Factorization and Primality Testing Chapter 5 Quadratic Residues

Robert C. Vaughan

October 11, 2023

Quadratic Congruences

- Our long term aim is to facotorize n by finding t, x, y so that $4tn = x^2 - y^2$.

Quadratic Congruences

- Our long term aim is to facotorize n by finding t, x, y so that $4tn = x^2 - y^2$.
- An essential ingredient will be a good understanding of quadratic congruences, and especially

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

Quadratic Congruences

- Our long term aim is to facotorize n by finding t, x, y so that $4tn = x^2 - y^2$.
- An essential ingredient will be a good understanding of 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.

Quadratic Congruences

- Our long term aim is to facotorize n by finding t, x, y so that $4tn = x^2 - y^2$.
- An essential ingredient will be a good understanding of 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,

Quadratic Congruences

- Our long term aim is to facotorize n by finding t, x, y so that $4tn = x^2 - y^2$.
- An essential ingredient will be a good understanding of 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

$$x^2 \equiv c \pmod{p}. \tag{1.1}$$

- Then we are interested in
$$x^2 \equiv c \pmod{p}. \tag{1.1}$$
- 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
$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

- Then we are interested in

$$x^2 \equiv c \pmod{p}. \tag{1.1}$$

- 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

$$x^2 \equiv b^2 - 4ac \pmod{p},$$

- Then we are interested in

$$x^2 \equiv c \pmod{p}. \tag{1.1}$$

- 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 (1.1).

- We know that (1.1)

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

has at most two solutions,

- We know that (1.1)

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

  has at most two solutions,
- and that sometimes it is soluble and sometimes not.

Example 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

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

- We know that (1.1)

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

has at most two solutions,

- and that sometimes it is soluble and sometimes not.

Example 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 (1.1) is $x \equiv 0 \pmod{p}$ (note that $p|x^2$ implies that $p|x$).

- We know that (1.1)

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

  has at most two solutions,
- and that sometimes it is soluble and sometimes not.

Example 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 (1.1) 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 (1.1)

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

is soluble?

- The fundamental question here is can we characterise or classify those c for which the congruence (1.1)

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

  is soluble?
- Better still can we quickly determine, given c, whether it is soluble?

- The fundamental question here is can we characterise or classify those c for which the congruence (1.1)

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

is soluble?

- Better still can we quickly determine, given c, whether it is soluble?
- There is then the even more difficult question of finding a solution.

- Important

Definition 2

If $c \not\equiv 0 \pmod{p}$, and (1.1) 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.

- Important

Definition 2

If $c \not\equiv 0 \pmod{p}$, and (1.1) 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.

- Important

Definition 2

If $c \not\equiv 0 \pmod{p}$, and (1.1) 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 prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. 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 quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- Now we prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. 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 quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- **Proof.** Suppose that $1 \le x < y \le \frac{1}{2}(p-1)$.

- Now we prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. 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 quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- **Proof.** Suppose that $1 \le x < y \le \frac{1}{2}(p-1)$.
- If $p | y^2 - x^2 = (y-x)(y+x)$, then $p | y - x$ or $p | y + x$.

- Now we prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. The numbers $1, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$ are distinct modulo p and give a complete set of quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- **Proof.** Suppose that $1 \le x < y \le \frac{1}{2}(p-1)$.
- If $p|y^2 - x^2 = (y-x)(y+x)$, then $p|y-x$ or $p|y+x$.
- But $0 < y - x < y + x < 2y \le p - 1 < p$ so the numbers in the list above are distinct modulo p.

- Now we prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. 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 quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- **Proof.** Suppose that $1 \le x < y \le \frac{1}{2}(p-1)$.
- If $p|y^2 - x^2 = (y-x)(y+x)$, then $p|y-x$ or $p|y+x$.
- But $0 < y - x < y + x < 2y \le p - 1 < p$ so the numbers in the list above are distinct modulo p.
- Suppose that c is a QR modulo p. Then there is an x with $1 \le x \le p-1$ such that $x^2 \equiv c \pmod{p}$.

- Now we prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. 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 quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- **Proof.** Suppose that $1 \le x < y \le \frac{1}{2}(p-1)$.
- If $p|y^2 - x^2 = (y-x)(y+x)$, then $p|y-x$ or $p|y+x$.
- But $0 < y - x < y + x < 2y \le p - 1 < p$ so the numbers in the list above are distinct modulo p.
- Suppose that c is a QR modulo p. Then there is an x with $1 \le x \le p-1$ such that $x^2 \equiv c \pmod{p}$.
- If $x \le \frac{1}{2}(p-1)$, then x^2 is in our list and represents c.

- Now we prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. The numbers $1, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$ are distinct modulo p and give a complete set of quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- **Proof.** Suppose that $1 \le x < y \le \frac{1}{2}(p-1)$.
- If $p | y^2 - x^2 = (y-x)(y+x)$, then $p | y - x$ or $p | y + x$.
- But $0 < y - x < y + x < 2y \le p - 1 < p$ so the numbers in the list above are distinct modulo p.
- Suppose that c is a QR modulo p. Then there is an x with $1 \le x \le p-1$ such that $x^2 \equiv c \pmod{p}$.
- If $x \le \frac{1}{2}(p-1)$, then x^2 is in our list and represents c.
- If $\frac{1}{2}(p-1) < x \le p-1$, then $(p-x)^2 \equiv x^2 \equiv c \pmod{p}$, $(p-x)^2$ represents c, and is in our list.

- Now we prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. 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 quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- **Proof.** Suppose that $1 \le x < y \le \frac{1}{2}(p-1)$.
- If $p | y^2 - x^2 = (y-x)(y+x)$, then $p | y-x$ or $p | y+x$.
- But $0 < y-x < y+x < 2y \le p-1 < p$ so the numbers in the list above are distinct modulo p.
- Suppose that c is a QR modulo p. Then there is an x with $1 \le x \le p-1$ such that $x^2 \equiv c \pmod{p}$.
- If $x \le \frac{1}{2}(p-1)$, then x^2 is in our list and represents c.
- If $\frac{1}{2}(p-1) < x \le p-1$, then $(p-x)^2 \equiv x^2 \equiv c \pmod{p}$, $(p-x)^2$ represents c, and is in our list.
- So each QR is listed and there are exactly $\frac{1}{2}(p-1)$ QR.

- Now we prove the following simple but useful theorem.

Theorem 3

Let p be an odd prime. 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 quadratic residues modulo p. There are exactly $\frac{1}{2}(p-1)$ QR modulo p and exactly $\frac{1}{2}(p-1)$ QNR.

- **Proof.** Suppose that $1 \le x < y \le \frac{1}{2}(p-1)$.
- If $p | y^2 - x^2 = (y-x)(y+x)$, then $p | y - x$ or $p | y + x$.
- But $0 < y - x < y + x < 2y \le p - 1 < p$ so the numbers in the list above are distinct modulo p.
- Suppose that c is a QR modulo p. Then there is an x with $1 \le x \le p - 1$ such that $x^2 \equiv c \pmod{p}$.
- If $x \le \frac{1}{2}(p-1)$, then x^2 is in our list and represents c.
- If $\frac{1}{2}(p-1) < x \le p - 1$, then $(p-x)^2 \equiv x^2 \equiv c \pmod{p}$, $(p-x)^2$ represents c, and is in our list.
- So each QR is listed and there are exactly $\frac{1}{2}(p-1)$ QR.
- The remaining $\frac{1}{2}(p-1)$ non-zero residues have to be QNR.

- We can use this in various ways.

Example 4

Find a complete set of quadratic residues r modulo 19 with $1 \leq r \leq 18$.

- We can use this in various ways.

Example 4

Find a complete set of quadratic residues r modulo 19 with $1 \le r \le 18$.

