Introduction

The integers

Divisibility

Prime Numbers

The fundamental theorem of arithmetic

Trial Division

Differences of Squares

The Floor Function

Factorization and Primality Testing Chapter 1 Background

Robert C. Vaughan

August 28, 2023

Introduction to Factorization and Primality Testing

- This course is concerned with the various mathematical theorems which underpin the factorization of integers into primes and the testing of integers for primality.

Introduction to Factorization and Primality Testing

- This course is concerned with the various mathematical theorems which underpin the factorization of integers into primes and the testing of integers for primality.
- A substantial portion of this course is theoretical and solutions to problems will require the writing of proofs.

Introduction to Factorization and Primality Testing

- This course is concerned with the various mathematical theorems which underpin the factorization of integers into primes and the testing of integers for primality.
- A substantial portion of this course is theoretical and solutions to problems will require the writing of proofs.
- Some other parts of the course will require the writing of computer programs using multiprecision arithmetic.

Introduction to Factorization and Primality Testing

- This course is concerned with the various mathematical theorems which underpin the factorization of integers into primes and the testing of integers for primality.
- A substantial portion of this course is theoretical and solutions to problems will require the writing of proofs.
- Some other parts of the course will require the writing of computer programs using multiprecision arithmetic.
- In view if the close connections with security protocols this is a rapidly moving area, and one is never quite sure of the current state-of-the-art since many security organizations do not publish their work.

- The text which is normally used for this course is Bressoud, Factorization and Primality Testing, Springer, ISBN–10: 0387970400, ISBN–13: 978-0387970400

- The text which is normally used for this course is Bressoud, Factorization and Primality Testing, Springer, ISBN–10: 0387970400, ISBN–13: 978-0387970400
- This was written especially for this course when it was first put on in the lat 1980s.

- The text which is normally used for this course is Bressoud, Factorization and Primality Testing, Springer, ISBN–10: 0387970400, ISBN–13: 978-0387970400
- This was written especially for this course when it was first put on in the lat 1980s.
- But it has never been revised so has no account of later developments such as those based on the theory of elliptic curves or the number field sieve, topics which are normally only covered in graduate courses.

- The text which is normally used for this course is Bressoud, Factorization and Primality Testing, Springer, ISBN–10: 0387970400, ISBN–13: 978-0387970400
- This was written especially for this course when it was first put on in the lat 1980s.
- But it has never been revised so has no account of later developments such as those based on the theory of elliptic curves or the number field sieve, topics which are normally only covered in graduate courses.
- Another deficiency is that there is no proper discussion of relative runtimes. This would need some understanding of analytic number theory, a topic which is also usually only covered in graduate classes.

- The text which is normally used for this course is Bressoud, Factorization and Primality Testing, Springer, ISBN–10: 0387970400, ISBN–13: 978-0387970400
- This was written especially for this course when it was first put on in the lat 1980s.
- But it has never been revised so has no account of later developments such as those based on the theory of elliptic curves or the number field sieve, topics which are normally only covered in graduate courses.
- Another deficiency is that there is no proper discussion of relative runtimes. This would need some understanding of analytic number theory, a topic which is also usually only covered in graduate classes.
- A more advanced text which covers these topics is Crandall and Pomerance, Prime Numbers:A Computational Perspective, Springer, ISBN–10: 0387252827, ISBN–13: 978-0387252827

- It is essential for the course that you have **some** familiarity with the concept of mathematical proof.

- It is essential for the course that you 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.

- It is essential for the course that you 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.
- However a proof can be very easy, e.g., the statement

$$105 = 3.5.7$$

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

- It is essential for the course that you 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.
- However a proof can be very easy, e.g., the statement

$$105 = 3.5.7$$

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

- And $101 = d.q + r$ with

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

gives a proof that 101 is prime.

- How about a not very big number like

$$100006561?$$

- 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?

- 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

$$\begin{aligned} 11111111111111111 &\quad \text{17 digits,} \\ 1111111111111111111 &\quad \text{19 digits.} \end{aligned}$$

One of them is prime, the other composite.

- 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

$$\begin{aligned} 11111111111111111 &\quad \text{17 digits,} \\ 1111111111111111111 &\quad \text{19 digits.} \end{aligned}$$

  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.

- Here is an example where a bit of theory is useful.
- There is a theorem which says that if p is prime, then 2^{p-1} leaves the remainder 1 on division by p.

- Here is an example where a bit of theory is useful.
- There is a theorem 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.

- Here is an example where a bit of theory is useful.
- There is a theorem 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 very easy.

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

- Here is an example where a bit of theory is useful.
- There is a theorem 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 very 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

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

- Here is an example where a bit of theory is useful.
- There is a theorem 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 very 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

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

- So any program which can do double precision can compute 2^{p-1} modulo p in linear time.

- This is a *proofs* based course. The proofs will be mostly short and simple.

- This is a *proofs* based course. The proofs will be mostly short and simple.
- One is often asked why one needs formal proofs.

- This is a *proofs* based course. The proofs will be mostly short and simple.
- One is often asked why one needs formal proofs.
- They are necessary, and as a general principle understanding the proof usually reveals the underlying structure which is the reason why the theorem is true.

