Number Theory, Lecture 6

Quadratic residues, quadratic reciprocity

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Summary

Summary

Summary

Summary

- N integer
- $f(x) = Ax^2 + Bx + C$
- Want to solve $f(x) \equiv 0 \mod N$
- CRT: if $N = mn$, $\gcd(m, n) = 1$, $f(a) \equiv 0 \mod m$, $f(b) \equiv 0 \mod n$, then exists unique c ($\mod mn$) with $c \equiv a \mod m$, $c \equiv b \mod n$, and hence $f(c) \equiv 0 \mod m$, $f(c) \equiv 0 \mod n$, so $f(c) \equiv 0 \mod N$
- Hensel lifting: suppose $f(a) \equiv 0 \mod p$. Then $f'(a) \equiv 2Aa + B \mod p$. If non-zero, a lifts uniquely to zero mod p^r.

- p prime
- $f(x) = Ax^2 + Bx + C$,
- $p \not| A$
-

$$\begin{aligned} Ax^2 + Bx + C &\equiv 0 \mod p \\ x^2 + A^{-1}Bx + A^{-1}C &\equiv 0 \mod p \\ x^2 + Dx + F &\equiv 0 \mod p \\ x^2 + 2Ex + F &\equiv 0 \mod p \\ (x+E)^2 &\equiv E^2 - F \mod p \\ t^2 &\equiv u \mod p \end{aligned}$$

Definition

- p prime
- $p \not| u$
- u is a quadratic residue modulo p if

$$x^2 \equiv u \mod p$$

is solvable, a quadratic non-residue otherwise

Example

$p = 5$, squares

x	0	1	2	3	4
x^2	0	1	4	4	1

1,4 q.r, 2,3 q.n.r. 0 square, not q.r.

Henceforth, p is an odd prime.

Lemma

Suppose $\langle g \rangle = \mathbb{Z}_p^*$. Then $u = g^s$ is a q.r. iff s is even. Thus, precisely half of the elements in $\mathbb{Z}_p^*$ are q.r, half are q.n.r.

Proof.

Let $x = g^t$. Then $x^2 = u \in \mathbb{Z}_p^*$ iff $2t \equiv s \mod p-1$. If s even, this is solvable, if s is odd, it is not. □

Furthermore, we see (Laplace) that when u is q.r, $x^2 \equiv u \mod p$ has two solns , $a, -a$.

Definition

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ q.r. w.r.t. } p \\ -1 & a \text{ q.n.r. w.r.t. } p \\ 0 & a \equiv 0 \mod p \end{cases}$$

Ususually, we only use $a \not\equiv 0 \mod p$. p is still an odd prime.

Theorem

p odd prime, $a, b \not\equiv 0 \mod p$. Then

- $\left(\frac{1}{p}\right) = 1$
- $\left(\frac{a^2}{p}\right) = 1$
- *If* $a \equiv b \mod p$ *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof.

Let $\langle g \rangle = \mathbb{Z}_p^*$, $a = g^s$, $b = g^t$. Since $\left(\frac{a}{p}\right) = (-1)^s$ et cetera, we have

$$\left(\frac{ab}{p}\right) = (-1)^{s+t} = (-1)^s(-1)^t = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Theorem (Euler criterion)

p odd prime, $P = (p-1)/2$, $a \not\equiv 0 \mod p$. Then

$$a^P \equiv \left(\frac{a}{p}\right) \mod p$$

Proof.

By Fermat, $a^{p-1} \equiv 1 \mod p$, so

$$0 \equiv a^{2P} - 1 \equiv (a^P + 1)(a^P - 1) \mod p$$

hence $a^P \equiv 1 \mod p$ or hence $a^P \equiv -1 \mod p$.
Let g be a primitive root, $a = g^s$, $a^P = g^{sP}$.

1. If s is even, then $p-1 | sP$, so $g^{sP} \equiv 1 \mod p$
2. If s is odd, then $p-1 \not| s\frac{p-1}{2}$, so $g^{sP} \not\equiv 1 \mod p$

□

When is -1 q.r.?

Theorem

$$\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) \equiv (-1)^P \mod p \equiv \begin{cases} +1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

Proof.

EC and $P = (4k+1-1)/2$ or $P = (4k+3-1)/2$. □

Lemma (Gauss)

- p, P, a *as before*
- $S = \{a, 2a, 3a, \ldots, Pa\}$
- *For* $s \in S$, *unique* $t \in (-p/2, p/2) \cap \mathbb{Z}$ *with* $s \equiv t \mod p$
- v *nr negative representatives*
- *Then:* $\left(\frac{a}{p}\right) = (-1)^v$.

Example

$p = 7, P = 3, a = 3$. $S = \{3, 6, 9\} \equiv \{3, -1, 2\} \subseteq (-7/2, 7/2)$. $v = 1$, $\left(\frac{3}{7}\right) = -1$.

Proof.

Clearly, $ia \not\equiv ja \mod p$ for $i \neq j$. Also: $ia \not\equiv -ja \mod p$. Otherwise: $0 \equiv ia + ja \equiv (i+j)a \mod p$, so $i + j \equiv 0 \mod p$, impossible since $1 \leq i, j \leq (p-1)/2$.

