MAU23101 Introduction to number theory 3 - Power residues, Legendre symbols, and quadratic reciprocity

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2020–2021
Version: October 21, 2020

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Main goal of this chapter

In this chapter, we fix a prime number $p \in \mathbb{N}$.

Remark

$\phi(p) = p - 1$.

In $(\mathbb{Z}/p\mathbb{Z})^\times$, how many elements are squares?

Example

-1 is a square in $\mathbb{Z}/5\mathbb{Z}$, since $2^2 = 4 \equiv -1 \bmod 5$.

Or more generally, how many k-th powers ($k \in \mathbb{N}$)?

And if $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a k-th power, how can we find $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $x = y^k$?

Reminder: discrete logarithm

Fix a primitive root $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ ($\exists$ since p is prime). Then the powers of g cover all of $(\mathbb{Z}/p\mathbb{Z})^\times$.

More precisely, for all $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, there exists $m \in \mathbb{Z}$ such that $x = g^m$, and this m is unique mod $\phi(p) = p - 1$.

Definition (Discrete logarithm in $(\mathbb{Z}/p\mathbb{Z})^\times$)

$$\underbrace{m = \log_g(x)}_{\in \mathbb{Z}/(p-1)\mathbb{Z}} \iff \underbrace{x = g^m}_{\in (\mathbb{Z}/p\mathbb{Z})^\times}.$$

$$\rightsquigarrow \text{ bijection } \quad \begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longleftrightarrow & \mathbb{Z}/(p-1)\mathbb{Z} \\ x & \longmapsto & m = \log_g x \\ x = g^m & \longleftarrow & m \end{array}.$$

The discrete log is really a log

Proposition

For all $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $m \in \mathbb{Z}$, we have

- $\log_g(xy) = \log_g(x) + \log_g(y)$,
- $\log_g(x^{-1}) = -\log_g(x)$,
- $\log_g(x^m) = m \log_g(x)$,
- $\log_g(x/y) = \log_g(x) - \log_g(y)$,
- $\log_g(1 \bmod p) = 0 \bmod p - 1$.

Proof.

Write $x = g^a$, $y = g^b$. Then

- $xy = g^{a+b}$,
- $x^{-1} = g^{-a}$,
- $x^m = g^{ma}$,

□

The discrete log is really a log

Proposition

For all $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$ *and* $m \in \mathbb{Z}$, *we have*

- $\log_g(xy) = \log_g(x) + \log_g(y)$,
- $\log_g(x^{-1}) = -\log_g(x)$,
- $\log_g(x^m) = m \log_g(x)$,
- $\log_g(x/y) = \log_g(x) - \log_g(y)$,
- $\log_g(1 \bmod p) = 0 \bmod p - 1$.

Proof.

Write $x = g^a$, $y = g^b$. Then

- $x/y = g^{a-b}$,
- $1 = g^0$.

□

k-th powers mod p

Corollary

Let $k \in \mathbb{Z}$ and $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then x is a k-th power iff. $\log_g(x)$ is a multiple of k in $\mathbb{Z}/(p-1)\mathbb{Z}$.

Proof.

If $x = y^k$, then $\log_g(x) = k \log_g(y)$.

If $\log_g(x) = km$ for some $m \in \mathbb{Z}/(p-1)\mathbb{Z}$, then $y = g^m$ satisfies $y^k = g^{km} = x$. □

Number of k-th powers mod p

Theorem

Let $k \in \mathbb{Z}$. Exactly

$$\frac{p-1}{\gcd(k, p-1)}$$

of the $p-1$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are k-th powers.

Proof.