- This is a *proofs* based course. The proofs will be mostly short and simple.
- One is often asked why one needs formal proofs.
- They are necessary, and as a general principle understanding the proof usually reveals the underlying structure which is the reason why the theorem is true.
- There is an instructive example due to J. E. Littlewood in 1912.

Littlewood

- 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

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

Littlewood

- 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^{22}.

x	$\pi(x)$	$\mathrm{li}(x)$
10^4	1229	1245
10^5	9592	9628
10^6	78498	78626
10^7	664579	664917
10^8	5761455	5762208
10^9	50847534	50849233
10^{10}	455052511	455055613
10^{11}	4118054813	4118066399
10^{12}	37607912018	37607950279
10^{13}	346065536839	346065645809
10^{14}	3204941750802	3204942065690
10^{15}	29844570422669	29844571475286
10^{16}	279238341033925	279238344248555
10^{17}	2623557157654233	2623557165610820
10^{18}	24739954287740860	24739954309690413
10^{19}	234057667276344607	234057667376222382
10^{20}	2220819602560918840	2220819602783663483
10^{21}	21127269486018731928	21127269486616126182
10^{22}	201467286689315906290	201467286691248261498

Littlewood's theorem

- In fact this table has been extended out to at least 10^{27}. So is

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

always true?

Littlewood's theorem

- In fact this table has been extended out to at least 10^{27}. So is

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

always true?

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

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

Littlewood's theorem

- In fact this table has been extended out to at least 10^{27}. 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
$$x \approx 1.387162 \times 10^{316} \tag{1.1}$$
well beyond what can be calculated directly.

Introduction to Number Theory

- For many years it was only known that the first sign change in $\pi(x) - \mathrm{li}(x)$ occurs for *some* x satisfying

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

Introduction to Number Theory

- 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.

Introduction to Number Theory

- 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.

Introduction to Number Theory

- 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.

x	$\pi(x)$	$\mathrm{li}(x)$
10^4	1229	1245
10^5	9592	9628
10^6	78498	78626
10^7	664579	664917
10^8	5761455	5762208
10^9	50847534	50849233
10^{10}	455052511	455055613
10^{11}	4118054813	4118066399
10^{12}	37607912018	37607950279
10^{13}	346065536839	346065645809
10^{14}	3204941750802	3204942065690
10^{15}	29844570422669	29844571475286
10^{16}	279238341033925	279238344248555
10^{17}	2623557157654233	2623557165610820
10^{18}	24739954287740860	24739954309690413
10^{19}	234057667276344607	234057667376222382
10^{20}	2220819602560918840	2220819602783663483
10^{21}	21127269486018731928	21127269486616126182
10^{22}	201467286689315906290	201467286691248261498

The Riemann Hypothesis

- So is it really true that for any $\theta > \frac{1}{2}$ and all large x we have
$$|\pi(x) - \mathrm{li}(x)| < x^{\theta}?$$

The Riemann Hypothesis

- 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.

The Riemann Hypothesis

- So is it really true that for any $\theta > \frac{1}{2}$ and all large x we have
$$|\pi(x) - \text{li}(x)| < x^{\theta}?$$
- 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.

The Riemann Hypothesis

- 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.

Introduction

The integers

Divisibility

Prime Numbers

The fundamental theorem of arithmetic

Trial Division

Differences of Squares

The Floor Function

Introduction to Number Theory

- 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*.

Introduction to Number Theory

- 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 $\mathbb{N}$

Introduction to Number Theory

- If you subtract one member of $\mathbb{Z}$ from another, e.g.

$$173 - 192 = -19$$

you get a third.

Introduction to Number Theory

- If you subtract one member of $\mathbb{Z}$ from another, e.g.

$$173 - 192 = -19$$

  you get a third.
- But this last fails for $\mathbb{N}$.

Introduction to Number Theory

- 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.

- We start with some definitions.

- We start with some definitions.
- We need some concept of divisibility and factorization.

- We start with some definitions.
- We need some concept of divisibility and factorization.
- 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 $a|b$.

Example 1

If $a|b$ and $b|c$, then $a|c$.

- We start with some definitions.
- We need some concept of divisibility and factorization.
- 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 $a|b$.

Example 1

If $a|b$ and $b|c$, then $a|c$.

- The proof is easy.

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. $\square$

- There are some facts which are useful.

- There are some facts which are useful.
- For any a we have $0a = 0$.

- There are some facts which are useful.
- For any a we have $0a = 0$.
- If $ab = 1$, then $a = \pm 1$ and $b = \pm 1$ (with the same sign in each case).

- There are some facts which are useful.
- For any a we have $0a = 0$.
- 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 $c = d$.

Introduction

The integers

Divisibility

Prime Numbers

The fundamental theorem of arithmetic

Trial Division

Differences of Squares

The Floor Function

- Prime Number.

Definition 2

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

- Prime Number.

Definition 2

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

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

- Prime Number.

Definition 2

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

- We will use the letter p to denote a prime number.
- An example

Example 3

101 is a prime number.

- Prime Number.

Definition 2

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

- We will use the letter p to denote a prime number.
- An example

Example 3

101 is a prime number.