- 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 modulo 19

- We can use this in various ways.

Example 4

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 modulo 19
- and then reduce them modulo 19 to give

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

- which we can rearrange as

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

- We require the following definition.

Definition 5

Given a prime $p > 2$ and $c \in \mathbb{Z}$ we define the *Legendre symbol*

$$\left(\frac{c}{p}\right)_L = \begin{cases} 0 & c \equiv 0 \pmod{p}, \\ 1 & c \text{ a QR } \pmod{p}, \\ -1 & c \text{ a QNR } \pmod{p}, \end{cases} \tag{1.2}$$

- We require the following definition.

Definition 5

Given a prime $p > 2$ and $c \in \mathbb{Z}$ we define the *Legendre symbol*

$$\left(\frac{c}{p}\right)_L = \begin{cases} 0 & c \equiv 0 \pmod{p}, \\ 1 & c \text{ a QR } \pmod{p}, \\ -1 & c \text{ a QNR } \pmod{p}, \end{cases} \tag{1.2}$$

- The Legendre symbol has lots of interesting properties.

Example 6

The Legendre symbol has the same value on replacing c by $c + kp$. Thus given p it is periodic in c with period p.

- Cancellation

Example 7

Suppose that p is an odd prime and $a \not\equiv 0 \pmod{p}$. Then

$$\sum_{x=1}^{p} \left(\frac{ax+b}{p}\right)_L = 0. \tag{1.3}$$

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.

- Counting solutions

Example 8

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 on more complicated congruences.

Example 9

Let $N(p;c)$ be the number of x, y with $x^2+y^2 \equiv c \pmod{p}$. Rewrite this as $z+w \equiv c \pmod{p}$ and count the number of x, y with $x^2 \equiv z \pmod{p}$ and $y^2 \equiv w \pmod{p}$. This is

$$\left(1+\left(\tfrac{z}{p}\right)_L\right)\left(1+\left(\tfrac{w}{p}\right)_L\right).$$

Also $w \equiv c-z \pmod{p}$, thus the total number of solutions is

$$\begin{aligned} N(p;c) &= \sum_{z=1}^{p}\left(1+\left(\tfrac{z}{p}\right)_L\right)\left(1+\left(\tfrac{c-z}{p}\right)_L\right) \\ &= p+\sum_{z=1}^{p}\left(\tfrac{z}{p}\right)_L+\sum_{z=1}^{p}\left(\tfrac{c-z}{p}\right)_L+\sum_{z=1}^{p}\left(\tfrac{z}{p}\right)_L\left(\tfrac{c-z}{p}\right)_L. \end{aligned}$$

The two sums are 0, so $N(p;c) = p+\sum_{z=1}^{p}\left(\frac{z}{p}\right)_L\left(\frac{c-z}{p}\right)_L$. The last sum can be evaluated, but we need to know more.

- We can combine the definition of the Legendre symbol with a criterion first enunciated by Euler.

Theorem 10 (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.

- We can combine the definition of the Legendre symbol with a criterion first enunciated by Euler.

Theorem 10 (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.

- Reminder

Remark 1

Recall that 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.

- Important

Remark 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.

- **Theorem 10.** Suppose p is an odd number. Then
$$\left(\frac{c}{p}\right)_L \equiv c^{\frac{p-1}{2}} \pmod{p}$$
and the Legendre symbol is totally multiplicative.

- **Theorem 10.** Suppose p is an odd number. Then
$$\left(\frac{c}{p}\right)_L \equiv c^{\frac{p-1}{2}} \pmod{p}$$
and the Legendre symbol is totally multiplicative.
- If c is a QR, then there is an $x \not\equiv 0 \pmod{p}$ such that $x^2 \equiv c \pmod{p}$.

- **Theorem 10.** Suppose p is an odd number. Then
$$\left(\frac{c}{p}\right)_L \equiv c^{\frac{p-1}{2}} \pmod{p}$$
and the Legendre symbol is totally multiplicative.
- If c is a QR, then there is an $x \not\equiv 0 \pmod{p}$ such that $x^2 \equiv c \pmod{p}$.
- Hence $c^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 = \left(\frac{c}{p}\right)_L \pmod{p}$.

- **Theorem 10.** Suppose p is an odd number. Then
$$\left(\frac{c}{p}\right)_L \equiv c^{\frac{p-1}{2}} \pmod{p}$$
and the Legendre symbol is totally multiplicative.
- If c is a QR, 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.

- **Theorem 10.** Suppose p is an odd number. Then
$$\left(\frac{c}{p}\right)_L \equiv c^{\frac{p-1}{2}} \pmod{p}$$
and the Legendre symbol is totally multiplicative.
- If c is a QR, 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 $c^{\frac{p-1}{2}} - 1$.

- **Theorem 10.** Suppose p is an odd number. Then
$$\left(\frac{c}{p}\right)_L \equiv c^{\frac{p-1}{2}} \pmod{p}$$
and the Legendre symbol is totally multiplicative.
- If c is a QR, 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 $c^{\frac{p-1}{2}} \equiv -1 = \left(\frac{c}{p}\right)_L \pmod{p}$.

- **Theorem 10.** Suppose p is an odd number. Then
$$\left(\frac{c}{p}\right)_L \equiv c^{\frac{p-1}{2}} \pmod p$$
and the Legendre symbol is totally multiplicative.
- If c is a QR, 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

$$\left(\frac{c_1 c_2}{p}\right)_L = \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$

- To prove the second part, we have to show that for any integers c_1, c_2 we have
$$\left(\frac{c_1c_2}{p}\right)_L = \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$
- If $c_1 \equiv 0 \pmod p$ or $c_2 \equiv 0 \pmod p$, then both sides are 0, so we can suppose that $c_1c_2 \not\equiv 0 \pmod p$.

- To prove the second part, we have to show that for any integers c_1, c_2 we have
$$\left(\frac{c_1c_2}{p}\right)_L = \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$
- If $c_1 \equiv 0 \pmod p$ or $c_2 \equiv 0 \pmod p$, then both sides are 0, so we can suppose that $c_1c_2 \not\equiv 0 \pmod p$.
- Now
$$\begin{aligned}\left(\frac{c_1c_2}{p}\right)_L &\equiv (c_1c_2)^{\frac{p-1}{2}}\\ &\equiv c_1^{\frac{p-1}{2}}c_2^{\frac{p-1}{2}}\\ &\equiv \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L \pmod p.\end{aligned}$$

- To prove the second part, we have to show that for any integers c_1, c_2 we have
$$\left(\frac{c_1c_2}{p}\right)_L = \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$
- If $c_1 \equiv 0 \pmod{p}$ or $c_2 \equiv 0 \pmod{p}$, then both sides are 0, so we can suppose that $c_1c_2 \not\equiv 0 \pmod{p}$.
- Now
$$\begin{aligned}\left(\frac{c_1c_2}{p}\right)_L &\equiv (c_1c_2)^{\frac{p-1}{2}}\\ &\equiv c_1^{\frac{p-1}{2}} c_2^{\frac{p-1}{2}}\\ &\equiv \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L \pmod{p}.\end{aligned}$$
- Thus p divides
$$\left(\frac{c_1c_2}{p}\right)_L - \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$

- To prove the second part, we have to show that for any integers c_1, c_2 we have
$$\left(\frac{c_1c_2}{p}\right)_L = \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$
- If $c_1 \equiv 0 \pmod p$ or $c_2 \equiv 0 \pmod p$, then both sides are 0, so we can suppose that $c_1c_2 \not\equiv 0 \pmod p$.
- Now
$$\begin{aligned}\left(\frac{c_1c_2}{p}\right)_L &\equiv (c_1c_2)^{\frac{p-1}{2}}\\ &\equiv c_1^{\frac{p-1}{2}} c_2^{\frac{p-1}{2}}\\ &\equiv \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L \pmod p.\end{aligned}$$
- Thus p divides
$$\left(\frac{c_1c_2}{p}\right)_L - \left(\frac{c_1}{p}\right)_L \left(\frac{c_2}{p}\right)_L.$$
- But this is $-2, 0$ or 2 and so has to be 0 since $p > 2$

- We can use the Criterion to evaluate the Legendre symbol.

