leq x < 2$. □

Euler's proof of Theorem 1.3 is the beginning of the modern approach.

9.6 Elementary Prime number theory

sec:nine6

The strongest results we know about the distribution of primes use complex analytic methods. However there are some very useful and basic results that can be established elementarily. Many expositions of the results we are going to describe use nothing more than properties of binomial coefficients, but it is good to start to get the flavour of more sophisticated interpretations. We start by introducing

def:eight12 **Definition 9.12** (**The von Mangoldt function).** *This is defined by*

$$\Lambda(n) = \begin{cases} 0 & \text{if } n = 1, \\ 0 & \text{if } p_1 p_2 | n \text{ with } p_1 \neq p_2, \\ \log p & \text{if } n = p^k. \end{cases}$$

The support of Λ is the prime powers. The higher powers are quite rare, at most $O(\sqrt{x})$ of them not exceeding x, and so the function is mostly concentrated on the primes themselves. This function is definitely not multiplicative, since $\Lambda(1) = 0$, but nevertheless it has an interesting and useful relationship with a familiar function as a consequence of the extension to prime powers.

Lemma 9.17. *Let $n \in \mathbb{N}$. Then*

$$\sum_{m|n} \Lambda(m) = \log n,$$

Proof. Write $n = p_1^{k_1} \dots p_r^{k_r}$ with the p_j distinct. Then for a non-zero contribution to the sum we have $m = p_s^{j_s}$ for some s with $1 \leq s \leq r$ and j_s with $1 \leq j_s \leq k_s$. Thus the sum is

$$\sum_{s=1}^{r} \sum_{j_s=1}^{k_s} \log p_s = \log n.$$

□

We need to know something about the average of $\log n$.

Lemma 9.18 (Stirling)**.** *Suppose that $X \in \mathbb{R}$ and $X \geq 2$. Then*

$$\sum_{n \leq X} \log n = X(\log X - 1) + O(\log X).$$

This can be thought of as the logarithm of Stirling's formula for $\lfloor X \rfloor !$.

Proof. We have

$$\begin{aligned}\sum_{n\leq X}\log n &= \sum_{n\leq X}\left(\log X - \int_n^X \frac{dt}{t}\right)\\ &= \lfloor X\rfloor \log X - \int_1^X \frac{\lfloor t\rfloor}{t}dt\\ &= X(\log X - 1) + \int_1^X \frac{t-\lfloor t\rfloor}{t}dt + O(\log X).\end{aligned}$$

□

Now we can say something about averages of the von Mangoldt function.

thm:zero16 **Theorem 9.19.** *Suppose that $X \in \mathbb{R}$ and $X \geq 2$. Then*

$$\sum_{m\leq X}\Lambda(m)\left\lfloor\frac{X}{m}\right\rfloor = X(\log X - 1) + O(\log X).$$

Proof. The sum in question is

$$= \sum_{m\leq X}\Lambda(m)\sum_{k\leq X/m} 1.$$

Collecting together the ordered pairs $mk = n$ for a given n and rearranging gives

$$\sum_{n\leq X}\sum_{\substack{k,m\\ km=n}}\Lambda(m)$$

and this is

$$\sum_{n\leq X}\sum_{m|n}\Lambda(m).$$

By the first lemma this is

$$\sum_{n\leq X}\log n$$

and by the second it is

$$X(\log X - 1) + O(\log X).$$

□

At this stage it is necessary to introduce some of the fundamental counting functions of prime number theory. For $X \geq 0$ we define

$$\begin{aligned}\psi(X) &= \sum_{n\leq X}\Lambda(n),\\ \vartheta(X) &= \sum_{p\leq X}\log p,\\ \pi(X) &= \sum_{p\leq X} 1.\end{aligned}$$

The following theorem shows the close relationship between these three functions.

thm:eight6 **Theorem 9.20.** *Suppose that $X \geq 2$. Then*

$$\begin{aligned}
\psi(X) &= \sum_k \vartheta(X^{1/k}), \\
\vartheta(X) &= \sum_k \mu(k)\psi(X^{1/k}), \\
\pi(X) &= \frac{\vartheta(X)}{\log X} + \int_2^X \frac{\vartheta(t)}{t\log^2 t}dt, \\
\vartheta(X) &= \pi(X)\log X - \int_2^X \frac{\pi(t)}{t}dt.
\end{aligned}$$

Note that each of these functions are 0 when $X < 2$, so the sums are all finite.