- **Proof** One has to check for divisors d with $1 < d < 100$.

- Prime Number.

Definition 2

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

- We will use the letter p to denote a prime number.
- An example

Example 3

101 is a prime number.

- **Proof** 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.

- Prime Number.

Definition 2

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

- We will use the letter p to denote a prime number.
- An example

Example 3

101 is a prime number.

- **Proof** 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.
- So we only need to check the primes $2, 3, 5, 7$. Moreover 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 simple proofs for facts about $\mathbb{N}$ there is one proof method which is very important.

- Since we are dealing with simple 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 it is the least member and given any $n \in \mathbb{N}$ the next member is $n + 1$. In this way one sees that $\mathbb{N}$ is *defined* inductively.

- Since we are dealing with simple 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 it is the least member and given any $n \in \mathbb{N}$ the next member is $n + 1$. In this way one sees that $\mathbb{N}$ is *defined* inductively.
- A fundamental theorem.

Theorem 4

Every member of $\mathbb{N}$ *is a product of prime numbers.*

- Since we are dealing with simple 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 it is the least member and given any $n \in \mathbb{N}$ the next member is $n + 1$. In this way one sees that $\mathbb{N}$ is *defined* inductively.
- A fundamental theorem.

Theorem 4

Every member of $\mathbb{N}$ is a product of prime numbers.

- **Proof.** This uses induction.

- Since we are dealing with simple 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 it is the least member and given any $n \in \mathbb{N}$ the next member is $n + 1$. In this way one sees that $\mathbb{N}$ is *defined* inductively.
- A fundamental theorem.

Theorem 4

Every member of $\mathbb{N}$ is a product of prime numbers.

- **Proof.** This uses induction.
- 1 is an "empty product" of primes, so case $n = 1$ holds.

- Since we are dealing with simple 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 it is the least member and given any $n \in \mathbb{N}$ the next member is $n+1$. In this way one sees that $\mathbb{N}$ is *defined* inductively.
- A fundamental theorem.

Theorem 4

Every member of $\mathbb{N}$ is a product of prime numbers.

- **Proof.** This uses induction.
- 1 is an "empty product" of primes, so case $n = 1$ holds.
- Suppose that we have proved the result for all $m \le n$. 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

Theorem 5 (*Euclid*)

There are infinitely many primes.

- We can use this to deduce

Theorem 5 (*Euclid*)

There are infinitely many primes.

- Hardy cites the proof as an example of beauty in mathematics.

- We can use this to deduce

Theorem 5 (*Euclid*)

There are infinitely many primes.

- Hardy cites the proof as an example of beauty in mathematics.
- **Proof.** We argue by contradiction. Suppose there are only a finite number of primes. Call them $p_1, p_2, \dots, p_n$ and consider the number

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

- We can use this to deduce

Theorem 5 (*Euclid*)

There are infinitely many primes.

- Hardy cites the proof as an example of beauty in mathematics.
- **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 $m > 1$.

- We can use this to deduce

Theorem 5 (*Euclid*)

There are infinitely many primes.

- Hardy cites the proof as an example of beauty in mathematics.
- **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 m is a product of primes, and in particular there is a prime p which divides m.

- We can use this to deduce

Theorem 5 (*Euclid*)

There are infinitely many primes.

- Hardy cites the proof as an example of beauty in mathematics.
- **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 m 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.

- There is a proof of the infinitude of primes which is essentially due to Euler. It is analytic in nature and quite different from Euclid's.

- There is a proof of the infinitude of primes which is essentially due to Euler. It 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.

- There is a proof of the infinitude of primes which is essentially due to Euler. It 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

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

- There is a proof of the infinitude of primes which is essentially due to Euler. It 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.

- Now consider

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

where the product is over the primes not exceeding x.

- Then $P(x) =$

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

- Now consider

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

where the product is over the primes not exceeding x.

- Then $P(x) =$

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

- Note that when one multiplies out the left hand side every fraction $\frac{1}{n}$ with $n \le x$ occurs.

- Now consider
$$P(x) = \prod_{p\le x} (1-1/p)^{-1}$$
where the product is over the primes not exceeding x.
- Then $P(x) =$
$$\prod_{p\le x}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) \ge \sum_{n\le x}\frac{1}{n} = S(x) \ge \log x.$$
- 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.

- Actually one can get something a bit more precise.

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

$$P(x) \geq \log x.$$

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

$$P(x) \ge \log x.$$

- Then

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

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

$$P(x) \ge \log x.$$

- Then

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

- Moreover the expression on the left is

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

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

$$P(x) \ge \log x.$$

- Then

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

- 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

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

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

$$P(x) \geq \log x.$$

- Then

$$-\sum_{p\leq x} \log(1-1/p) \geq \log\log x.$$

- Moreover the expression on the left is

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

- Here the terms with $k \geq 2$ contribute at most

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

- Hence we have just proved that

$$\sum_{p\leq x} \frac{1}{p} \geq \log\log x - \frac{1}{2}.$$

- Euler's result on primes is often quoted as follows.

Theorem 6 (Euler)

The sum

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

diverges.

- We now come to something very important

Theorem 7 (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 $a = dq + r, \quad 0 \le r < d$.