By discrete log, $(\mathbb{Z}/p\mathbb{Z})^\times \longleftrightarrow \mathbb{Z}/(p-1)\mathbb{Z}$. So

$$\begin{aligned} &\#\{x \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \exists y \in (\mathbb{Z}/p\mathbb{Z})^\times : \ x = y^k\} \\ =&\#\{n \in \mathbb{Z}/(p-1)\mathbb{Z} \mid \exists m \in \mathbb{Z} : n \equiv km \bmod p-1\} \\ =&\#\{km \bmod p-1, \ m \in \mathbb{Z}\} \\ =&\operatorname{AO}(k \bmod p-1) = \frac{p-1}{\gcd(k, p-1)}. \end{aligned}$$

□

Number of k-th powers mod p

Theorem

Let $k \in \mathbb{Z}$. Exactly

$$\frac{p-1}{\gcd(k, p-1)}$$

of the $p-1$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are k-th powers.

Corollary

The map $\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \longmapsto & x^k \end{array}$ *is* $\gcd(k, p-1)$*-to-*1.

Example

The number of $(p-1)$-th powers in $(\mathbb{Z}/p\mathbb{Z})^\times$ is only 1.
Indeed, for all $y \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have $y^{p-1} = 1$ by Fermat!

k-th roots mod p

Theorem

If $k \in \mathbb{Z}$ is coprime to $p-1$, then every $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ has a unique k-th root, which is

$$\sqrt[k]{x} = x^\ell$$

where $\ell = (k \bmod p-1)^{-1} \in \mathbb{Z}/(p-1)\mathbb{Z}$.

Proof.

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \xrightarrow{x\mapsto x^k} & (\mathbb{Z}/p\mathbb{Z})^\times \\ \updownarrow & & \updownarrow \\ \mathbb{Z}/(p-1)\mathbb{Z} & \underset{k^{-1}m \leftarrow\!\shortmid\, m}{\overset{m\mapsto km}{\longleftrightarrow}} & \mathbb{Z}/(p-1)\mathbb{Z} \end{array}$$

□

k-th roots mod p

Theorem

If $k \in \mathbb{Z}$ is coprime to $p-1$, then every $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ has a unique k-th root, which is

$$\sqrt[k]{x} = x^\ell$$

where $\ell = (k \bmod p-1)^{-1} \in \mathbb{Z}/(p-1)\mathbb{Z}$.

Example

In $\mathbb{Z}/29\mathbb{Z}$, $\sqrt[3]{2} = 2^{(3 \bmod 28)^{-1}}$. We have $3u + 28v = 1$ for $u = -9$, $v = 1$, so $(3 \bmod 28)^{-1} = -9 = 19$.
Mod 29, $2^2 = 4$, $2^4 = (2^2)^2 = 4^2 = 16 = -13$,
$2^8 = (2^4)^2 = (-13)^2 = -5$, $2^{16} = (2^8)^2 = (-5)^2 = -4$,
whence $\sqrt[3]{2} = 2^{19} = 2^{16}2^2 2^1 = -4 \times 4 \times 2 = -32 = -3$.
Indeed, $-3^3 = -27 = 2 \bmod 29$.

The Legendre symbol: definition and properties

Squares mod p

We now study squares in $\mathbb{Z}/p\mathbb{Z}$.

If $p = 2$, then $\mathbb{Z}/p\mathbb{Z} = \{0, 1\} = \{0^2, 1^2\}$, so **we suppose that** $p \geqslant 3$ **from now on.** In particular, p is odd.

Joke

2 is the oddest prime.

Squares mod p

We now study squares in $\mathbb{Z}/p\mathbb{Z}$.

If $p = 2$, then $\mathbb{Z}/p\mathbb{Z} = \{0, 1\} = \{0^2, 1^2\}$, so **we suppose that** $p \geqslant 3$ **from now on.** In particular, p is odd.

Then in $(\mathbb{Z}/p\mathbb{Z})^\times$, there are $\frac{p-1}{\gcd(p-1,2)} = \frac{p-1}{2}$ squares, i.e. 50% are squares and 50% are not.

Definition

$$p' = \frac{p-1}{2}.$$

Remark

If $p \equiv 1 \bmod 4$, the p' is even.
If $p \equiv 3 \equiv -1 \bmod 4$, then p' is odd.