Proof. By the definition of Λ we have

$$\psi(X) = \sum_k \sum_{p \leq X^{1/k}} \log p = \sum_k \vartheta(X^{1/k}).$$

Hence we have

$$\sum_k \mu(k)\psi(X^{1/k}) = \sum_k \mu(k) \sum_l \vartheta(X^{1/(kl)}).$$

Collecting together the terms for which $kl = m$ for a given m this becomes

$$\sum_m \vartheta(X^{1/m}) \sum_{k|m} \mu(k) = \vartheta(X).$$

We also have

$$\begin{aligned}
\pi(X) &= \sum_{p \leq X} (\log p) \left(\frac{1}{\log X} + \int_p^X \frac{dt}{t\log^2 t} \right) \\
&= \frac{\vartheta(X)}{\log X} + \int_2^X \frac{\vartheta(t)}{t\log^2 t}dt.
\end{aligned}$$

The final identity is similar.

$$\vartheta(X) = \sum_{p \leq X} \log X - \sum_{p \leq X} \int_p^X \frac{dt}{t}$$

etcetera. □

Now we come to a series of theorems which are still used frequently.

thm:eight7 **Theorem 9.21** (Chebyshev)**.** *There are positive constants C_1 and C_2 such that for each $X \in \mathbb{R}$ with $X \geq 2$ we have*

$$C_1 X < \psi(X) < C_2 X.$$

Proof. Recall the function

$$b(x) = \lfloor x \rfloor - 2 \left\lfloor \frac{x}{2} \right\rfloor$$

defined in Theorem 9.16 for $x \in \mathbb{R}$. There we showed that b is periodic with period 2 and

$$b(x) = \begin{cases} 0 & (0 \leq x < 1), \\ 1 & (1 \leq x < 2). \end{cases}$$

Hence

$$\begin{aligned} \psi(X) &\geq \sum_{n \leq X} \Lambda(n) b(X/n) \\ &= \sum_{n \leq X} \Lambda(n) \left\lfloor \frac{X}{n} \right\rfloor - 2 \sum_{n \leq X/2} \Lambda(n) \left\lfloor \frac{X/2}{n} \right\rfloor. \end{aligned}$$

Here we used the fact that there is no contribution to the second sum when $X/2 < n \leq X$. Now we apply Theorem 9.19 and obtain for $x \geq 4$

$$X(\log X - 1) - 2\frac{X}{2}\left(\log \frac{X}{2} - 1)\right) + O(\log X) = X \log 2 + O(\log X).$$

This establishes the first inequality of the theorem for all $X > C$ for some positive constant C. Since $\psi(X) \geq \log 2$ for all $X \geq 2$ the conclusion follows if C_1 is small enough.

We also have, for $X \geq 4$,

$$\psi(X) - \psi(X/2) \leq \sum_{n \leq X} \Lambda(n) f(X/n)$$

and we have already seen that this is

$$X \log 2 + O(\log X).$$

Hence for some positive constant C we have, for all $X > 0$,

$$\psi(X) - \psi(X/2) \leq CX.$$

Hence, for any $k \geq 0$,

$$\psi(X2^{-k}) - \psi(X2^{-k-1}) < CX2^{-k}.$$

Summing over all k gives the desired upper bound. □

We can now obtain the following.

thm:zero19 **Corollary 9.22** (Chebyshev)**.** *There are positive constants C_3, C_4, C_5, C_6 such that for every $X \geq 2$ we have*

$$\begin{aligned} C_3 X <&\vartheta(X) < C_4 X, \\ \frac{C_5 X}{\log X} <&\pi(X) < \frac{C_6 X}{\log X}. \end{aligned}$$

Proof. The second result of Theorem 9.20 states that

$$\vartheta(X) = \sum_{k=1}^{\infty} \mu(k)\psi(X^{1/k}).$$

Remember that the series is really finite because the terms are all 0 when $X^{1/k} < 2$, i.e $k > (\log X)/(\log 2)$. Thus by the previous theorem

$$\left| \sum_{k=2}^{\infty} \mu(k)\psi(X^{1/k}) \right| \leq C_2 X^{1/2} + C_2 X^{1/3} \frac{\log X}{\log 2} < C X^{1/2}$$

for some constant C. Thus

$$|\vartheta(X) - \psi(X)| < C X^{1/2}$$

and so by the previous theorem again

$$C_1 X - C X^{1/2} < \vartheta(X) < C_2 + C X^{1/2} < C_4 X$$

with, say $C_4 = C_2 + C$. If we take $0 < C' < C_1$, then

$$C' X < C_1 X - C X^{1/2}$$

provided that $X > X_0 = \left(\frac{C}{C_1 - C'}\right)^2$. Since $\vartheta(X_)) \geq \log 2$ whenever $X \geq 2$ we can take C_3 to be the minimum of C' and

$$\min_{2 \leq X \leq X_0} \left(\frac{\vartheta(X)}{X} \right).$$

Now turn to $\pi(X)$. By the third formula in Theorem 9.20 we have

$$\pi(X) = \frac{\vartheta(X)}{\log X} + \int_2^X \frac{\vartheta(t)}{t \log^2 t} dt.$$

Thus, at once

$$\pi(X) \geq \frac{\vartheta(X)}{\log X} \geq \frac{C_3 X}{\log X}.$$

The upper bound is more annoying. We have

$$\pi(X) \leq \frac{C_4 X}{\log X} + \int_2^X \frac{C_4 dt}{\log^2 t}.$$

The integral here is bounded by

$$\int_2^{\sqrt{X}} \frac{C_4 dt}{(\log 2)^2} + \int_{\sqrt{X}}^X \frac{C_4 dt}{(\log \sqrt{X})^2} < \frac{C_4\sqrt{X}}{(\log 2)^2} + \frac{4C_4 X}{(\log X)^2} < \frac{C' X}{\log X}.$$