- We now come to something very important

Theorem 7 (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 $a = dq + r, \quad 0 \le r < d$.

- We call q the quotient and r the remainder.

- We now come to something very important

Theorem 7 (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 $a = dq + r, \quad 0 \le r < d$.

- We call q the quotient and r the remainder.
- **Proof.** Let $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.

- We now come to something very important

Theorem 7 (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 $a = dq + r, \quad 0 \le r < d$.

- We call q the quotient and r the remainder.
- **Proof.** Let $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, then $a \in \mathcal{D}$, and if $a < 0$, then $a - d(a-1) > 0$.

- We now come to something very important

Theorem 7 (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 $a = dq + r, \quad 0 \le r < d$.

- We call q the quotient and r the remainder.
- **Proof.** Let $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, 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 $a = dq + r, \quad 0 \le r$.

- We now come to something very important

Theorem 7 (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 $a = dq + r, \quad 0 \le r < d$.

- We call q the quotient and r the remainder.
- **Proof.** Let $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, 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 $a = dq + r, \quad 0 \le r$.
- Moreover if $r \ge d$, then $a = d(q+1) + (r - d)$ gives another solution, but with $0 \le r - d < r$ contradicting the minimality of r.

- We now come to something very important

Theorem 7 (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 $a = dq + r, \quad 0 \le r < d$.

- We call q the quotient and r the remainder.
- **Proof.** Let $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, 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 $a = dq + r, \quad 0 \le r$.
- Moreover if $r \ge d$, then $a = d(q+1) + (r-d)$ gives another solution, but with $0 \le r - d < r$ contradicting the minimality of r.
- Hence $r < d$ as required.

- We now come to something very important

Theorem 7 (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 $a = dq + r, \quad 0 \le r < d$.

- We call q the quotient and r the remainder.
- **Proof.** Let $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, 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 $a = dq + r, \quad 0 \le r$.
- Moreover if $r \ge d$, then $a = d(q+1) + (r-d)$ gives another solution, but with $0 \le r - d < r$ contradicting the minimality of r.
- Hence $r < d$ as required.
- For uniqueness note that a second solution $a = dq' + r'$, $0 \le r' < d$ gives $0 = a - a = (dq' + r') - (dq + r)$ $= d(q' - q) + (r' - r)$, and if $q' \ne q$, then $d \le d|q' - q| = |r' - r| < d$ which is impossible.

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

Example 8

Try dividing 17 into 192837465 by the method you were taught at primary school.

- We will make frequent use of the division algorithm, e.g.

Theorem 9

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 $c|(a,b)$.

- We will make frequent use of the division algorithm, e.g.

Theorem 9

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 $c|(a,b)$.

- GCD

Definition 10

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 $GCD(a,b)$.

- We will make frequent use of the division algorithm, e.g.

Theorem 9

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 $c|(a,b)$.

- GCD

Definition 10

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 $GCD(a,b)$.

- Note that $GCD(a,b)$ divides every member of $\mathcal{D}(a,b)$.

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.
- Likewise if $b > 0$.

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.
- Likewise if $b > 0$.
- If $a < 0$, then $a(-1) + b.0 > 0$, and again likewise if $b < 0$.

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.
- Likewise if $b > 0$.
- If $a < 0$, then $a(-1) + b.0 > 0$, and again likewise if $b < 0$.
- The remaining case $a = b = 0$ which is excluded. Thus $\mathcal{D}(a, b)$ does have positive elements and so (a, b) exists.

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.
- Likewise if $b > 0$.
- If $a < 0$, then $a(-1) + b.0 > 0$, and again likewise if $b < 0$.
- The remaining case $a = b = 0$ which is excluded. Thus $\mathcal{D}(a, b)$ does have positive elements and so (a, b) exists.
- Assume (i) false, $(a, b) \nmid a$. By the division algorithm $a = (a, b)q + r$ with $0 \le r < (a, b)$, and $(a, b) \nmid a$ implies $0 < r$.

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.
- Likewise if $b > 0$.
- If $a < 0$, then $a(-1) + b.0 > 0$, and again likewise if $b < 0$.
- The remaining case $a = b = 0$ which is excluded. Thus $\mathcal{D}(a, b)$ does have positive elements and so (a, b) exists.
- Assume (i) false, $(a, b) \nmid a$. By the division algorithm $a = (a, b)q + r$ with $0 \le r < (a, b)$, and $(a, b) \nmid a$ implies $0 < r$.
- Thus $r = a - (a, b)q = a - (ax + by)q$ for some integers x and y. Hence $r = a(1 - xq) + b(-yq)$.

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.
- Likewise if $b > 0$.
- If $a < 0$, then $a(-1) + b.0 > 0$, and again likewise if $b < 0$.
- The remaining case $a = b = 0$ which is excluded. Thus $\mathcal{D}(a, b)$ does have positive elements and so (a, b) exists.
- Assume (i) false, $(a, b) \nmid a$. By the division algorithm $a = (a, b)q + r$ with $0 \le r < (a, b)$, and $(a, b) \nmid a$ implies $0 < r$.
- 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).