The Legendre symbol

Definition (Legendre symbol)

Let $x \in \mathbb{Z}$ *or* $\mathbb{Z}/p\mathbb{Z}$.

$$\left(\frac{x}{p}\right) = \begin{cases} 0, & \text{if } x = 0 \bmod p \\ +1, & \text{if } x \neq 0 \text{ and is a square } \bmod p \\ -1, & \text{if } x \neq 0 \text{ and is not a square } \bmod p. \end{cases}$$

Properties of the Legendre symbol

Theorem

- *For all* $x, y \in \mathbb{Z}/p\mathbb{Z}$, $\left(\dfrac{xy}{p}\right) = \left(\dfrac{x}{p}\right)\left(\dfrac{y}{p}\right)$.
- $\left(\dfrac{-1}{p}\right) = (-1)^{p'} = \begin{cases} +1, & \text{if } p \equiv 1 \bmod 4, \\ -1, & \text{if } p \equiv -1 \bmod 4. \end{cases}$
- $\left(\dfrac{2}{p}\right) = \begin{cases} +1, & \text{if } p \equiv \pm 1 \bmod 8, \\ -1, & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$
- *If* $q \neq p$ *is another odd prime, then*

$$\left(\frac{q}{p}\right) = (-1)^{p'q'} \left(\frac{p}{q}\right).$$

Properties of the Legendre symbol

Example

Is $x = -13$ a square mod $p = 71$?

$$\left(\frac{-13}{71}\right) = \left(\frac{-1}{71}\right)\left(\frac{13}{71}\right) = -(-1)^{13'71'}\left(\frac{71}{13}\right) = -\left(\frac{71}{13}\right)$$
$$= -\left(\frac{6}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right)$$
$$= (-1)^{3'13'}\left(\frac{13}{3}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = +1,$$

so yes!

Application to quadratic equations

Theorem

Let $a, b, c \in \mathbb{Z}/p\mathbb{Z}$ with $a \neq 0$, and $\Delta = b^2 - 4ac$. Then the number of solutions of $ax^2 + bx + c = 0$ in $\mathbb{Z}/p\mathbb{Z}$ is

$$\begin{cases} 2, & \text{if } \left(\frac{\Delta}{p}\right) = +1 \\ 0, & \text{if } \left(\frac{\Delta}{p}\right) = -1 \\ 1, & \text{if } \left(\frac{\Delta}{p}\right) = 0. \end{cases}$$

Proof.

$$ax^2+bx+c = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{(2a)^2}\right).$$

If $\Delta = \delta^2$, that's

$$a\left(x - \frac{-b+\delta}{2a}\right)\left(x - \frac{-b-\delta}{2a}\right);$$

as p is prime, one of the factors must vanish. □

The Legendre symbol: proofs, part $1/3$

Legendre as a group morphism

Lemma

For all $x \in \mathbb{Z}$, we have $x^{p'} \equiv \left(\frac{x}{p}\right) \bmod p$.

Proof.

If $p \mid x$ OK. Suppose now $x \in (\mathbb{Z}/p\mathbb{Z})^\times$.
Let $y = x^{p'}$. Then in $\mathbb{Z}/p\mathbb{Z}$, we have $y^2 = x^{2p'} = x^{p-1} = 1$ by Fermat, so $(y-1)(y+1) = y^2 - 1 = 0$ whence $y = \pm 1$ as p is prime.
Now if $x = z^2$ is a square in $\mathbb{Z}/p\mathbb{Z}$, then $y = z^{p-1} = +1$.
Conversely, since the polynomial $X^{p'} - 1$ has at most deg$= p'$ roots in $\mathbb{Z}/p\mathbb{Z}$ and since there are p' squares in $\mathbb{Z}/p\mathbb{Z}$, then $y \neq 1$ if x is not a square. □

Legendre as a group morphism

Lemma

For all $x \in \mathbb{Z}$*, we have* $x^{p'} \equiv \left(\frac{x}{p}\right) \bmod p$*.*

Corollary

$\left(\frac{-1}{p}\right) = (-1)^{p'}$*, and* $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$ *for all* $x, y \in \mathbb{Z}$*.*

Proof.