□

Chebychev's theorem can be used to establish a companion to Theorem 9.15.

thm:nine13 **Theorem 9.23.** *For every $\varepsilon > 0$ there are infinitely many n such that*

$$d(n) > \exp\left(\frac{(\log 2 - \varepsilon)\log n}{\log\log n}\right).$$

Proof. Let $n = \prod_{p \leq X} p$ so that

$$\log n = \vartheta(X).$$

Then, by Chebyshev

$$X \ll \log n \ll X$$

and so

$$\log X \sim \log\log n.$$

Moreover

$$d(n) = 2^{\pi(X)},$$

whence

$$\begin{aligned} \log d(n) &= (\log 2)\pi(X) \\ &\geq (\log 2)\frac{\vartheta(X)}{\log X} \\ &\sim (\log 2)\frac{\log n}{\log\log n}. \end{aligned}$$

□

It is also possible to establish a more precise version of Euler's result on the primes.

thm:zero20 **Theorem 9.24** (Mertens)**.** *There is a constant B and a positive constant c such that whenever $X \geq 2$ we have*

$$\sum_{n\leq X} \frac{\Lambda(n)}{n} = \log X + O(1), \tag{9.6}$$ eq:eightM1

$$\sum_{p\leq X} \frac{\log p}{p} = \log X + O(1), \tag{9.7}$$ eq:eightM2

$$\sum_{p\leq X} \frac{1}{p} = \log\log X + B + O\left(\frac{1}{\log X}\right), \tag{9.8}$$ eq:eightM3

$$\prod_{p\leq X}\left(1-\frac{1}{p}\right) = \frac{c}{\log X} + O\left(\frac{1}{(\log X)^2}\right). \tag{9.9}$$ eq:eightM4

Proof. By Theorem 9.19 we have

$$\sum_{m\leq X} \Lambda(m)\left\lfloor \frac{X}{m}\right\rfloor = X(\log X - 1) + O(\log X).$$

The left hand side is

$$X\sum_{m\leq X}\frac{\Lambda(m)}{m} + O(\psi(X)).$$

Hence by Cheyshev's theorem we have

$$X\sum_{m\leq X}\frac{\Lambda(m)}{m} = X\log X + O(X).$$

Dividing by X gives the first result.

We also have

$$\sum_{m\leq X}\frac{\Lambda(m)}{m} = \sum_k \sum_{p^k\leq X}\frac{\log p}{p^k}.$$

The terms with $k \geq 2$ contribute

$$\leq \sum_p \sum_{k\geq 2}\frac{\log p}{p^k} \leq \sum_{n=2}^{\infty}\frac{\log n}{n(n-1)}$$

which is convergent, and this gives the second expression.

Finally we can see that

$$\begin{aligned}\sum_{p\leq X}\frac{1}{p} &= \sum_{p\leq X}\frac{\log p}{p}\left(\frac{1}{\log X} + \int_p^X \frac{dt}{t\log^2 t}\right)\\ &= \frac{1}{\log X}\sum_{p\leq X}\frac{\log p}{p} + \int_2^X \sum_{p\leq t}\frac{\log p}{p}\frac{dt}{t\log^2 t}.\end{aligned}$$

Let

$$E(t) = \sum_{p \le t} \frac{\log p}{p} - \log t$$

so that by the second part of the theorem we have $E(t) \ll 1$. Then the above is

$$\begin{aligned} =& \frac{\log X + E(X)}{\log X} + \int_2^X \frac{\log t + E(t)}{t \log^2 t} dt \\ =& \log\log X + 1 - \log\log 2 + \int_2^\infty \frac{E(t)}{t \log^2 t} dt \\ &+ \frac{E(X)}{\log X} - \int_X^\infty \frac{E(t)}{t \log^2 t} dt. \end{aligned}$$

The first integral here converges and the last two terms are

$$\ll \frac{1}{\log X}.$$

For the final assertion of the theorem observe that

$$-\log\left(1 - \frac{1}{p}\right) = \sum_{k=1}^\infty \frac{1}{kp^k}$$

and so

$$-\log \prod_{p \le X} \left(1 - \frac{1}{p}\right) = \sum_{p \le X} \frac{1}{p} + B_1 - \sum_{p > X} \sum_{k=2}^\infty \frac{1}{kp^k}$$

where

$$B_1 = \sum_p \sum_{k=2}^\infty \frac{1}{kp^k}$$

which converges absolutely since

$$\sum_{k=2}^\infty \frac{1}{kp^k} \le \sum_{k=2}^\infty \frac{1}{p^k} = \frac{1}{p(p-1)}.$$

The other series is bounded by

$$\sum_{p > X} \frac{1}{p(p-1)} \ll X^{-1}.$$

Hence, by the third part of the theorem,

$$-\log \prod_{p \le X} \left(1 - \frac{1}{p}\right) = \log\log X + B_2 + O\left(\frac{1}{\log X}\right)$$

for some real constant B_2. Exponentiating both sides gives the desired conclusion. □

There are several interesting applications of the above which lead to some important developments.