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.
- Likewise if $b > 0$.
- If $a < 0$, then $a(-1) + b.0 > 0$, and again likewise if $b < 0$.
- The remaining case $a = b = 0$ which is excluded. Thus $\mathcal{D}(a, b)$ does have positive elements and so (a, b) exists.
- Assume (i) false, $(a, b) \nmid a$. By the division algorithm $a = (a, b)q + r$ with $0 \le r < (a, b)$, and $(a, b) \nmid a$ implies $0 < r$.
- 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).

- **Proof of Theorem 9.** If $a > 0$, then $a.1 + b.0 = a > 0$.
- Likewise if $b > 0$.
- If $a < 0$, then $a(-1) + b.0 > 0$, and again likewise if $b < 0$.
- The remaining case $a = b = 0$ which is excluded. Thus $\mathcal{D}(a, b)$ does have positive elements and so (a, b) exists.
- Assume (i) false, $(a, b) \nmid a$. By the division algorithm $a = (a, b)q + r$ with $0 \le r < (a, b)$, and $(a, b) \nmid a$ implies $0 < r$.
- 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.

- The GCD has some interesting properties.
- Here is one

Example 11

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 $d = 1$.

- The GCD has some interesting properties.
- Here is one

Example 11

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

Example 12

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

Example 13

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 have a corollary.

Corollary 14

Suppose that a and b are integers not both 0. Then there are integers x and y such that

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

- Following from the previous theorem we have a corollary.

Corollary 14

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.

- Following from the previous theorem we have a corollary.

Corollary 14

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

Theorem 15 (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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

- If you multiply two elements, 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 of the same kind.

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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

- If you multiply two elements, 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 of the same kind.
- We define a "prime" p in this system if it is only divisible by 1 and itself in the system.

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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

- If you multiply two elements, 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 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 $\mathcal{A}$.

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

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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

- If you multiply two elements, 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 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.

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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

- If you multiply two elements, 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 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 $\mathcal{A}$.

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

- 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.

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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

- If you multiply two elements, 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 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 $441 = 9 \times 49 = 21^2$.

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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

- If you multiply two elements, 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 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 $441 = 9 \times 49 = 21^2$.
- Wait a minute, here factorisation is not unique!

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

Example 16

Consider the set $\mathcal{A}$ of integers of the form $4k+1$.

- If you multiply two elements, 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 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 $441 = 9\times 49 = 21^2$.
- 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!

Introduction
The integers
Divisibility
Prime Numbers
The fundamental theorem of arithmetic
Trial Division
Differences of Squares
The Floor Function

- What is the difference between $\mathbb{Z}$ and $\mathcal{A}$?

- What is the difference between $\mathbb{Z}$ and $\mathcal{A}$?
- Well $\mathbb{Z}$ has an additive structure and $\mathcal{A}$ does not.

- 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.

- 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 $\mathcal{A}$.

- 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.

- 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.

- Getting back to
  Theorem 15 (Euclid). *Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.*

- Getting back to
  Theorem 15 (Euclid). *Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.*
- **Proof of Euclid's theorem.** If a or b are 0, then clearly $p|a$ or $p|b$.

- Getting back to
  Theorem 15 (Euclid). *Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.*
- **Proof of Euclid's theorem.** If a or b are 0, then clearly $p|a$ or $p|b$.
- Thus we may assume $ab \neq 0$.

- Getting back to
  Theorem 15 (Euclid). *Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.*
- **Proof of 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 $(a,p)|a$.

- Getting back to
  Theorem 15 (Euclid). *Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.*
- **Proof of 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.

- Getting back to
  Theorem 15 (Euclid). *Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.*
- **Proof of 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 $1 = ax + py$ for some x and y.

- Getting back to
  Theorem 15 (Euclid). *Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.*
- **Proof of 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 $1 = ax + py$ for some x and y.
- 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

Theorem 17

Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and

$$p \mid p_1 p_2 \ldots p_r.$$

Then $p = p_j$ for some j.

- We can use Euclid's theorem to establish the following

Theorem 17

Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and

$$p \big| p_1 p_2 \ldots p_r.$$

Then $p = p_j$ for some j.

- We can prove this by induction on r.

- We can use Euclid's theorem to establish the following

Theorem 17

Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and

$$p \big| p_1 p_2 \ldots p_r.$$

Then $p = p_j$ for some j.

- We can prove this by induction on r.
- **Proof.** The case $r = 1$ is immediate from the definition of prime.

Introduction

The integers

Divisibility

Prime Numbers

The fundamental theorem of arithmetic

Trial Division

Differences of Squares

The Floor Function

- We can use Euclid's theorem to establish the following

Theorem 17

Suppose that $p, p_1, p_2, \ldots, p_r$ *are prime numbers and*

$$p \big| p_1 p_2 \ldots p_r.$$

Then $p = p_j$ *for some* j.

- We can prove this by induction on r.
- **Proof.** The case $r = 1$ is immediate from the definition of prime.
- Suppose we have established the r-th case and that we have $p \big| p_1 p_2 \ldots p_{r+1}$.

- We can use Euclid's theorem to establish the following

Theorem 17

Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and

$$p \mid p_1 p_2 \ldots p_r.$$

Then $p = p_j$ for some j.