Example 11

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.

- We can use the Criterion to evaluate the Legendre symbol.

Example 11

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.

- We can use the Criterion to evaluate the Legendre symbol.

Example 11

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 $p > 2$ dividing $x^2 + 1$ satisfies $p \equiv 1 \pmod 4$.

- We can use the Criterion to evaluate the Legendre symbol.

Example 11

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 $p > 2$ dividing $x^2 + 1$ satisfies $p \equiv 1 \pmod 4$.
- 2. There are infinitely many primes of the form $4k + 1$.

- We can use the Criterion to evaluate the Legendre symbol.

Example 11

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 $p > 2$ dividing $x^2 + 1$ satisfies $p \equiv 1 \pmod 4$.
- 2. There are infinitely many primes of the form $4k + 1$.
- To see 1. observe that for any such prime factor -1 has to be a quadratic residue, so its Legendre symbol is 1.

- We can use the Criterion to evaluate the Legendre symbol.

Example 11

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 $p > 2$ dividing $x^2 + 1$ satisfies $p \equiv 1 \pmod 4$.
- 2. There are infinitely many primes of the form $4k + 1$.
- To see 1. 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 assuming there are only finitely many and take x to be twice their product.

- A famous question, first asked by I. M. Vinogradov in 1919, concerns the size $n_2(p)$ of the *least* positive QNR modulo p.

- 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.

- 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.
- Vinogradov 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!

- 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.
- Vinogradov 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 $\varepsilon > \frac{1}{4\sqrt{e}}$.

- 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.
- Vinogradov 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?

- 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.
- Vinogradov 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.

Theorem 12

Suppose that p is an odd prime. Then

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- Here is an easier result.

Theorem 12

Suppose that p is an odd prime. Then

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- **Proof.** Let k be the smallest k such that $p < kn_2(p)$.

- Here is an easier result.

Theorem 12

Suppose that p is an odd prime. Then

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- **Proof.** Let k be the smallest k such that $p < kn_2(p)$.
- $n_2(p)$ cannot divide p so $p < kn_2(p) < p + n_2(p)$.

- Here is an easier result.

Theorem 12

Suppose that p is an odd prime. Then

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- **Proof.** Let k be the smallest k such that $p < kn_2(p)$.
- $n_2(p)$ cannot divide p so $p < kn_2(p) < p + n_2(p)$.
- Thus $kn_2(p)$ is a QR, and so k is a QNR.

- Here is an easier result.

Theorem 12

Suppose that p is an odd prime. Then

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- **Proof.** Let k be the smallest k such that $p < kn_2(p)$.
- $n_2(p)$ cannot divide p so $p < kn_2(p) < p + n_2(p)$.
- Thus $kn_2(p)$ is a QR, and so k is a QNR.
- Therefore $n_2(p) \le k$.

- Here is an easier result.

Theorem 12

Suppose that p is an odd prime. Then

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- **Proof.** Let k be the smallest k such that $p < kn_2(p)$.
- $n_2(p)$ cannot divide p so $p < kn_2(p) < p + n_2(p)$.
- Thus $kn_2(p)$ is a QR, and so k is a QNR.
- Therefore $n_2(p) \le k$.
- Hence $n_2(p)^2 \le p + n_2(p) - 1$.

- Here is an easier result.

Theorem 12

Suppose that p is an odd prime. Then

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- **Proof.** Let k be the smallest k such that $p < kn_2(p)$.
- $n_2(p)$ cannot divide p so $p < kn_2(p) < p + n_2(p)$.
- Thus $kn_2(p)$ is a QR, and so k is a QNR.
- Therefore $n_2(p) \le k$.
- Hence $n_2(p)^2 \le p + n_2(p) - 1$.
- This can be rearranged as $n_2(p)^2 - n_2(p) \le p - 1$, so $(n_2(p) - \frac{1}{2})^2 \le p - \frac{3}{4}$.

- Here is an easier result.

Theorem 12

Suppose that p is an odd prime. Then

$$n_2(p) \le \frac{1}{2} + \sqrt{p - \frac{3}{4}}.$$

- **Proof.** Let k be the smallest k such that $p < kn_2(p)$.
- $n_2(p)$ cannot divide p so $p < kn_2(p) < p + n_2(p)$.
- Thus $kn_2(p)$ is a QR, and so k is a QNR.
- Therefore $n_2(p) \le k$.
- Hence $n_2(p)^2 \le p + n_2(p) - 1$.
- This can be rearranged as $n_2(p)^2 - n_2(p) \le p - 1$, so $(n_2(p) - \frac{1}{2})^2 \le p - \frac{3}{4}$.
- 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.

- 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.

- 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 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.

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.

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.

- Here is a table of values of $(q|p)_L$ for primes out to 29

Example 13

.

$p\backslash q$	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

- Here is a table of values of $(q|p)_L$ for primes out to 29

Example 13

.

$p\backslash q$	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

- 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.

- Gauss was fascinated by this and eventually found at least seven (!) different proofs.
- The first step in many of them is Gauss' Lemma.

Theorem 14 (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 $ax=q_xp+r_x$ 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

$$m\equiv\sum_{1\le x<p/2}\left\lfloor\frac{2ax}{p}\right\rfloor \pmod 2.$$

- Gauss was fascinated by this and eventually found at least seven (!) different proofs.
- The first step in many of them is Gauss' Lemma.

Theorem 14 (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.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.

Example 15

Take $a = 2$.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.

Example 15

Take $a = 2$.

- Consider the numbers $2x$ with $1 \le x < \frac{1}{2}p$. They satisfy $2 \le 2x < p$ and are their own remainder, so we need to count the x with $\frac{1}{2}p < 2x < p$, that is $\frac{1}{4}p < x < \frac{1}{2}p$.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.

Example 15

Take $a = 2$.

- Consider the numbers $2x$ with $1 \le x < \frac{1}{2}p$. They satisfy $2 \le 2x < p$ and are their own remainder, so we need to count the 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 $m = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor$.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\dfrac{a}{p}\right)_L = (-1)^m$, $m \equiv \displaystyle\sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.

Example 15

Take $a = 2$.

- Consider the numbers $2x$ with $1 \le x < \frac{1}{2}p$. They satisfy $2 \le 2x < p$ and are their own remainder, so we need to count the 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 $p = 8k + 7$, $m = 2k + 2$ is also even.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.

Example 15

Take $a = 2$.

- Consider the numbers $2x$ with $1 \le x < \frac{1}{2}p$. They satisfy $2 \le 2x < p$ and are their own remainder, so we need to count the 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 $p = 8k + 7$, $m = 2k + 2$ is also even.
- Similarly if $p \equiv 3$ or $5 \pmod 8$, then m is odd.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.

Example 15

Take $a = 2$.

- Consider the numbers $2x$ with $1 \le x < \frac{1}{2}p$. They satisfy $2 \le 2x < p$ and are their own remainder, so we need to count the 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 $p = 8k + 7$, $m = 2k + 2$ is also even.
- Similarly if $p \equiv 3$ or $5 \pmod 8$, then m is odd.
- $\left(\frac{2}{p}\right)_L = \pm 1$ according as $p \equiv \pm 1$ or $\pm 3 \pmod 8$.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.

Example 15

Take $a = 2$.

