Math 412: Number Theory
Lecture 18 Law of quadratic reciprocity

Gexin Yu
gyu@wm.edu

College of William and Mary

Quadratic residue/nonresidue and Legendre symbols

- Legendre symbol of d modulo p: let p be an odd prime. Define the

$$\left(\frac{d}{p}\right) = \begin{cases} 1, & \text{if } d \text{ is a quadratic residue modulo } p \\ -1, & \text{if } d \text{ is a quadratic nonresidue modulo } p \\ 0, & \text{if } p|d \end{cases}$$

- Thm (Euler Criterion): Let prime $p > 2$ and $p \not| d$. Then

$$\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \pmod{p}.$$

- Properties of Legendre symbols:
  - $\left(\frac{d}{p}\right) = \left(\frac{p+d}{p}\right)$
  - $\left(\frac{cd}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{d}{p}\right)$
  - If $p \not| d$, then $\left(\frac{d^2}{p}\right) = 1$
  - $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

- Gauss Lemma: Let p be an odd prime, and let $a \in Z$ with $(a, p) = 1$. Let $A = \underline{\{j : t \equiv aj \pmod{p}, 1 \leq j \leq \frac{p-1}{2}, \frac{p}{2} < t < p\}}$ and $n = |A|$ Then
$$\left(\frac{a}{p}\right) = (-1)^n.$$

$$aj = \left\lfloor \frac{aj}{p} \right\rfloor \cdot p + t$$

- Gauss Lemma: Let p be an odd prime, and let $a \in Z$ with $(a, p) = 1$. Let $A = \{j : t \equiv aj \pmod{p}, 1 \leq j \leq \frac{p-1}{2}, \frac{p}{2} < t < p\}$ and $n = |A|$ Then
$$\left(\frac{a}{p}\right) = (-1)^n.$$
- Proof: for $1 \leq i < j \leq p/2$, $ia - ja$ and $ia + ja$ are not divisible by p, that is, $ia \not\equiv ja \pmod{p}$. $p \mid ai - aj \Rightarrow p \mid i - j \Rightarrow i - j = 0$
- Let $m_i a \pmod{p}$ with $i \in A$ be greater than $p/2$. Then $p - m_i a \pmod{p}$ with $i \notin A$ are also greater than $p/2$, and they are different from those with $i \in A$. $m_i a < p/2 \Rightarrow p - m_i a > p/2$
- It follows that $\{p - m_1 a, p - m_2 a, \ldots, p - m_n a, m_{n+1} a, \ldots, m_t a\} = \{1, 2, \ldots, (p-1)/2\}$.
- Now
$$\prod_{i=1}^{(p-1)/2} ia \equiv (-1)^n (p - m_1 a) \ldots (p - m_n a)(m_{n+1} a) \ldots (m_t a)$$
$$\equiv (-1)^n 1 \cdot 2 \cdot \ldots (p-1)/2 \pmod{p}.$$

So we have $a^{(p-1)/2} \equiv (-1)^n \pmod{p}$

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$

Thm: 2 is a quadratic residue modulo p iff $p \equiv \pm 1 \pmod 8$. OR

$$\boxed{\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.}$$

$\left(\frac{2}{p}\right) = (-1)^n$ where n is the element in $\{1\cdot 2, 2\cdot 2, \dots, \frac{p-1}{2}\cdot 2\}$, that are $> p/2$

$= \{2, 2\cdot 2, \dots, p-1\}$

Need to find i s.t. $2i > p/2$.

$\underline{p = 8k + r}$: $r = 1, 3, 5, 7$

$\underline{r=1}$: $2i > \frac{p}{2} = \frac{8k+1}{2} \Rightarrow i \geq 2k+1$. $\Rightarrow n = \overset{p-1}{(8k+1-1)} - 2k$

$= 6k$ $\underline{\text{even}}$

$\Rightarrow \left(\frac{2}{p}\right) = (-1)^{6k} = 1$,

$\underline{r=3}$: $2i > \frac{p}{2} = \frac{8k+3}{2} \Rightarrow i \geq 2k+2 \Rightarrow n = (8\underline{k+3}-1) - (2k+1)$

$= 6k+1$ odd

$\left(\frac{2}{p}\right) = (-1)^{6k+1} = -1$.

$r=5$: hold

$r=7$: never

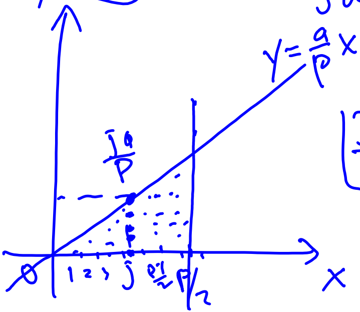
The law of quadratic reciprocity (Gauss 1795)

- Lem: let p be odd prime and a odd integer and $(a, p) = 1$, then

$$\left(\frac{a}{p}\right) = (-1)^T, \quad \text{where } \boxed{T = \underline{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor}}.$$

$ja = p \cdot \left\lfloor \frac{ja}{p} \right\rfloor + t$

integer pts in this region



$\left\lfloor \frac{ja}{p} \right\rfloor$ — # integer pts on $x = \frac{ja}{p}$. between x & $y = \frac{a}{p}x$

The law of quadratic reciprocity (Gauss 1795)

- Lem: let p be odd prime and a odd integer and $(a, p) = 1$, then

$$\left(\frac{a}{p}\right) = (-1)^T, \quad \text{where} \quad T = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor .$$

PF: Let $ja = p\lfloor \frac{ja}{p} \rfloor + t_j$ for $1 \le j \le \frac{p-1}{2}$. Then $\sum_{j=1}^{(p-1)/2} ja = pT + \sum_j t_j$.