- We can prove this by induction on r.
- **Proof.** The case $r = 1$ is immediate from the definition of prime.
- Suppose we have established the r-th case and that we have $p \mid p_1 p_2 \ldots p_{r+1}$.
- Then by the previous theorem we have $p \mid p_{r+1}$ or $p \mid p_1 p_2 \ldots p_r$.

- We can use Euclid's theorem to establish the following

Theorem 17

Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and

$$p | p_1 p_2 \ldots p_r.$$

Then $p = p_j$ for some j.

- We can prove this by induction on r.
- **Proof.** The case $r = 1$ is immediate from the definition of prime.
- Suppose we have established the r-th case and that we have $p | p_1 p_2 \ldots p_{r+1}$.
- Then by the previous theorem we have $p | p_{r+1}$ or $p | p_1 p_2 \ldots p_r$.
- If $p | p_{r+1}$, then we must have $p = p_{r+1}$.

- We can use Euclid's theorem to establish the following

Theorem 17

Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and

$$p | p_1 p_2 \ldots p_r.$$

Then $p = p_j$ for some j.

- We can prove this by induction on r.
- **Proof.** The case $r = 1$ is immediate from the definition of prime.
- Suppose we have established the r-th case and that we have $p | p_1 p_2 \ldots p_{r+1}$.
- Then by the previous theorem we have $p | p_{r+1}$ or $p | p_1 p_2 \ldots p_r$.
- If $p | p_{r+1}$, then we must have $p = p_{r+1}$.
- If $p | p_1 p_2 \ldots p_r$, then by the inductive hypothesis we must have $p = p_j$ for some j with $1 \le j \le r$.

- We can now establish the main result of this section.

Theorem 18 (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

$$a = (\pm 1) p_1 p_2 \dots p_r$$

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

- We can now establish the main result of this section.

Theorem 18 (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

$$a = (\pm 1) p_1 p_2 \dots p_r$$

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

- Note that we can even write

$$a = (\pm 1) p_1 p_2 \dots p_r$$

when $a = \pm 1$ by interpreting the product over primes as an empty product in that case.

- **Proof of Theorem 17.** Clearly we may suppose that $a > 0$ and hence $a \geq 2$.

- **Proof of Theorem 17.** Clearly we may suppose that $a > 0$ and hence $a \geq 2$.

- **Proof of Theorem 17.** Clearly we may suppose that $a > 0$ and hence $a \geq 2$.
- Theorem 4 tells us that a will be a product of r primes, say $a = p_1 p_2 \dots p_r$ with $r \geq 1$. It remains to prove uniqueness.

- **Proof of Theorem 17.** Clearly we may suppose that $a > 0$ and hence $a \geq 2$.
- Theorem 4 tells us that a will be a product of r primes, say $a = p_1 p_2 \dots p_r$ with $r \geq 1$. It remains to prove uniqueness.
- We prove that by induction on r.

- **Proof of Theorem 17.** Clearly we may suppose that $a > 0$ and hence $a \geq 2$.
- Theorem 4 tells us that a will be a product of r primes, say $a = p_1 p_2 \dots p_r$ 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 $a = p'_1 \dots p'_s$ where $s \geq 1$.

- **Proof of Theorem 17.** Clearly we may suppose that $a > 0$ and hence $a \geq 2$.
- Theorem 4 tells us that a will be a product of r primes, say $a = p_1 p_2 \ldots p_r$ 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.

- **Proof of Theorem 17.** Clearly we may suppose that $a > 0$ and hence $a \geq 2$.
- Theorem 4 tells us that a will be a product of r primes, say $a = p_1 p_2 \ldots p_r$ 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

$$a = p_1 p_2 \ldots p_{r+1} = p'_1 \ldots p'_s.$$

- **Proof of Theorem 17.** Clearly we may suppose that $a > 0$ and hence $a \geq 2$.
- Theorem 4 tells us that a will be a product of r primes, say $a = p_1 p_2 \ldots p_r$ 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

$$a = p_1 p_2 \ldots p_{r+1} = p_1' \ldots p_s'.$$

- Then we see from the previous theorem that $p_1' = p_j$ for some j and then

$$p_2' \ldots p_s' = p_1 p_2 \ldots p_{r+1} / p_j$$

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

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

- 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.

- 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.

- For example if $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, then

$$20 = p_1^2 p_2^0 p_3^1,\ 75 = p_1^0 p_2^1 p_3^2,\ (20, 75) = 5 = p_1^0 p_2^0, p_3^1.$$

- 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.

- For example if $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, then

$$20 = p_1^2 p_2^0 p_3^1,\ 75 = p_1^0 p_2^1 p_3^2,\ (20, 75) = 5 = p_1^0 p_2^0, p_3^1.$$

- Then it can be checked easily that

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

- We can now introduce the idea of least common multiple

Definition 19

We can also introduce here the *least common multiple* LCM

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

and this could also be defined by

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

- We can now introduce the idea of least common multiple

Definition 19

We can also introduce here the *least common multiple* LCM

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

and this could also be defined by

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

- The $LCM[a, b]$ 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

Definition 20

A composite number is a number $n \in \mathbb{N}$ with $n > 1$ which is not prime. In particular a composite number n can be written

$$n = m_1 m_2$$

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

- As I hope was clear from the example 101 the simplest way to try to factorize a number n is by 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 $m_1 \leq m_2$.