$+1$, 0, and -1 are all distinct in $\mathbb{Z}/p\mathbb{Z}$ for $p \geq 3$. □

The Legendre symbol: proofs, part 2/3

Legendre as a transfer map

Let $S = \{1, 2, \cdots, p'\}$.

Since $\mathbb{Z}/p\mathbb{Z} = \{-p', -p'+1, \cdots, p'\}$, every $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ can be written uniquely as

$$x = \varepsilon_x s_x \quad \text{where } \varepsilon_x = \pm 1 \text{ and } s_x \in S.$$

Proposition

For all $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have $\left(\frac{x}{p}\right) = \prod_{t \in S} \varepsilon_{tx}$.

Example

Take $p = 7$, $x = 3$. Then $p' = 3$, $S = \{1, 2, 3\}$,

$$1x = 3 = +3, \quad 2x = 6 = -1, \quad 3x = 9 = +2,$$

so $\left(\frac{3}{7}\right) = +1 \times -1 \times +1 = -1$.

Legendre as a transfer map

For each $t \in S$, decompose $tx = \varepsilon_{tx} s_{tx}$.

Lemma

For $t_1, t_2 \in S$, $s_{t_1 x} = s_{t_2 x}$ only when $t_1 = t_2$.

Proof.

$s_{t_1 x} = s_{t_2 x}$ implies $t_1 x = \pm t_2 x$, whence $t_1 = \pm t_2$ as $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, whence $t_1 = t_2$ as $t_1, t_2 \in S$. □

Corollary

The map $\begin{array}{ccc} S & \longrightarrow & S \\ t & \longmapsto & s_{tx} \end{array}$ *is bijective.*

Legendre as a transfer map

Corollary

The map $\begin{array}{ccc} S & \longrightarrow & S \\ t & \longmapsto & s_{tx} \end{array}$ *is bijective.*

Proof that $\left(\frac{x}{p}\right) = \prod_{t \in S} \varepsilon_{tx}$.

$$x^{p'} \prod_{t \in S} t = \prod_{t \in S} (tx) = \prod_{t \in S} (\varepsilon_{tx} s_{tx})$$

$$= \left(\prod_{t \in S} \varepsilon_{tx}\right) \left(\prod_{t \in S} s_{tx}\right) = \left(\prod_{t \in S} \varepsilon_{tx}\right) \left(\prod_{t \in S} t\right).$$

Now simplify by $\prod_{t \in S} t$ (legitimate as $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$). □

Proof of the formula for $\left(\frac{2}{p}\right)$

In $2 \times 1, \cdots, 2 \times p' = p - 1$, the terms having $\varepsilon = -1$ are the ones $> p'$. Euclidean-divide $p = 8q + r$, $r \in \{1, 3, 5, 7\}$. Then

$$
\begin{aligned}
&\# \{t \in \mathbb{Z} \mid p' < 2t \leq p - 1\} \\
=&\# \left\{t \in \mathbb{Z} \mid 2q + \frac{r-1}{4} < t \leq 4q + \frac{r-1}{2}\right\} \\
\equiv&\# \left\{t \in \mathbb{Z} \mid \frac{r-1}{4} < t \leq \frac{r-1}{2}\right\} \bmod 2
\end{aligned}
$$

$$
\rightsquigarrow \left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } r = 1, \\ -1 & \text{if } r = 3, \\ -1 & \text{if } r = 5, \\ +1 & \text{if } r = 7. \end{cases}
$$

The Legendre symbol: proofs, part 3/3: quadratic reciprocity

Notation

Given $x \in \mathbb{R}$, let $\lfloor x \rfloor$ be the largest $n \in \mathbb{Z}$ such that $n \leq x$.