- Consider the numbers $2x$ with $1 \le x < \frac{1}{2}p$. They satisfy $2 \le 2x < p$ and are their own remainder, so we need to count the 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 $p = 8k + 7$, $m = 2k + 2$ is also even.
- Similarly if $p \equiv 3$ or $5 \pmod 8$, then m is odd.
- $\left(\frac{2}{p}\right)_L = \pm 1$ according as $p \equiv \pm 1$ or $\pm 3 \pmod 8$.
- Alternatively $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}$.

- **Theorem 14.** Suppose $p>2$ and $p\nmid a$. Write each of the numbers ax with $1\le x<\frac12 p$ as $ax=q_xp+r_x$ with $0\le r_x<p$. Let m be the number of r_x with $\frac12 p<r_x<p$. Then $\left(\frac{a}{p}\right)_L=(-1)^m$, $m\equiv \sum_{1\le x<p/2}\left\lfloor\frac{2ax}{p}\right\rfloor \pmod 2$.

- **Theorem 14.** Suppose $p>2$ and $p\nmid a$. Write each of the numbers ax with $1\le x<\frac12 p$ as $ax=q_xp+r_x$ with $0\le r_x<p$. Let m be the number of r_x with $\frac12 p<r_x<p$. Then $\left(\frac{a}{p}\right)_L=(-1)^m$, $m\equiv\sum_{1\le x<p/2}\left\lfloor\frac{2ax}{p}\right\rfloor \pmod 2$.
- **Proof.** The proof is a counting argument. Consider

$$a^{\frac{p-1}{2}}\prod_{1\le x<p/2}x=\prod_{1\le x<p/2}ax.$$

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.
- **Proof.** The proof is a counting argument. Consider
$$a^{\frac{p-1}{2}} \prod_{1 \le x < p/2} x = \prod_{1 \le x < p/2} ax.$$
- This is $\equiv \prod_{1 \le x < p/2} r_x \pmod p$.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1 \le x < p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.
- **Proof.** The proof is a counting argument. Consider

$$a^{\frac{p-1}{2}} \prod_{1 \le x < p/2} x = \prod_{1 \le x < p/2} ax.$$

- 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 rest.

- **Theorem 14.** Suppose $p > 2$ and $p \nmid a$. Write each of the 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 $\left(\frac{a}{p}\right)_L = (-1)^m$, $m \equiv \sum_{1\le x<p/2} \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2$.
- **Proof.** The proof is a counting argument. Consider
$$a^{\frac{p-1}{2}} \prod_{1\le x<p/2} x = \prod_{1\le x<p/2} ax.$$
- 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 rest.
- Then card $\mathcal{A} = m$ and rearranging gives $a^{\frac{p-1}{2}} \prod_{1\le x<p/2} x \equiv$
$$\left(\prod_{x\in\mathcal{A}} r_x\right) \prod_{x\in\mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x\in\mathcal{A}} (p-r_x)\right) \prod_{x\in\mathcal{B}} r_x \pmod p \tag{2.4}$$

- $$a^{\frac{p-1}{2}} \prod_{1 \le x < p/2} x \equiv$$

$$\left(\prod_{x \in \mathcal{A}} r_x\right) \prod_{x \in \mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x \in \mathcal{A}} (p - r_x)\right) \prod_{x \in \mathcal{B}} r_x \pmod{p}.$$

- $a^{\frac{p-1}{2}} \prod_{1\le x<p/2} x \equiv$

$$\left(\prod_{x\in\mathcal{A}} r_x\right) \prod_{x\in\mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x\in\mathcal{A}} (p-r_x)\right) \prod_{x\in\mathcal{B}} r_x \pmod{p}.$$

- 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 $x \ne y$ and so the r_x are distinct.

- $$a^{\frac{p-1}{2}} \prod_{1 \le x < p/2} x \equiv$$
$$\left(\prod_{x\in\mathcal{A}} r_x\right) \prod_{x\in\mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x\in\mathcal{A}} (p-r_x)\right) \prod_{x\in\mathcal{B}} r_x \pmod p.$$
- 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 $x \ne y$ and so the r_x are distinct.
- Also since $p \nmid a$ and $1 \le x, y < p/2$ we have $p - r_x - r_y \equiv -a(x+y) \not\equiv 0 \pmod p$.

- $$a^{\frac{p-1}{2}} \prod_{1\le x<p/2} x \equiv$$
$$\left(\prod_{x\in\mathcal{A}} r_x\right) \prod_{x\in\mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x\in\mathcal{A}} (p-r_x)\right) \prod_{x\in\mathcal{B}} r_x \pmod p.$$
- 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 $x \ne y$ and so the r_x are distinct.
- Also since $p \nmid a$ and $1 \le x, y < p/2$ we have $p - r_x - r_y \equiv -a(x+y) \not\equiv 0 \pmod p$.
- Thus the $p - r_x$ with $x \in \mathcal{A}$ differ from the r_y with $y \in \mathcal{B}$.

- $$a^{\frac{p-1}{2}} \prod_{1\le x<p/2} x \equiv \left(\prod_{x\in\mathcal{A}} r_x\right) \prod_{x\in\mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x\in\mathcal{A}} (p-r_x)\right) \prod_{x\in\mathcal{B}} r_x \pmod{p}.$$
- 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 $x \ne y$ and so the r_x are distinct.
- Also since $p \nmid a$ and $1 \le x, y < p/2$ we have $p - r_x - r_y \equiv -a(x+y) \not\equiv 0 \pmod{p}$.
- Thus the $p - r_x$ with $x \in \mathcal{A}$ differ from the r_y with $y \in \mathcal{B}$.
- Hence the $\frac{1}{2}(p-1)$ numbers $p - r_x$ and r_x are just a permutation of the numbers z with $1 \le z \le \frac{1}{2}(p-1)$.

- $a^{\frac{p-1}{2}} \prod_{1\le x<p/2} x \equiv$
$$\left(\prod_{x\in\mathcal{A}} r_x\right)\prod_{x\in\mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x\in\mathcal{A}} (p-r_x)\right)\prod_{x\in\mathcal{B}} r_x \pmod{p}.$$
- 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 $x \ne y$ and so the r_x are distinct.
- Also since $p \nmid a$ and $1 \le x, y < p/2$ we have $p - r_x - r_y \equiv -a(x+y) \not\equiv 0 \pmod{p}$.
- Thus the $p - r_x$ with $x \in \mathcal{A}$ differ from the r_y with $y \in \mathcal{B}$.
- Hence 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 (2.4) 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, by Euler's Criterion, $\left(\frac{a}{p}\right)_L \equiv a^{\frac{p-1}{2}} \equiv (-1)^m$.

- $a^{\frac{p-1}{2}} \prod_{1\le x<p/2} x \equiv$
$$\left(\prod_{x\in\mathcal{A}} r_x\right)\prod_{x\in\mathcal{B}} r_x \equiv (-1)^m \left(\prod_{x\in\mathcal{A}}(p-r_x)\right)\prod_{x\in\mathcal{B}} r_x \pmod p.$$
- 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 $x \ne y$ and so the r_x are distinct.
- Also since $p \nmid a$ and $1 \le x, y < p/2$ we have $p - r_x - r_y \equiv -a(x+y) \not\equiv 0 \pmod p$.
- Thus the $p - r_x$ with $x \in \mathcal{A}$ differ from the r_y with $y \in \mathcal{B}$.
- Hence 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 (2.4) 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, by Euler's Criterion, $\left(\frac{a}{p}\right)_L \equiv a^{\frac{p-1}{2}} \equiv (-1)^m$.
- Now the difference is -2, 0 or 2.

- For the final formula we note that

$$r_x = ax - p\left\lfloor \frac{ax}{p} \right\rfloor \tag{2.5}$$

so that $0 \le r_x < p$.

- For the final formula we note that

$$r_x = ax - p\left\lfloor \frac{ax}{p} \right\rfloor \tag{2.5}$$

so that $0 \le r_x < p$.