thm:nine24 **Theorem 9.25.** *Suppose that $n \geq 3$. Let c be the constant of Theorem 9.24. Then*

$$\prod_{p|n}\left(1-\frac{1}{p}\right) \geq \frac{c}{\log\log n} + O\left(\frac{1}{(\log\log n)^2}\right)$$

and

$$\frac{cn}{\log\log n} + O\left(\frac{n}{(\log\log n)^2}\right) \leq \phi(n) < n.$$

Proof. Suppose that n has k different prime factors and p_j denotes the j-th prime in order of magnitude. Then

$$\prod_{p|n}\left(1-\frac{1}{p}\right) \geq \prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right) = \prod_{p\leq p_k}\left(1-\frac{1}{p}\right).$$

By Theorem 9.24 this is

$$\frac{c}{\log p_k} + O\left(\frac{1}{(\log p_k)^2}\right).$$

Moreover

$$n \geq \prod_{j\leq k} p_j = \exp\big(\vartheta(p_k)\big).$$

Hence $\log n \geq \vartheta(p_k)$ and so by Chebyshev's theorem $p_k \ll \log n$. Hence $\log p_k \leq \log\log n + O(1)$ and the conclusions follow.

□

9.6.1 Exercises

bsec:nine6.1

1. Let $P(Y) = \prod_{p\leq Y} p$. Prove that if $X \geq 1$, then

$$\pi(X) = \pi(\sqrt{X}) - 1 + \sum_{m|P(\sqrt{X})} \mu(m)\left\lfloor\frac{X}{m}\right\rfloor.$$

2. When $X \geq 1$ let

$$T(X) = \sum_{m\leq X}\frac{\mu(m)}{m}.$$

(i) Prove that

$$\sum_{m\leq X}\mu(m)\left\lfloor\frac{X}{m}\right\rfloor = 1.$$

(ii) Prove that

$$-1+\frac{1}{X}\le T(X)\le \frac{1}{X}+1.$$

Actually $T(X)\to 0$ as $X\to\infty$, but this is non-trivial, and con be proved by the same methods as those used to prove the prime number theorem.

3. Suppose that $m\in\mathbb{N}$, $a,b\in\mathbb{Z}$ and $(a,m)=1$. Prove that

$$\sum_{x=1}^{m}\left(\frac{ax+b}{m}-\left\lfloor\frac{ax+b}{m}\right\rfloor-\frac{1}{2}\right)=-\frac{1}{2}.$$

4. Let $A(x)=\lfloor x\rfloor-\lfloor x/2\rfloor-\lfloor x/3\rfloor-\lfloor x/6\rfloor$.
(i) Prove that $A(x)$ is periodic with period 6 and

$$A(x)=\begin{cases}0 & x\in[0,1),\\ 1 & x\in[1,5),\\ 2 & x\in[5,6).\end{cases}$$

(ii) Let

$$S(x)=\sum_{m\le x}\Lambda(m)A(x/m).$$

Prove that if $x\ge 6$, then $S(x)=cx+O(\log x)$ where

$$c=\frac{1}{2}\log 2+\frac{1}{3}\log 3+\frac{1}{6}\log 6=1.01140\ldots.$$

(iii) Prove that if $x\ge 0$, then

$$\psi(x)+\psi(x/5)-2\psi(x/6)\le S(x)\le\psi(x)+\psi(x/5).$$

(iv) Prove that if $x\ge 2$, then

$$\psi(x)\le\frac{6c}{5}x+O(\log^2 x).$$

5. For $x\ge 0$ define $B(x)=\lfloor x\rfloor-\lfloor x/2\rfloor-\lfloor x/3\rfloor-\lfloor x/5\rfloor+\lfloor x/30\rfloor$.
(i) Prove that $B(x)$ is periodic with period 30,

$$B(x)=\begin{cases}0 & x\in[0,1),\\ 1 & x\in[1,6),\\ 0 & x\in[6,7),\\ 1 & x\in[7,10),\\ 0 & x\in[10,11),\\ 1 & x\in[11,12),\\ 0 & x\in[12,13),\\ 1 & x\in[13,15)\end{cases}$$

and that if $0 \le x < 15$, then $B(x+15) = B(x) + \lfloor x/2 \rfloor - \lfloor (x+1)/2 \rfloor$. Deduce that $0 \le B(x) \le 1$ for all x.

(ii) Let $T(x) = \sum_{m \le x} \Lambda(m) B(x/m)$. Prove that $B(x) = c'x + O(\log x)$ where $c' = \frac{1}{2}\log 2 + \frac{1}{3}\log 3 + \frac{1}{5}\log 5 - \frac{1}{30}\log 30 = 0.9212\ldots$.

(iii) Prove that $\psi(x) - \psi(x/6) \le T(x) \le \psi(x)$.

(iv) Prove that if $x \ge 2$, then

$$c'x + O(\log x) \le \psi(x) \le \frac{6c'}{5}x + O(\log^2 x).$$

Remark: $6c'/5 = 1.1054\ldots$.

6. (i) Prove that if $x \ge 1$, then

$$\int_1^x \frac{\psi(u)}{u^2} du = \log x + O(1).$$

(ii) Prove that $\limsup_{x\to\infty} \frac{\psi(x)}{x} \ge 1$ and $\liminf_{x\to\infty} \frac{\psi(x)}{x} \le 1$.