- 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 $m_1 \le m_2$.
- Thus $m_1^2 \le m_1 m_2 = n$ and

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

- 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 $m_1 \le m_2$.
- Thus $m_1^2 \le m_1 m_2 = n$ and

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

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

- 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 $m_1 \le m_2$.
- Thus $m_1^2 \le m_1 m_2 = n$ and

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

- Hence we can try each $m_1 \le \sqrt{n}$ 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

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

- 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 $m_1 \le m_2$.
- Thus $m_1^2 \le m_1 m_2 = n$ and
$$m_1 \le \sqrt{n}.$$
- Hence we can try each $m_1 \le \sqrt{n}$ 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
$$2 \le p \le \sqrt{n}.$$
- 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.

- The number $\pi(x)$ of primes $p \le x$ 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

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

- The number $\pi(x)$ of primes $p \le x$ 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.

- The number $\pi(x)$ of primes $p \le x$ 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 $\pi(x)$.

- 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.

- 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 $x \le 10^{27}$ 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 mutliples.

- 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

- 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.

- 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 $p \leq 100$.

- 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.

- 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.
- By counting the entries that remain one finds that $\pi(100) = 25$.

- The sieve of Eratosthenes produces approximately

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

numbers in about

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

operations.

- The sieve of Eratosthenes produces approximately

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

numbers in about

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

operations.

- Another big constraint is storage.

Factorization and Primality Testing Chapter 1 Background

Robert C. Vaughan

Introduction

The integers

Divisibility

Prime Numbers

The fundamental theorem of arithmetic

Trial Division

Differences of Squares

The Floor Function

- Here is an idea that goes back to Fermat.

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

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

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

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

- Since the polynomial on the right factorises as

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

maybe we have a way of factoring n.

- Here is an idea that goes back to Fermat.
- Given n suppose we can find x and y so that
$$n = x^2 - y^2, \quad 0 \le y < x.$$
- 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.

- Here is an idea that goes back to Fermat.
- Given n suppose we can find x and y so that
$$n = x^2 - y^2, \quad 0 \le y < x.$$
- 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.

- Here is an idea that goes back to Fermat.
- Given n suppose we can find x and y so that
$$n = x^2 - y^2, \quad 0 \le y < x.$$
- 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.

- If $n = m_1 m_2$ with n odd and $m_1 \le m_2$, then m_1 and m_2 are both odd and there is a solution with

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

- If $n = m_1 m_2$ with n odd and $m_1 \le m_2$, then m_1 and m_2 are both odd and there is a solution with

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

- A simple example

Example 21

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

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

- 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

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

- A simple example

Example 21

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

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

- Another

Example 22

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

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

- 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.

- 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.

- 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.

- 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.

- 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.
- 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.

- 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.
- 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.

- To illustrate this consider

Example 23

Let $n = 10001$. Then

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

Now

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

- To illustrate this consider

Example 23

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.

- To illustrate this consider

Example 23

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

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

in the variables k, s, y.

- There is a function which we will use from time to time. This is 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.

Definition 24

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 $x \le u$. The difference $x - \lfloor x\rfloor$ is often called **the fractional part** of x and is sometimes denoted by $\{x\}$.

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

Definition 24

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 $x \le u$. The difference $x - \lfloor x \rfloor$ is often called **the fractional part** of x and is sometimes denoted by $\{x\}$.

- By the way of illustration.

Example 25

$\lfloor \pi \rfloor = 3$, $\lceil \pi \rceil = 4$, $\lfloor \sqrt{2} \rfloor = 1$, $\lfloor -\sqrt{2} \rfloor = -2$, $\lceil -\sqrt{2} \rceil = -1$.

- The floor function has some useful properties.

Theorem 26 (Properties of the floor function)

(i) For any $x \in \mathbb{R}$ we have $0 \le x - \lfloor x \rfloor < 1$.
(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 $x, y \in \mathbb{R}$, $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.

- The floor function has some useful properties.

Theorem 26 (Properties of the floor function)

(i) For any $x \in \mathbb{R}$ *we have* $0 \le x - \lfloor x \rfloor < 1$.
(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 $x, y \in \mathbb{R}$, $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.

- **Proof.** (i) We argue by contradiction.

- The floor function has some useful properties.

Theorem 26 (Properties of the floor function)

(i) For any $x \in \mathbb{R}$ we have $0 \le x - \lfloor x \rfloor < 1$.
(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 $x, y \in \mathbb{R}$, $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.

- **Proof.** (i) We argue by contradiction.
- If $x - \lfloor x \rfloor < 0$, then $x < \lfloor x \rfloor$ contradicting the definition.

- The floor function has some useful properties.

Theorem 26 (Properties of the floor function)

(i) For any $x \in \mathbb{R}$ *we have* $0 \le x - \lfloor x \rfloor < 1$.
(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 $x, y \in \mathbb{R}$, $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.