- Now $0 < 2r_x/p < 2$ and so $\lfloor 2r_x/p \rfloor = 0$ or 1 and is 1 precisely when $p/2 < r_x < p$.

- For the final formula we note that

$$r_x = ax - p\left\lfloor \frac{ax}{p} \right\rfloor \tag{2.5}$$

  so that $0 \le r_x < p$.
- 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

$$m = \sum_{1 \le x < p/2} \lfloor 2r_x/p \rfloor.$$

- For the final formula we note that

$$r_x = ax - p\left\lfloor \frac{ax}{p} \right\rfloor \tag{2.5}$$

so that $0 \le r_x < p$.
- 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

$$m = \sum_{1 \le x < p/2} \lfloor 2r_x/p \rfloor .$$

- Moreover, by (2.5)

$$\begin{aligned}\lfloor 2r_x/p \rfloor &= \left\lfloor \frac{2ax}{p} - 2\left\lfloor \frac{ax}{p} \right\rfloor \right\rfloor = \left\lfloor \frac{2ax}{p} \right\rfloor - 2\left\lfloor \frac{ax}{p} \right\rfloor \\ &\equiv \left\lfloor \frac{2ax}{p} \right\rfloor \pmod 2\end{aligned}$$

and the final formula follows.

- Restricting to odd a gives a useful variant.

Theorem 16

Suppose $p > 2$ and $(a, 2p) = 1$. Then $\left(\frac{a}{p}\right)_L = (-1)^n$ where $n = \sum_{1 \le x < p/2} \left\lfloor \frac{ax}{p} \right\rfloor$. We also have $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}$.

- Restricting to odd a gives a useful variant.

Theorem 16

Suppose $p > 2$ and $(a, 2p) = 1$. Then $\left(\frac{a}{p}\right)_L = (-1)^n$ where $n = \sum_{1 \le x < p/2} \left\lfloor \frac{ax}{p} \right\rfloor$. We also have $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}$.

- **Proof.** $\left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L = \left(\frac{2}{p}\right)_L \left(\frac{a+p}{p}\right)_L = \left(\frac{4}{p}\right)_L \left(\frac{(a+p)/2}{p}\right)_L$

$$= \left(\frac{(a+p)/2}{p}\right)_L = (-1)^l$$

- Restricting to odd a gives a useful variant.

Theorem 16

Suppose $p > 2$ and $(a, 2p) = 1$. Then $\left(\dfrac{a}{p}\right)_L = (-1)^n$ where $n = \sum_{1\le x<p/2} \left\lfloor \frac{ax}{p} \right\rfloor$. We also have $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}$.

- **Proof.** $\left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L = \left(\frac{2}{p}\right)_L \left(\frac{a+p}{p}\right)_L = \left(\frac{4}{p}\right)_L \left(\frac{(a+p)/2}{p}\right)_L$

$$= \left(\frac{(a+p)/2}{p}\right)_L = (-1)^l$$

- where $l = \displaystyle\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{(a+p)x}{p} \right\rfloor = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{ax}{p} + x \right\rfloor =$
$$\sum_{x=1}^{(p-1)/2} \left(\left\lfloor \frac{ax}{p} \right\rfloor + x \right) = n + \frac{p^2-1}{8}.$$

- Restricting to odd a gives a useful variant.

Theorem 16

Suppose $p > 2$ and $(a, 2p) = 1$. Then $\left(\frac{a}{p}\right)_L = (-1)^n$ where $n = \sum_{1 \le x < p/2} \left\lfloor \frac{ax}{p} \right\rfloor$. We also have $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}$.

- **Proof.** $\left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L = \left(\frac{2}{p}\right)_L \left(\frac{a+p}{p}\right)_L = \left(\frac{4}{p}\right)_L \left(\frac{(a+p)/2}{p}\right)_L$

$$= \left(\frac{(a+p)/2}{p}\right)_L = (-1)^l$$

- where $l = \displaystyle\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{(a+p)x}{p} \right\rfloor = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{ax}{p} + x \right\rfloor =$

$$\sum_{x=1}^{(p-1)/2} \left(\left\lfloor \frac{ax}{p} \right\rfloor + x \right) = n + \frac{p^2-1}{8}.$$

- If we take $a = 1$, then we have the formula for $\left(\frac{2}{p}\right)_L$.

- Restricting to odd a gives a useful variant.

Theorem 16

Suppose $p > 2$ and $(a, 2p) = 1$. Then $\left(\frac{a}{p}\right)_L = (-1)^n$ where $n = \sum_{1\le x<p/2} \left\lfloor \frac{ax}{p} \right\rfloor$. We also have $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}$.

- **Proof.** $\left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L = \left(\frac{2}{p}\right)_L \left(\frac{a+p}{p}\right)_L = \left(\frac{4}{p}\right)_L \left(\frac{(a+p)/2}{p}\right)_L$

$$= \left(\frac{(a+p)/2}{p}\right)_L = (-1)^l$$

- where $l = \displaystyle\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{(a+p)x}{p} \right\rfloor = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{ax}{p} + x \right\rfloor =$ $\displaystyle\sum_{x=1}^{(p-1)/2} \left(\left\lfloor \frac{ax}{p} \right\rfloor + x \right) = n + \frac{p^2-1}{8}.$
- If we take $a = 1$, then we have the formula for $\left(\frac{2}{p}\right)_L$.
- Then factoring this out gives 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 17 (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

$$\left(\frac{q}{p}\right)_L = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)_L,$$

- Now we come to the big one. This is the Law of Quadratic Reciprocity. Gauss called it “Theorema Aureum”, the Golden Theorem.

Theorem 17 (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.

- We can use this to compute rapidly Legendre symbols.

Example 18

Is $x^2 \equiv 951 \pmod{2017}$ soluble? 2017 is prime, but $951 = 3 \times 317$.

- We can use this to compute rapidly Legendre symbols.

Example 18

Is $x^2 \equiv 951 \pmod{2017}$ soluble? 2017 is prime, but $951 = 3 \times 317$.

- Thus $\left(\frac{951}{2017}\right)_L = \left(\frac{3}{2017}\right)_L \left(\frac{317}{2017}\right)_L$.

- We can use this to compute rapidly Legendre symbols.

Example 18

Is $x^2 \equiv 951 \pmod{2017}$ soluble? 2017 is prime, but $951 = 3 \times 317$.

- Thus $\left(\frac{951}{2017}\right)_L = \left(\frac{3}{2017}\right)_L \left(\frac{317}{2017}\right)_L$.
- By the law, as $2017 \equiv 1 \pmod 4$,

$$\left(\frac{3}{2017}\right)_L = \left(\frac{2017}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1$$

$$\left(\frac{317}{2017}\right)_L = \left(\frac{2017}{317}\right)_L = \left(\frac{115}{317}\right)_L = \left(\frac{5}{317}\right)_L \left(\frac{23}{317}\right)_L.$$

- We can use this to compute rapidly Legendre symbols.

Example 18

Is $x^2 \equiv 951 \pmod{2017}$ soluble? 2017 is prime, but $951 = 3 \times 317$.

- Thus $\left(\frac{951}{2017}\right)_L = \left(\frac{3}{2017}\right)_L \left(\frac{317}{2017}\right)_L$.
- By the law, as $2017 \equiv 1 \pmod 4$,

$$\left(\frac{3}{2017}\right)_L = \left(\frac{2017}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1$$

$$\left(\frac{317}{2017}\right)_L = \left(\frac{2017}{317}\right)_L = \left(\frac{115}{317}\right)_L = \left(\frac{5}{317}\right)_L \left(\frac{23}{317}\right)_L.$$

- 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 $\left(\frac{951}{2017}\right)_L = -1$.

- We can use this to compute rapidly Legendre symbols.

Example 18

Is $x^2 \equiv 951 \pmod{2017}$ soluble? 2017 is prime, but $951 = 3 \times 317$.