Example

$\lfloor 3 \rfloor = \lfloor \pi \rfloor = \lfloor 3.99 \rfloor = 3.$

Euclidean division $a = bq + r \rightsquigarrow q = \lfloor a/b \rfloor$.

Let $p \neq q$ be primes ≥ 3.

Proof of quadratic reciprocity

For each $x \in \mathbb{Z}$, Divide $xq = p \left\lfloor \frac{xq}{p} \right\rfloor + r_x, \ 0 \leq r_x < p$.

- If $0 \leq r_x \leq p'$, then $s_{xq} = r_x, \ \ \varepsilon_{xq} = +1$.
- If $p' < r_x < p$, then $s_{xq} = p - r_x, \ \ \varepsilon_{xq} = -1$.

So mod 2 we have

$$\sum_{x=1}^{p'} r_x = \sum_{\varepsilon_{xq}=+1} s_{xq} + \sum_{\varepsilon_{xq}=-1} p - s_{xq} \equiv \sum_{\varepsilon_{xq}=+1} s_{xq} + \sum_{\varepsilon_{xq}=-1} 1 + \sum_{\varepsilon_{xq}=-1} s_{xq}$$

$$= \sum_{x=1}^{p'} s_{xq} + \sum_{\varepsilon_{xq}=-1} 1 = \sum_{t \in S} t + \sum_{\varepsilon_{xq}=-1} 1.$$

Besides $q \sum_{x \in S} x = \sum_{x=1}^{p'} xq = \sum_{x=1}^{p'} p \left\lfloor \frac{xq}{p} \right\rfloor + \sum_{x=1}^{p'} r_x$,

so $\sum_{x=1}^{p'} \cancel{p} \left\lfloor \frac{xq}{p} \right\rfloor \equiv \cancel{q} \sum_{x \in S} x - \sum_{x=1}^{p'} r_x \equiv - \sum_{\varepsilon_{xq}=-1} 1$

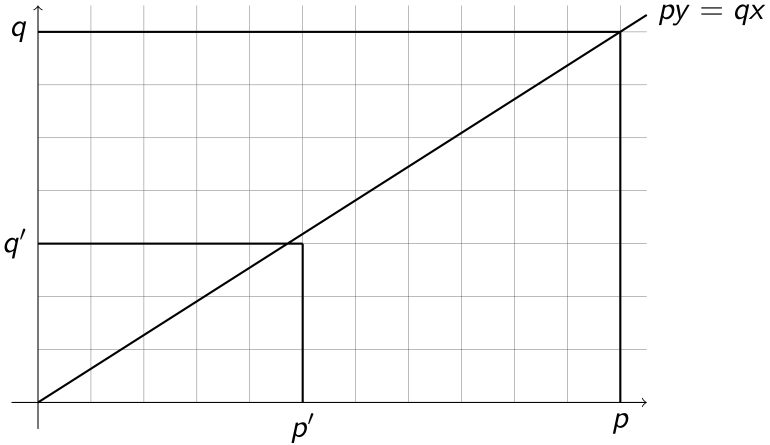
Proof of quadratic reciprocity

$$\text{so} \sum_{x=1}^{p'} \cancel{p} \left\lfloor \frac{xq}{p} \right\rfloor \equiv \cancel{q} \sum_{x \in S} x - \sum_{x=1}^{p'} r_x \equiv - \sum_{\varepsilon_{xq}=-1} 1$$

$$\rightsquigarrow \left(\frac{q}{p}\right) = (-1)^{\sum_{x=1}^{p'} \left\lfloor \frac{xq}{p} \right\rfloor}.$$

Similarly, $\left(\frac{p}{q}\right) = (-1)^{\sum_{y=1}^{q'} \left\lfloor \frac{yp}{q} \right\rfloor}$.

Proof of quadratic reciprocity



$$\sum_{x=1}^{p'} \left\lfloor \frac{xq}{p} \right\rfloor + \sum_{y=1}^{q'} \left\lfloor \frac{yp}{q} \right\rfloor = p'q' \quad \rightsquigarrow \quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{p'q'}.$$