- **Proof.** (i) We argue by contradiction.
- If $x - \lfloor x \rfloor < 0$, then $x < \lfloor x \rfloor$ contradicting the definition.
- If $1 \le x - \lfloor x \rfloor$, then $1 + \lfloor x \rfloor \le x$ contradicting defn.

- The floor function has some useful properties.

Theorem 26 (Properties of the floor function)

(i) For any $x \in \mathbb{R}$ we have $0 \le x - \lfloor x \rfloor < 1$.
(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 $x, y \in \mathbb{R}$, $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.

- **Proof.** (i) We argue by contradiction.
- If $x - \lfloor x \rfloor < 0$, then $x < \lfloor x \rfloor$ contradicting the definition.
- If $1 \le x - \lfloor x \rfloor$, then $1 + \lfloor x \rfloor \le x$ contradicting defn.
- This also shows that $\lfloor x \rfloor$ is unique.

- The floor function has some useful properties.

Theorem 26 (Properties of the floor function)

(i) For any $x \in \mathbb{R}$ *we have* $0 \le x - \lfloor x \rfloor < 1$.
(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 $x, y \in \mathbb{R}$, $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.

- **Proof.** (i) We argue by contradiction.
- If $x - \lfloor x \rfloor < 0$, then $x < \lfloor x \rfloor$ contradicting the definition.
- If $1 \le x - \lfloor x \rfloor$, then $1 + \lfloor x \rfloor \le x$ contradicting defn.
- This also shows that $\lfloor x \rfloor$ is unique.
- (ii) One way to see this is to observe that by (i) we have $x = \lfloor x \rfloor + \theta$ for some θ with $0 \le \theta < 1$.

- The floor function has some useful properties.

Theorem 26 (Properties of the floor function)

(i) For any $x \in \mathbb{R}$ *we have* $0 \le x - \lfloor x \rfloor < 1$.
(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 $x, y \in \mathbb{R}$, $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.

- **Proof.** (i) We argue by contradiction.
- If $x - \lfloor x \rfloor < 0$, then $x < \lfloor x \rfloor$ contradicting the definition.
- If $1 \le x - \lfloor x \rfloor$, then $1 + \lfloor x \rfloor \le x$ contradicting defn.
- This also shows that $\lfloor x \rfloor$ is unique.
- (ii) One way to see this is to observe that by (i) we have $x = \lfloor x \rfloor + \theta$ for some θ with $0 \le \theta < 1$.
- Then $x + k - \lfloor x \rfloor - k = \theta$ and since there is only one integer l with $0 \le x + k - l < 1$, and this l is $\lfloor x + k \rfloor$ we must have $\lfloor x + k \rfloor = \lfloor x \rfloor + k$.

- **Theorem 26.** (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 $x, y \in \mathbb{R}$,
  $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.

- **Theorem 26.** (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 $x, y \in \mathbb{R}$,
  $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.
- **Proof continued.** (iii) We know by (i) that $\theta = x/n - \lfloor x/n \rfloor$ satisfies $0 \le \theta < 1$.

- **Theorem 26.** (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 $x, y \in \mathbb{R}$,
  $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.
- **Proof continued.** (iii) We know by (i) that $\theta = x/n - \lfloor x/n \rfloor$ satisfies $0 \le \theta < 1$.
- Now $x = n\lfloor x/n \rfloor + n\theta$ and so by (ii) $\lfloor x \rfloor = n\lfloor x/n \rfloor + \lfloor n\theta \rfloor$.

- **Theorem 26.** (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 $x, y \in \mathbb{R}$,
  $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.
- **Proof continued.** (iii) We know by (i) that $\theta = x/n - \lfloor x/n \rfloor$ satisfies $0 \le \theta < 1$.
- 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 $\lfloor x/n \rfloor \le \lfloor x \rfloor / n < \lfloor x/n \rfloor + 1$ and so $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$.

- **Theorem 26.** (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 $x, y \in \mathbb{R}$,
  $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.
- **Proof continued.** (iii) We know by (i) that $\theta = x/n - \lfloor x/n \rfloor$ satisfies $0 \le \theta < 1$.
- 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 $\lfloor x/n \rfloor \le \lfloor x \rfloor / n < \lfloor x/n \rfloor + 1$ and so $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$.
- (iv) Put $x = \lfloor x \rfloor + \theta$ and $y = \lfloor y \rfloor + \phi$ where $0 \le \theta, \phi < 1$.

- **Theorem 26.** (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 $x, y \in \mathbb{R}$,
  $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor \le \lfloor x \rfloor + \lfloor y \rfloor + 1$.
- **Proof continued.** (iii) We know by (i) that $\theta = x/n - \lfloor x/n \rfloor$ satisfies $0 \le \theta < 1$.
- 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 $\lfloor x/n \rfloor \le \lfloor x \rfloor / n < \lfloor x/n \rfloor + 1$ and so $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$.
- (iv) Put $x = \lfloor x \rfloor + \theta$ and $y = \lfloor y \rfloor + \phi$ where $0 \le \theta, \phi < 1$.
- Then $\lfloor x + y \rfloor = \lfloor \theta + \phi \rfloor + \lfloor x \rfloor + \lfloor y \rfloor$ and $0 \le \theta + \phi < 2$.