- Thus $\left(\frac{951}{2017}\right)_L = \left(\frac{3}{2017}\right)_L \left(\frac{317}{2017}\right)_L$.
- By the law, as $2017 \equiv 1 \pmod 4$,

$$\left(\frac{3}{2017}\right)_L = \left(\frac{2017}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1$$

$$\left(\frac{317}{2017}\right)_L = \left(\frac{2017}{317}\right)_L = \left(\frac{115}{317}\right)_L = \left(\frac{5}{317}\right)_L \left(\frac{23}{317}\right)_L.$$

- 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 $2 \pmod{p}$.

Example 19

Let $p > 3$ be an odd prime. Then

$$\left(\frac{3}{p}\right)_L = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)_L .$$

- We can also use the law to obtain general rules, like that for $2 \pmod{p}$.

Example 19

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 $p \equiv 1 \pmod{3}$.

- We can also use the law to obtain general rules, like that for $2 \pmod p$.

Example 19

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 use the law to obtain general rules, like that for $2 \pmod p$.

Example 19

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

$$\left(\frac{3}{p}\right)_L = \begin{cases} (-1)^{\frac{p-1}{2}} & (p \equiv 1 \pmod 3) \\ -(-1)^{\frac{p-1}{2}} & (p \equiv 2 \pmod 3). \end{cases}$$

- We can also combine this with the formula in the case of $-1 \pmod p$ which follows from the Euler Criterion. Thus

$$\left(\frac{-3}{p}\right)_L = \begin{cases} 1 & (p \equiv 1 \pmod 3) \\ -1 & (p \equiv 2 \pmod 3). \end{cases}$$

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.
- Then $\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$ where $u = \sum_{1\le x<p/2} \left\lfloor \frac{qx}{p} \right\rfloor$ and $v = \sum_{1\le y<q/2} \left\lfloor \frac{py}{q} \right\rfloor$.

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.
- Then $\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$
  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 $1 \le y \le qx/p$.

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.
- Then $\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$ 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 $1 \le y < qx/p$.

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.
- Then $\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$
  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 $1 \le x < py/q$

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.
- Then $\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$ 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 $xq/p < y < q/2$.

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.
- Then $\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$
  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 $1 \le y < q/2$.

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.
- Then $\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$ 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.

- **Proof of the Law of Quadratic Reciprocity.** We start from two applications of the previous theorem.
- Then $\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = (-1)^{u+v}$ 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.

- In Example 18, there were several occasions when we needed to factorise the a in $\left(\frac{a}{p}\right)_L$.

- In Example 18, 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.

Definition 20

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.

- 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 $x^2 \equiv a \pmod{m}$.

Example 21

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 $\left(\frac{a_1 a_2}{m}\right)_J = \left(\frac{a_1}{m}\right)_J \left(\frac{a_2}{m}\right)_J$.

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 m_j are odd. Then $\left(\frac{a}{m_1 m_2}\right)_J = \left(\frac{a}{m_1}\right)_J \left(\frac{a}{m_2}\right)_J$.

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 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 $\left(\frac{a_1}{m}\right)_J = \left(\frac{a_2}{m}\right)_J$.

Properties of the Jacobi symbol

- 1. Suppose that m is odd. Then $\left(\frac{a_1a_2}{m}\right)_J = \left(\frac{a_1}{m}\right)_J\left(\frac{a_2}{m}\right)_J$.
- 2. Suppose m_j are odd. Then $\left(\frac{a}{m_1m_2}\right)_J = \left(\frac{a}{m_1}\right)_J\left(\frac{a}{m_2}\right)_J$.
- 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 $\left(\frac{-1}{m}\right)_J = (-1)^{\frac{m-1}{2}}$.

Properties of the Jacobi symbol

- 1. Suppose that m is odd. Then $\left(\frac{a_1a_2}{m}\right)_J = \left(\frac{a_1}{m}\right)_J\left(\frac{a_2}{m}\right)_J$.
- 2. Suppose m_j are odd. Then $\left(\frac{a}{m_1m_2}\right)_J = \left(\frac{a}{m_1}\right)_J\left(\frac{a}{m_2}\right)_J$.
- 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 $\left(\frac{2}{m}\right)_J = (-1)^{\frac{m^2-1}{8}}$.

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 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

$$\left(\frac{n}{m}\right)_J \left(\frac{m}{n}\right)_J = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}.$$

Properties of the Jacobi symbol

- 1. Suppose that m is odd. Then $\left(\frac{a_1a_2}{m}\right)_J = \left(\frac{a_1}{m}\right)_J\left(\frac{a_2}{m}\right)_J$.
- 2. Suppose m_j are odd. Then $\left(\frac{a}{m_1m_2}\right)_J = \left(\frac{a}{m_1}\right)_J\left(\frac{a}{m_2}\right)_J$.
- 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 follow from the definition. The rest depend on algebraic identities and induction on the number of prime factors. For 4. $\frac{m_1-1}{2}+\frac{m_2-1}{2} \equiv \frac{m_1m_2-1}{2} \pmod{2}$,

Properties of the Jacobi symbol

- 1. Suppose that m is odd. Then $\left(\frac{a_1a_2}{m}\right)_J = \left(\frac{a_1}{m}\right)_J\left(\frac{a_2}{m}\right)_J$.
- 2. Suppose m_j are odd. Then $\left(\frac{a}{m_1m_2}\right)_J = \left(\frac{a}{m_1}\right)_J\left(\frac{a}{m_2}\right)_J$.
- 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 follow from the definition. The rest depend on algebraic identities and induction on the number of prime factors. For 4. $\frac{m_1-1}{2}+\frac{m_2-1}{2} \equiv \frac{m_1m_2-1}{2} \pmod{2}$,
- 5. depends on $\frac{m_1^2-1}{8}+\frac{m_2^2-1}{8} \equiv \frac{m_1^2m_2^2-1}{8} \pmod{2}$.

Properties of the Jacobi symbol

- 1. Suppose that m is odd. Then $\left(\frac{a_1a_2}{m}\right)_J = \left(\frac{a_1}{m}\right)_J\left(\frac{a_2}{m}\right)_J$.
- 2. Suppose m_j are odd. Then $\left(\frac{a}{m_1m_2}\right)_J = \left(\frac{a}{m_1}\right)_J\left(\frac{a}{m_2}\right)_J$.
- 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 follow from the definition. The rest depend on algebraic identities and induction on the number of prime factors. For 4. $\frac{m_1-1}{2}+\frac{m_2-1}{2} \equiv \frac{m_1m_2-1}{2} \pmod{2}$,
- 5. depends on $\frac{m_1^2-1}{8}+\frac{m_2^2-1}{8} \equiv \frac{m_1^2m_2^2-1}{8} \pmod{2}$.
- 6. uses $\frac{l-1}{2}\cdot\frac{m-1}{2}+\frac{n-1}{2}\cdot\frac{m-1}{2} \equiv \frac{ln-1}{2}\cdot\frac{m-1}{2} \pmod{2}$.

- Return to Example 18, where we evaluated $\left(\frac{951}{2017}\right)_L$.

Example 22

Now we don't have to factor 951. By the Jacobi version of the law

$$\begin{aligned}\left(\frac{951}{2017}\right)_L &= \left(\frac{2017}{951}\right)_J = \left(\frac{115}{951}\right)_J = -\left(\frac{951}{115}\right)_J \\ &= -\left(\frac{31}{115}\right)_J = \left(\frac{115}{31}\right)_J = \left(\frac{22}{31}\right)_J \\ &= -\left(\frac{31}{11}\right)_J = -\left(\frac{9}{11}\right)_J = -1.\end{aligned}$$

- Return to Example 18, where we evaluated $\left(\frac{951}{2017}\right)_L$.