(iii) Prove that if there is a constant c such that $\psi(x) \sim cx$ as $x \to \infty$, then $c = 1$.

(iv) Prove that if there is a constant c such that $\pi(x) \sim c\frac{x}{\log x}$ as $x \to \infty$, then $c = 1$.

7. (i) Let $d_n = \operatorname{lcm}[1, 2, \ldots, n]$. Show that $d_n = e^{\psi(n)}$.

(ii) Let $P \in \mathbb{Z}[x]$, $\deg P \le n$. Put $I = I(P) = \int_0^1 P(x)\,dx$. Show that $Id_{n+1} \in \mathbb{Z}$, and hence that $d_{n+1} \ge 1/|I|$ if $I \ne 0$.

(iii) Show that there is a polynomial P as above so that $Id_{n+1} = 1$.

(iv) Verify that $\max_{0\le x\le 1} |x^2(1-x)^2(2x-1)| = 5^{-5/2}$.

(v) For $P(x) = \big(x^2(1-x)^2(2x-1)\big)^{2n}$, verify that $0 < I < 5^{-5n}$.

(vi) Show that $\psi(10n+1) \ge (\frac{1}{2}\log 5)\cdot 10n$.

9.7 The Normal Number of Prime Factors

sec:nine7

As a companion to the definition of a multiplicative function we have

def:eight13 **Definition 9.13.** *An $f \in \mathcal{A}$ is* **additive** *when it satisfies $f(mn) = f(m)+f(n)$ whenever $(m,n) = 1$.*

Now we introduce two further functions.

def:eight14 **Definition 9.14.** *We define $\omega(n)$ to be the number of different prime factors of n and $\Omega(n)$ to be the total number of prime factors of n.*

ex:eight2 **Example 9.4.** *We have $360 = 2^3 3^2 5$ so that $\omega(360) = 3$ and $\Omega(360) = 6$. Generally, when the p_j are distinct, $\omega(p_1^{k_1}\ldots p_r^{k_r}) = r$ and $\Omega(p_1^{k_1}\ldots p_r^{k_r}) = k_1 + \cdots k_r$.*

One might expect that most of the time Ω is appreciably bigger than ω, but in fact this is not so. By the way, there is some connection with the divisor function. It is not hard to show that

$$2^{\omega(n)} \le d(n) \le 2^{\Omega(n)}.$$

In fact this is a simple consequence of the chain of inequalities

$$2 \le k+1 \le 2^k.$$

thm:eight12 **Theorem 9.26.** *Suppose that $X \ge 2$. Then*

$$\sum_{n\le X} \omega(n) = X\log\log X + BX + O\left(\frac{X}{\log X}\right)$$

where B is the constant of Theorem 9.24, and

$$\sum_{n\le X} \Omega(n) = X\log\log X + \left(B + \sum_p \frac{1}{p(p-1)}\right)X + O\left(\frac{X}{\log X}\right).$$

Proof. We have

$$\begin{aligned}\sum_{n\le X}\omega(n) &= \sum_{n\le X}\sum_{p\mid n} 1 = \sum_{p\le X}\left\lfloor \frac{X}{p}\right\rfloor \\ &= X\sum_{p\le X}\frac{1}{p} + O\big(\pi(X)\big)\end{aligned}$$

and the result follows by combining Corollary 9.22 and (9.8) of Theorem 9.24.

The case of Ω is similar. We have

$$\sum_{n\le X}\Omega(n) = X\sum_{\substack{p,k\\ p^k\le X}}\frac{1}{p^k} + O\left(\sum_{k\le(\log X)/(\log 2)}\pi(X^{1/k})\right).$$

When $k\ge 2$ the terms in the error are $\ll X^{1/2}$ and so the total contribution from the $k\ge 2$ is $\ll X^{1/2}\log X$. In the main term, when $k\ge 2$ it remains to understand the behaviour of

$$\sum_{k\ge 2}\sum_{p>X^{1/k}}\frac{1}{p^k} \le \sum_{p>X^{1/2}}\frac{1}{p^2} + \sum_{k\ge 3}\frac{1}{(X^{1/k})^{k/2}}\sum_p\frac{1}{p^{k/2}}.$$

The first sum is $\ll X^{-1/2}$ and the second is

$$\ll X^{-1/2}\sum_p\frac{1}{p(p^{1/2}-1)} \ll X^{-1/2}.$$

□

Hardy and Ramanujan made the remarkable discovery that $\log\log n$ is not just the average of $\omega(n)$, but is its normal order. Later Turán found a simple proof of this.

Theorem 9.27 (Hardy & Ramanujan)**.** *Suppose that $X \geq 2$. Then*

$$\sum_{n\leq X}\left(\omega(n)-\sum_{p\leq X}\frac{1}{p}\right)^2 \ll X\sum_{p\leq X}\frac{1}{p},$$

$$\sum_{n\leq X}\left(\omega(n)-\log\log X\right)^2 \ll X\log\log X$$

and

$$\sum_{2\leq n\leq X}\left(\omega(n)-\log\log n\right)^2 \ll X\log\log X.$$

This theorem says that the normal number of prime factors of n is $\log\log n$.