So $ia \equiv \varepsilon(i)\sigma(i)a \mod p$, $\varepsilon(i) \in \{-1, 1\}$, $\sigma : \{1, 2, \ldots, P\} \to \{1, 2, \ldots, P\}$ permutation.

$$\prod_{i=1}^{P} ia \equiv \prod_{i=1}^{P} \varepsilon(i)\sigma(i)a$$

Cancel $P!$, get

$$a^P \equiv \prod_{i=1}^{P} \varepsilon(i) = (-1)^v.$$

□

Theorem

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$$

Proof

Gauss's lemma: reducing $S = \{2, 4, 6, \ldots, 2P = p-1\}$ to $(-p/2, p/2)$, how many negative? Count $S \cap (p/2, p)$.

$$p/2 < 2x < p \quad \Longleftrightarrow \quad p/4 < x < p/2, \qquad x \in \mathbb{Z}$$

Put $p = 8k + r$, $r \in \{1, 3, 5, 7\}$.

$$2k + r/4 < x < 4k + r/2, \quad x \in \mathbb{Z}$$

$2k$ and $4k$ even integers, so parity of number integer x does not change if we instead consider

$$r/4 < x < r/2.$$

Proof.

- $r = 1$:

  $$1/4 < x < 1/2, \quad x \in \mathbb{Z}$$

  has no solns
- $r = 3$:

  $$3/4 < x < 3/2, \quad x \in \mathbb{Z}$$

  has 1 soln, $x = 1$
- $r = 5$:

  $$5/4 < x < 5/2, \quad x \in \mathbb{Z}$$

  has 1 soln, $x = 2$
- $r = 7$:

  $$7/4 < x < 7/2, \quad x \in \mathbb{Z}$$

  has 2 soln, $x = 2, 3$

So even number of solns if $r = 1$, $r = 7$. □

Example

- $p = 11,\ P = 5$
- $S = \{2, 4, 6, 8, 10\} \equiv \{2, 4, -5, -3, -1\}$
- $v = 3,\ \left(\frac{2}{11}\right) = -1$
- $r = 3,$
- Integer solns to

$$11/2 < x < 11$$
$$\frac{8*1+3}{2} < 2x < 8*1+3$$
$$\frac{8*1+3}{4} < x < \frac{8*1+3}{2}$$
$$2 + \frac{3}{4} < x < 4 + \frac{3}{2}$$

is $x = 3, 4, 5$

- Integer solns to

$$\frac{3}{4} < x < \frac{3}{2}$$

is $x = 1$.

Theorem

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \mod 12 \\ -1 & p \equiv \pm 3 \mod 12 \end{cases}$$

Theorem

$$\left(\frac{p-3}{p}\right) = \left(\frac{-3}{p}\right) = \begin{cases} +1 & p \equiv 1 \mod 6 \\ -1 & p \equiv -1 \mod 6 \end{cases}$$

Proof.

Gauss's lemma, or wait for quadratic reciprocity! □

Theorem (Euler)

- p_1, p_2, p_3 *odd primes,*
- a *integer,* $p_i \not| a$
- $p_i = 4ak_i + r_i$, $0 < r_i < 4a$
- $r_2 = r_1$
- $r_3 = 4a - r_1$

Then:

- $\left(\frac{a}{p_2}\right) = \left(\frac{a}{p_1}\right)$
- $\left(\frac{a}{p_3}\right) = \left(\frac{a}{p_1}\right)$

Example

- $\left(\frac{5}{23}\right) = \left(\frac{5}{43}\right)$, $4a = 20$, $r = 3$
- $\left(\frac{8}{37}\right) = \left(\frac{8}{59}\right)$, $4a = 32$, $r = 4$, $4a - 5 = 27$

Proof I

- p odd prime
- $P = (p-1)/2$
- $S = \{a, 2a, \ldots, Pa\}$
- Reduce to $(-p/2, p/2)$, v is nr negatives
- Put $b = a/2$ if a even or $b = (a-1)/2$ if a odd
- v is nr integers in S and simultaneously in

$$(\frac{1}{2}p, p) \cup (\frac{3}{2}p, 2p) \cup \cdots \cup ((b-\frac{1}{2})p, bp)$$

- No endpoints integers, no overlap, easy counting
- Want

$$xa \in (\frac{1}{2}p, p) \cup (\frac{3}{2}p, 2p) \cup \cdots \cup ((b-\frac{1}{2})p, bp)$$

Proof II

- Equivalent: integer x lies in

$$\bigcup_{\ell=1}^{P}\left(\frac{2\ell-1}{2a}p,\frac{\ell}{a}p\right)$$

- Replace p with $4ak+r$, get

$$\bigcup_{\ell=1}^{P}\left((2\ell-1)2k+\frac{2\ell-1}{2a}r,4\ell k+\frac{\ell}{a}r\right)$$

- Different k, same r: the v's differ by an even integer, same $\left(\frac{a}{p}\right)$
- In particular, can replace with just r, get: count nr integers in

$$\bigcup_{\ell=1}^{P}\left(\frac{2\ell-1}{2a}r,\frac{\ell}{a}r\right)$$

Proof III

- Second part of proof: same idea, a bit harder
- Left as exercise :-)