Example 22

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.

- Suppose we are interested in $\left(\frac{n}{m}\right)_L$ where n and m are odd.
- Follow the Euclidean algorithm and obtain

$$\begin{aligned} n &= q_1 m + r_1, \\ m &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ \vdots \quad & \quad \vdots \end{aligned}$$

- Suppose we are interested in $\left(\frac{n}{m}\right)_L$ where n and m are odd.
- Follow the Euclidean algorithm and obtain

$$\begin{aligned} n &= q_1 m + r_1, \\ m &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ \vdots &\quad\ \ \vdots \end{aligned}$$

- When $m, n, r_1, r_2, \ldots$ are odd, for suitable $t_1, t_2, \ldots$,

$$\begin{aligned} \left(\frac{n}{m}\right)_J = \left(\frac{r_1}{m}\right)_J &= (-1)^{t_1} \left(\frac{m}{r_1}\right)_J \\ &= (-1)^{t_1} \left(\frac{r_2}{r_1}\right)_J = (-1)^{t_2} \left(\frac{r_1}{r_2}\right)_J \\ &= (-1)^{t_2} \left(\frac{r_3}{r_2}\right)_J = (-1)^{t_3} \left(\frac{r_2}{r_3}\right)_J \\ &\ \ \vdots \qquad\qquad\quad \vdots \qquad\qquad\quad \vdots \end{aligned}$$

- Suppose we are interested in $\left(\frac{n}{m}\right)_L$ where n and m are odd.
- Follow the Euclidean algorithm and obtain

$$\begin{aligned} n &= q_1 m + r_1, \\ m &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ \vdots \quad & \quad \vdots \end{aligned}$$

- When $m, n, r_1, r_2, \ldots$ are odd, for suitable $t_1, t_2, \ldots$,

$$\begin{aligned} \left(\frac{n}{m}\right)_J &= \left(\frac{r_1}{m}\right)_J = (-1)^{t_1}\left(\frac{m}{r_1}\right)_J \\ &= (-1)^{t_1}\left(\frac{r_2}{r_1}\right)_J = (-1)^{t_2}\left(\frac{r_1}{r_2}\right)_J \\ &= (-1)^{t_2}\left(\frac{r_3}{r_2}\right)_J = (-1)^{t_3}\left(\frac{r_2}{r_3}\right)_J \\ \vdots \quad & \quad \vdots \quad \quad \vdots \end{aligned}$$

- If any of the r_j are even we first take out the powers of 2.

- I am now going to describe three algorithms which will make great use of, and which you will need to implement in your favourite programming software.

- I am now going to describe three algorithms which will make great use of, and which you will need to implement in your favourite programming software.
- The first algorithm computes the Jacobi symbol

$$\left(\frac{m}{n}\right)_J$$

for a given positive odd integer n and integer m.

- I am now going to describe three algorithms which will make great use of, and which you will need to implement in your favourite programming software.
- The first algorithm computes the Jacobi symbol

$$\left(\frac{m}{n}\right)_J$$

for a given positive odd integer n and integer m.
- It is just an immediate application of the law of quadratic reciprocity through the use of the division algorithm as organised in Euclid's algorithm, together with the removal of any powers of 2 at each stage and an evaluation of the corresponding

$$\left(\frac{2}{n}\right)_J.$$

- **Algorithm LJ.** Given an integer m and a positive integer n, compute $\left(\frac{m}{n}\right)_J$.

- **Algorithm 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 that 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 to give new 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 satisfies $0 \le m <$ new n.
  }

- **Algorithm 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 that the new m satisfies $0 \le m < n$. Put $t = 1$.
  1.2. While $m \ne 0$ {
  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 to give new 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 satisfies $0 \le m <$ new n.
  }
- 2. Output.
  2.1. If $n = 1$, then return t.
  2.2. Else return 0.

- **Algorithm QC357/8.** Given a $p \equiv 3, 5, 7 \pmod 8$ and a with $\left(\frac{a}{p}\right)_L = 1$, compute solution to $x^2 \equiv a \pmod p$.

- **Algorithm QC357/8.** Given a $p \equiv 3, 5, 7 \pmod 8$ and a with $\left(\frac{a}{p}\right)_L = 1$, compute solution to $x^2 \equiv a \pmod p$.
- If $p \equiv 3$ or $7 \pmod 8$, then compute $x \equiv a^{(p+1)/4} \pmod p$. Return x.

- **Algorithm QC357/8.** Given a $p \equiv 3, 5, 7 \pmod 8$ and a with $\left(\frac{a}{p}\right)_L = 1$, compute solution to $x^2 \equiv a \pmod p$.
- If $p \equiv 3$ or $7 \pmod 8$, then compute $x \equiv a^{(p+1)/4} \pmod p$. Return x.
- If $p \equiv 5$, take $x \equiv a^{(p+3)/8} \pmod p$. Compute x^2.
  2.1. If $x^2 \equiv a \pmod p$, then return x.
  2.2. If $x^2 \not\equiv a \pmod p$, compute $x \equiv x2^{(p-1)/4} \pmod p$. Return x.

- **Algorithm QC357/8.** Given a $p \equiv 3, 5, 7 \pmod 8$ and a with $\left(\frac{a}{p}\right)_L = 1$, compute solution to $x^2 \equiv a \pmod p$.
- If $p \equiv 3$ or $7 \pmod 8$, then compute $x \equiv a^{(p+1)/4} \pmod p$. Return x.
- If $p \equiv 5$, take $x \equiv a^{(p+3)/8} \pmod p$. Compute x^2.
  2.1. If $x^2 \equiv a \pmod p$, then return x.
  2.2. If $x^2 \not\equiv a \pmod p$, compute $x \equiv x2^{(p-1)/4} \pmod p$. Return x.
- **Proof.** When $p \equiv 3 \pmod 4$ we have $\frac{p+1}{4} \in \mathbb{N}$, so $a^{(p+1)/4}$ makes sense and by Euler's criterion.
  $x^2 \equiv a^{(p+1)/2} = a^{1+\frac{p-1}{2}} \equiv a\left(\frac{a}{p}\right)_L = a \pmod p$.

- **Algorithm QC357/8.** Given a $p \equiv 3, 5, 7 \pmod 8$ and a with $\left(\frac{a}{p}\right)_L = 1$, compute solution to $x^2 \equiv a \pmod p$.
- If $p \equiv 3$ or $7 \pmod 8$, then compute $x \equiv a^{(p+1)/4} \pmod p$. Return x.
- If $p \equiv 5$, take $x \equiv a^{(p+3)/8} \pmod p$. Compute x^2.
  2.1. If $x^2 \equiv a \pmod p$, then return x.
  2.2. If $x^2 \not\equiv a \pmod p$, compute $x \equiv x2^{(p-1)/4} \pmod p$. Return x.
- **Proof.** When $p \equiv 3 \pmod 4$ we have $\frac{p+1}{4} \in \mathbb{N}$, so $a^{(p+1)/4}$ makes sense and by Euler's criterion.
  $x^2 \equiv a^{(p+1)/2} = a^{1+\frac{p-1}{2}} \equiv a\left(\frac{a}{p}\right)_L = a \pmod p$.
- When $p \equiv 5 \pmod 8$, the issue is when $a^{(p+3)/4} \not\equiv a \pmod p$, i.e. $a^{(p-1)/4} \not\equiv 1 \pmod p$. By Euler's criterion $a^{(p-1)/2} \equiv 1 \pmod p$, so $a^{(p-1)/4} \equiv \pm 1 \pmod p$, and so $a^{(p-1)/4} \equiv -1 \pmod p$. Thus the new x gives
  $x^2 \equiv a^{(p+3)/4} 2^{(p-1)/2} \equiv (-a)\left(\frac{2}{p}\right) = (-a)(-1) = a \pmod p$.