Proof. (Turán). By (9.8), we have

$$\sum_{n\leq X}\left(\sum_{p\leq X}\frac{1}{p}-\log\log X\right)^2 \ll X$$

and, since for $\sqrt{X} < n \leq X$, we have

$$\begin{aligned}0 \leq \log\log X-\log\log n &< \log\log X-\log\log\sqrt{X}\\ &= \log X-\log\frac{1}{2}\log X\\ &= \log 2,\end{aligned}$$

it follows that

$$\begin{aligned}\sum_{2\leq n\leq X}(\log\log X-\log\log n)^2 &\ll \sqrt{X}(\log\log X)^2+\sum_{\sqrt{X}n\leq X}1\\ &\ll X.\end{aligned}$$

Thus it suffices to prove the second statement in the theorem. We have

$$\begin{aligned}\sum_{n\leq X}\omega(n)^2 &= \sum_{n\leq X}\sum_{p_1|n}\sum_{p_2|n}1\\ &= \sum_{p_1\leq X}\sum_{\substack{p_2\leq X\\ p_2\neq p_1}}\left\lfloor\frac{X}{p_1p_2}\right\rfloor+\sum_{p\leq X}\left\lfloor\frac{X}{p}\right\rfloor\\ &\leq \sum_{p_1\leq X}\sum_{\substack{p_2\leq X\\ p_2\neq p_1}}\frac{X}{p_1p_2}+\sum_{p\leq X}\frac{X}{p}\\ &\leq X(\log\log X)^2+O(X\log\log X)\end{aligned}$$

by (9.8). Hence, by 9.26

$$\sum_{n\le X}(\omega(n)-\log\log X)^2 \le 2X(\log\log X)^2 - 2(\log\log X)\sum_{n\le X}\omega(n) + O(X\log\log X)$$

and this is $\ll X\log\log X$. □

One way of interpreting this theorem is to think of it probabilistically. It is saying that the events $p|n$ are approximately independent and occur with probability $\frac{1}{p}$. Thus we can think of $\omega(n)$ as being a sum of independent random variables, and so the cental limit theorem should apply. That is, one might guess that the distribution is normal. This indeed is true and was established by Erdős and Kac in 1940. Let

$$\Phi(a,b) = \lim_{x\to\infty}\frac{1}{x}\text{card}\{n\le x : a < \frac{\omega(n)-\log\log n}{\sqrt{\log\log n}} \le b\}.$$

Then

$$\Phi(a,b) = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-t^2/2}dt.$$

This lead to a whole new subject, *Probabilistic Number Theory.*

9.7.1 Exercises

1. Let $\lambda(n) = (-1)^{\Omega(n)}$ (Liouville's function). Prove that

$$\lambda(n) = \sum_{m^2|n}\mu\left(n/m^2\right).$$

2. Prove that $\Omega(n) \le \frac{\log n}{\log 2}$.

3. Let y be any real number with $y > 1$.

(i) By considering the prime divisors p of n with $p > y$, or otherwise, prove that $y^{\omega(n)-y} \le n$, i.e.

$$\omega(n) \le y + \frac{\log n}{\log y}.$$

(ii) Prove that $f(x) = 2x^{\frac{1}{2}} - \log x$ is an increasing function of x for $x \ge 1$. Deduce that if $n \ge 3$, then

$$(\log n)^{\frac{1}{2}} < \frac{2\log n}{\log\log n}.$$

(iii) Prove that if $n \ge 3$, then $\omega(n) \le \frac{4\log n}{\log\log n}$.

4. Suppose that $X \ge 2$. Prove that

$$\sum_{n\le X}\left(\Omega(n) - \sum_{p\le X}\frac{1}{p}\right)^2 \ll X\sum_{p\le X}\frac{1}{p},$$

$$\sum_{n\le X}(\Omega(n)-\log\log X)^2 \ll X\log\log X$$

and

$$\sum_{2\le n\le X}(\Omega(n)-\log\log n)^2\,.$$

5. Let $\varepsilon>0$. Prove that the set $E(X)$ of $n\le X$ for which

$$(\log n)^{\log 2-\varepsilon} < d(n) < (\log n)^{\log 2+\varepsilon}$$

does not hold satisfies $\operatorname{card} E(X) \ll \frac{X}{\log\log X}$.

This reveals the curious fact that whereas the average value of $d(n)$ is $\log n$, $d(n)$ is normally smaller, about $(\log n)^{\log 2}$. The reason is that the average is dominated by the exceptionally large values of $d(n)$.

9.8 Primes in arithmetic progressions

sec:nine8

We finish the chapter by developing the ultimate version of Euclid's proof that there are infinitely many primes. Let $k\in\mathbb{N}$ and let $\Phi_k(z)$ denote the k-th cyclotomic polynomial.

$$\Phi_k(z)=\prod_{\substack{l=1\\(k,k)=1}}^{k}(z-\varpi^l)$$

where

$$\varpi=e^{2\pi i/k}.$$

Thus Φ_k is the monic polynomial whose roots are the primitive k-th roots of unity and its degree is Euler's function $\phi(k)$. Note that $\Phi_k(z)$ is a (polynomial) factor of z^k-1.

We can use the Möbius function to remove the condition that $(l,k)=1$. Thus

$$\begin{aligned}\Phi_k(z)&=\prod_{l=1}^{k}(z-\varpi^l)^{\sum_{m|(l,k)}\mu(m)}\\&=\prod_{l=1}^{k}\prod_{m|(l,k)}(z-\varpi^l)^{\mu(m)}\\&=\prod_{m|k}\left(\prod_{n=1}^{k/m}(z-\varpi^{nm})\right)^{\mu(m)}.\end{aligned}$$

Therefore

$$\Phi_k(z)=\prod_{m|k}(z^{k/m}-1)^{\mu(m)}. \tag{9.10}$$

eq:eighta1

Example 9.5. *The cases $k = 4$ and 6 are*

$$\Phi_4(z) = (z - i)(z + i) = z^2 + 1 = \frac{z^4 - 1}{z^2 - 1}$$

and

$$\Phi_6(z) = (z - \varpi)(z - \varpi^5) = z^2 - z + 1 = \frac{(z^6 - 1)(z - 1)}{(z^3 - 1)(z^2 - 1)}.$$

For any prime p

$$\Phi_p(z) = z^{p-1} + z^{p-2} + \cdots + z + 1.$$

We can use (9.10) to prove that the cyclotomic polynomials have integer coefficients.

Theorem 9.28. *The k-th cyclotomic polynomial has integer coefficients.*

Proof. By the formula (9.10), when $|z| < 1$, we have

$$\begin{aligned} z^{\phi(k)}\Phi_k(1/z) &= \prod_{m|k}(1 - z^{k/m})^{\mu(m)} \\ &= \prod_{\substack{m|k \\ \mu(m)=1}} (1 - z^{k/m}) \prod_{\substack{m|k \\ \mu(m)=-1}} (1 + z^{k/m} + z^{2k/m} + \cdots). \end{aligned}$$

□

We have a finite product of absolutely convergent series with integer coefficients whose product is a polynomial. Collecting together terms shows that $\Phi_k(z)$ has integer coefficients.

The constant term of $\Phi_k(z)$ is

$$\prod_{\substack{l=1 \\ (l,k)=1}}^{k} (-\varpi^l)$$

which has modulus 1. Thus it is ± 1.

We can use these polynomials to show that given any $k \in \mathbb{N}$ there are infinitely many primes of the form $kx + 1$.

thm:eight14 **Theorem 9.29.** *Suppose that $k \in \mathbb{N}$. Then there are infinitely many primes of the form $kx + 1$.*

Proof. Suppose that $r \in \mathbb{N}$, $r > 1$ and p is a prime with $p \nmid k$ and $p|\Phi_k(r)$. Then $p|r^k - 1$ and $p \nmid r$. Thus $e = \operatorname{ord}_p r|k$, and if $m|k$ and $p|r^m - 1$, then $e|m$. Write $r^e = 1 + up^v$ for some positive integers u and v with $p \nmid u$. Then

$$r^{el} - 1 = (1 + up^v)^l - 1 \equiv lup^v \pmod{p^{2v}}.$$

Thus if $l|k$, so that $p \nmid l$, p^v is the exact power of p dividing $r^{el}-1$. Thus the exact power of p dividing $\Phi_k(r)$ is

$$\prod_{\substack{m|k\\ e|m}} (p^v)^{\mu(m)} = p^{v\sum_{l|k} /e\mu((k/e)/l)}.$$

and the exponent is 0 unless $e = k$. Thus we have shown that if $p \nmid k$ and $p|\Phi_k(r)$, then r has order k modulo p. Thus $k = \operatorname{ord} p(r)|p-1$.

Now suppose there are only a finite number of primes $p_1, \dots, p_j$ in the residue class 1 modulo k and let $r = kyp_1 \dots p_j$ where y is chosen to ensure that $\Phi_k(r) > 1$. Then there is at least one prime with $p|\Phi_k(r)$ and from above $p \equiv 1 \pmod{k}$. Thus $p|r$ also. Hence p divides the constant term of $\Phi_k(z) = \pm 1$ which is absurd. □

9.8.1 Exercises

lbsec:nine8.1

1. Prove that if p is a prime, then

$$\Phi_{pk}(z) = \begin{cases} \frac{\Phi_k(z^p)}{\Phi_k(z)} & (p \nmid k), \\ \Phi_k(z^p) & (p|k). \end{cases}$$

2. Prove that if $2 \nmid k$, $j \geq 1$ and $k > 1$, then

$$\Phi_{2^j k} = \Phi_k\big(-z^{2^{j-1}}\big).$$

3. Prove that if $k > 1$, then $\Phi_k(0) = 1$.

4. (i) Prove that if k is the product of at most two distinct primes, then the coefficients of $\Phi_k(z)$ are ± 1 or 0.

(ii) Prove that the coefficient of z^7 in $\Phi_{105}(z)$ is -2.

5. Prove that $\Phi_k(1) = e^{\Lambda(k)}$, where Λ is the von Mangoldt function.

6. (i) Suppose that $2|x$, p is prime and $p|x^4+1$. Show that $8|p-1$.