- **Algorithm 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 $x^2 \equiv a \pmod p$.

- **Algorithm 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 each 2 in $p-1$, so that $p - 1 = 2^s u$ with u odd. Compute $d \equiv a^u \pmod p$ and $f \equiv b^u \pmod p$.

- **Algorithm 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 each 2 in $p - 1$, so that $p - 1 = 2^s u$ with u odd. Compute $d \equiv a^u \pmod p$ and $f \equiv b^u \pmod p$.
- 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_s. This will satisfy $df^{m_s} \equiv 1 \pmod p$ and m_s will be even.

- **Algorithm 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 each 2 in $p - 1$, so that $p - 1 = 2^s u$ with u odd. Compute $d \equiv a^u \pmod p$ and $f \equiv b^u \pmod p$.
- 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_s. This will satisfy $df^{m_s} \equiv 1 \pmod p$ and m_s will be even.
- 4. Compute $x \equiv a^{(u+1)/2} f^{m_s/2} \pmod p$. Return x.

- **Proof.** Initially we find b with $\left(\frac{b}{p}\right)_L = -1$, and s and u with $p-1 = 2^s u$ and u odd, $d \equiv a^u \pmod{p}$ and $f \equiv b^u \pmod{p}$.

- **Proof.** Initially we find b with $\left(\frac{b}{p}\right)_L = -1$, and s and u with $p-1 = 2^s u$ and u odd, $d \equiv a^u \pmod{p}$ and $f \equiv b^u \pmod{p}$.
- We will show below that there is an m so that $df^m \equiv 1 \pmod{p}$ and m is even. Then $x \equiv a^{(u+1)/2} f^{m/2} \pmod{p}$ satisfies

$$x^2 \equiv \left(a^{\frac{u+1}{2}} f^{\frac{m}{2}}\right)^2 = a^{u+1} f^m = adf^m \equiv a \pmod{p}.$$

Thus it all depends on the computation of m.

- Recall b with $\left(\frac{b}{p}\right)_L = -1$, s, u with $p-1=2^s u$ and u odd, $d \equiv a^u \pmod{p}$, $f \equiv b^u \pmod{p}$. To compute m so $df^m \equiv 1 \pmod{p}$ and $2|m$ as follows. Let $m_0 = 0$. For $i = 0, 1, \ldots, s-1$ compute $g \equiv (df^{m_i})^{2^{s-1-i}} \pmod{p}$. If $g \equiv -1 \pmod{p}$, then put $m_{i+1} = m_i + 2^i$. Else take $m_{i+1} = m_i$. Claim $df^{m_s} \equiv 1 \pmod{p}$, $2|m_s$.

- Recall b with $\left(\frac{b}{p}\right)_L = -1$, s, u with $p-1 = 2^s u$ and u odd, $d \equiv a^u \pmod{p}$, $f \equiv b^u \pmod{p}$. To compute m so $df^m \equiv 1 \pmod{p}$ and $2|m$ as follows. Let $m_0 = 0$. For $i = 0, 1, \ldots, s-1$ compute $g \equiv (df^{m_i})^{2^{s-1-i}} \pmod{p}$. If $g \equiv -1 \pmod{p}$, then put $m_{i+1} = m_i + 2^i$. Else take $m_{i+1} = m_i$. Claim $df^{m_s} \equiv 1 \pmod{p}$, $2|m_s$.
- By Euler's criterion $d^{2^{s-1}} \equiv a^{2^{s-1}u} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. So $\mathrm{ord}_p(d)|2^{s-1}$ and $f^{2^{s-1}} \equiv b^{2^{s-1}u} = b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Also $f^{2s} \equiv b^{p-1} \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(f) = 2^s$.

- Recall b with $\left(\frac{b}{p}\right)_L = -1$, s, u with $p-1 = 2^s u$ and u odd, $d \equiv a^u \pmod{p}$, $f \equiv b^u \pmod{p}$. To compute m so $df^m \equiv 1 \pmod{p}$ and $2|m$ as follows. Let $m_0 = 0$. For $i = 0, 1, \ldots, s-1$ compute $g \equiv (df^{m_i})^{2^{s-1-i}} \pmod{p}$. If $g \equiv -1 \pmod{p}$, then put $m_{i+1} = m_i + 2^i$. Else take $m_{i+1} = m_i$. Claim $df^{m_s} \equiv 1 \pmod{p}$, $2|m_s$.
- By Euler's criterion $d^{2^{s-1}} \equiv a^{2^{s-1}u} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. So $\mathrm{ord}_p(d)|2^{s-1}$ and $f^{2^{s-1}} \equiv b^{2^{s-1}u} = b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Also $f^{2s} \equiv b^{p-1} \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(f) = 2^s$.
- Prove by induction for $0 \le i \le s$ that $(df^{m_i})^{2^{s-i}} \equiv 1$.

- Recall b with $\left(\frac{b}{p}\right)_L = -1$, s, u with $p-1 = 2^s u$ and u odd, $d \equiv a^u \pmod{p}$, $f \equiv b^u \pmod{p}$. To compute m so $df^m \equiv 1 \pmod{p}$ and $2|m$ as follows. Let $m_0 = 0$. For $i = 0, 1, \ldots, s-1$ compute $g \equiv (df^{m_i})^{2^{s-1-i}} \pmod{p}$. If $g \equiv -1 \pmod{p}$, then put $m_{i+1} = m_i + 2^i$. Else take $m_{i+1} = m_i$. Claim $df^{m_s} \equiv 1 \pmod{p}$, $2|m_s$.
- By Euler's criterion $d^{2^{s-1}} \equiv a^{2^{s-1}u} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. So $\mathrm{ord}_p(d)|2^{s-1}$ and $f^{2^{s-1}} \equiv b^{2^{s-1}u} = b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Also $f^{2s} \equiv b^{p-1} \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(f) = 2^s$.
- Prove by induction for $0 \le i \le s$ that $(df^{m_i})^{2^{s-i}} \equiv 1$.
- For $i = 0$, $m_0 = 0$ so $(df^{m_0})^{2^s} = d^{2^s} \equiv 1 \pmod{p}$.

- Recall b with $\left(\frac{b}{p}\right)_L = -1$, s, u with $p-1=2^s u$ and u odd, $d \equiv a^u \pmod{p}$, $f \equiv b^u \pmod{p}$. To compute m so $df^m \equiv 1 \pmod{p}$ and $2|m$ as follows. Let $m_0 = 0$. For $i = 0, 1, \ldots, s-1$ compute $g \equiv (df^{m_i})^{2^{s-1-i}} \pmod{p}$. If $g \equiv -1 \pmod{p}$, then put $m_{i+1} = m_i + 2^i$. Else take $m_{i+1} = m_i$. Claim $df^{m_s} \equiv 1 \pmod{p}$, $2|m_s$.
- By Euler's criterion $d^{2^{s-1}} \equiv a^{2^{s-1}u} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. So $\mathrm{ord}_p(d)|2^{s-1}$ and $f^{2^{s-1}} \equiv b^{2^{s-1}u} = b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Also $f^{2s} \equiv b^{p-1} \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(f) = 2^s$.
- Prove by induction for $0 \le i \le s$ that $(df^{m_i})^{2^{s-i}} \equiv 1$.
- For $i = 0$, $m_0 = 0$ so $(df^{m_0})^{2^s} = d^{2^s} \equiv 1 \pmod{p}$.
- Inductive step assume for an i with $0 \le i \le s-1$ that $(df^{m_i})^{2^{s-i}} \equiv 1 \pmod{p}$. 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 $(df^{m_{i+1}})^{2^{s-1-i}} \equiv (df^{2^i+m_i})^{2^{s-1-i}} = (df^{m_i})^{2^{s-1-i}} f^{2^{s-1}} \equiv -b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ once more, by Euler's criterion.