(ii) Suppose that $x \equiv 3 \pmod{41^2}$. Show that 41 divides x^4+1, but 41^2 does not. Hence show that there are infinitely many primes $p \equiv 9 \pmod{16}$.

7. By considering the polynomial $x^2 - 5$ show that there are infinitely many primes p satisfying $p \equiv -1 \pmod{5}$.

9.9 Notes

sec:nine9

§1. Möbius discovered Mobius inversion in 1832. The exercise 9.2.1.2 is in E. Hille (1937). *The inversion problem of Möbius*, Duke Math. J. **3**, 549–568.

§3. As in the remark after Gauss' Theorem 9.9 let $E(X) = G(X) - \pi X$. The best bound we have for $E(X)$ is in Huxley 2002, "Integer points, exponential sums and

the Riemann zeta function", Number theory for the millennium, II (Urbana, IL, 2000) pp.275–290, pub. A K Peters, where it is shown that

$$E(X) = O(X^\theta)$$

for any $\theta > \frac{131}{416}$. We also know (Hardy and Landau, independently [1915]) that one cannot take $\theta < \frac{1}{4}$.

Euler investigated $S(X)$ and C_0 in 1735. Sometimes γ is used to denote C_0 (Mascheroni 1790).

Theorem 9.11 occurs in J.P.G.L. Dirichlet (1849) "Über die Bestimmung der mittleren Werte in der Zahlentheorie," Abh. Akad. Wiss. Berlin,2, 49–66. A huge amount of work has gone into bounding $\Delta(X)$. Suppose that θ is such that

$$\Delta(X) \ll X^\theta$$

for every $X \geq 1$. Then the current world record is that this holds for any $\theta > 131/416 = 0.31490\cdots$ and is in M. N. Huxley (2003), "Exponential sums and lattice points III", Proc. London Math. Soc. 87 (3), 591–609. In the other direction Hardy [1916] proved that one cannot take $\theta < \frac{1}{4}$.

Theorem 9.12, or rather the exercise 9.3.1.8 is sometimes known as the primitive lattice point problem. The error term is connected with the Riemann Hypothesis.

Apropos Exercise 9.3.1.10, Ramanujan (1916) "Some formulæ in the analytic theory of numbers", Messenger of Mathematics, 45, 81-84, formula (3), states that

$$\sum_{n\leq x} d(n)^2 = \frac{1}{\pi^2}x(\log x)^3 + Bx(\log x)^2 + Cx\log x + Dx + O(x^\theta)$$

holds for certain constants B, C and D and for any $\theta > 3/5$.

§6. Chebyshev established Theorems 9.21 and 9.22 in P. L. Chebyshev (1848, 1850), "Sur la fonction qui détermine la totalité des nombres premiers inférieurs à une limite donné", Mem. Acad. Sci. St. Petersburg 6, 1-19 and "Mémoire sur nombres premiers", Mem. Acad. Sci. St. Petersburg 7, 17-33. The various parts of Theorem 9.24 appeared in F. Mertens (both 1874), "Über einige asymptotische Gesetze der Zahlentheorie", J. Reine Angew. Math. 77, 289-338 and "Ein Beitrag zur analytischen Zahlentheorie, J. Reine Angew. Math. 78, 46-62.

§7. Theorem 9.26 is in G. H. Hardy & S. Ramanujan (1920) "The normal order of prime factors of a number n", Quart. J. Math. 48, 76-92 and the proof we give is in P. Turán (1934) "On a theorem of Hardy and Ramanujan", J. London Math. Soc. 9, 274-276. The Erdős-Kac theorem is in P. Erdős & M. Kac (1940). "The Gaussian Law of Errors in the Theory of Additive Number Theoretic Functions", American Journal of Mathematics. 62 (1/4), 738–742.

§8. Theorem 9.29 was first proved by Legendre in 1830. Curiously there seems to be no way of developing these ideas further to establish that a general reduced residue class contains infinitely many primes. Dirichlet' s proof of this instead is essentially

analytic and can be considered the ultimate version of Euler's proof. However there are connections between Dirchlet's proof and algebraic number theory, especially the zeta function associated with a ring of integers.

Exercise 4 was first noticed by A. Migotti, "Aur Theorie der Kreisteilungsgleichung", Z. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien, 87, 7-14 (1883). In spite of initial appearances to the contrary the coefficients can get surprisingly large. Let $A(k)$ denote the absolute value of the largest coefficient of $\Phi_k(z)$. Schur in a letter to Landau in 1935 showed that the sequence $A(k)$ is unbounded, and following work of P. Erdős, "On the coefficients of the cyclotomic polynomials", Bull. Amer. Math. Soc., 52, 179-181, (1946) and "On the coefficients of the cyclotomic polynomials", Portugal. Math. 8, 63-71 (1949), it was shown in R. C. Vaughan, "Bounds for the coefficients of cyclotomic polynomials", Michigan Math. J. 21, 289-295 (1975) that there are arbitrarily large n such that

$$A(n) > \exp\left(\exp\left((\log 2)\frac{\log n}{\log\log n}\right)\right)$$

and that this is essentially best possible.