- Let $A = \{j : t_j > p/2\}$, i.e., the set defined in Gauss Lemma. Then

$$\sum_j t_j = \sum_{i \notin A} s_i + \sum_{i \in A} r_i = \sum_{i \notin A} s_i + \sum_{i \in A} (p - r_i) - np + 2\sum_i r_i$$

//

$$\underline{\sum_{j=1}^{\frac{p-1}{2}} aj - pT}$$

$$= \underline{\sum_{i=1}^{(p-1)/2} i - np + \boxed{2\sum_i r_i}.}$$

$$p(T-n) \equiv \sum_{j=1}^{\frac{p-1}{2}} \underset{\substack{\uparrow \\ \text{even}}}{(a-1)}\, j \pmod 2$$

- It follows that $T \equiv n \pmod 2$, so the conclusion by Gauss Lemma.

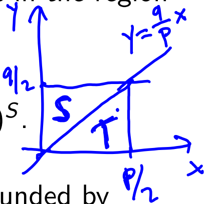
- Thm (Quadratic Reciprocity Law of Gauss): let p, q be distinct odd primes. Then

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

- Thm (Quadratic Reciprocity Law of Gauss): let p, q be distinct odd primes. Then

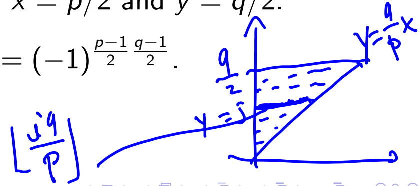
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

PF: We should note that T is the number of integer points in the region bounded by x-axis, $x = p/2$ and $y = ax/p$.



- Let $S = \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor$ with odd prime q, then $\left(\frac{p}{q}\right) = (-1)^S$.
- But S is the number of integer points in the region bounded by y-axis, $y = q/2$, and $x = qy/p$, and $S + T$ is the integer points in the region bounded by x-axis, y-axis, $x = p/2$ and $y = q/2$.
- It follows that $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{S+T} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

$(-1)^T$ $(-1)^S$



- Thm (Quadratic Reciprocity Law of Gauss): let p, q be distinct odd primes. Then
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

PF: We should note that T is the number of integer points in the region bounded by x-axis, $x = p/2$ and $y = ax/p$.

- Let $S = \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor$ with odd prime q, then $\left(\frac{p}{q}\right) = (-1)^S$.
- But S is the number of integer points in the region bounded by y-axis, $y = q/2$, and $x = qy/p$, and $S + T$ is the integer points in the region bounded by x-axis, y-axis, $x = p/2$ and $y = q/2$.
- It follows that $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{S+T} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

p or q is 1 (mod 4)

Corollary: $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p, q \equiv 3 \pmod 4$; otherwise, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

Law of quadratic reciprocity (applications)

$\boxed{137 \equiv 1 \pmod 4}$, $227 \equiv 3 \pmod 4$

- Ex: compute $\left(\frac{137}{227}\right)$ $= \left(\frac{227}{137}\right) = \left(\frac{90}{137}\right) = \left(\frac{3^2 \cdot 2 \cdot 5}{137}\right)$

$$= \underline{\left(\frac{3^2}{137}\right)} \cdot \left(\frac{2}{137}\right) \cdot \left(\frac{5}{137}\right) = 1 \cdot 1 \cdot \left(\frac{5}{137}\right)$$

$137 \equiv 1 \pmod 8$

$5 \equiv 1 \pmod 4$

$$= \left(\frac{137}{5}\right) = \left(\frac{2}{5}\right) = -1$$

$\underline{5 \equiv 5 \pmod 8}$

Cyclic numbers

- A *cyclic number* is an $(n-1)$-digit integer that, when multiplied by $1, 2, 3, \ldots, n-1$, produces the same digits in a different order. For example, 142857 is a cyclic number with 6 digits. Prove that if 10 is a primitive root modulo p, where p is a prime, then $(10^{p-1}-1)/p$ is a cyclic number.

$$\frac{1}{7} = 0.\overline{142857}$$

Cyclic numbers

- A *cyclic number* is an $(n-1)$-digit integer that, when multiplied by $1, 2, 3, \ldots, n-1$, produces the same digits in a different order. For example, 142857 is a cyclic number with 6 digits. Prove that if 10 is a primitive root modulo p, where p is a prime, then $(10^{p-1}-1)/p$ is a cyclic number.
- Let $C(k)$ be an integer of k digits, and $C(k,i)$ be a rotation of $C(k)$ by moving the first i digits to the right. Let $M(i)$ be the number formed by the first i digits of $C(k)$. For example, $C(6) = 142857$, $C(6,2) = 285714$, and $M(2) = 14$. Then

$$C(k,i) = 10^i \cdot C(k) - M(i)(10^k - 1)$$

$$= 10^i C(k) - M(i) \cdot 10^k + M(i)$$

Cyclic numbers

- A *cyclic number* is an $(n-1)$-digit integer that, when multiplied by $1, 2, 3, \ldots, n-1$, produces the same digits in a different order. For example, 142857 is a cyclic number with 6 digits. Prove that if 10 is a primitive root modulo p, where p is a prime, then $(10^{p-1}-1)/p$ is a cyclic number.
- Let $C(k)$ be an integer of k digits, and $C(k,i)$ be a rotation of $C(k)$ by moving the first i digits to the right. Let $M(i)$ be the number formed by the first i digits of $C(k)$. For example, $C(6) = 142857$, $C(6,2) = 285714$, and $M(2) = 14$. Then
$$C(k,i) = 10^i \cdot C(k) - M(i)(10^k - 1)$$
- Let 10 be a primitive root for p, and let $C(p-1) = (10^{p-1}-1)/p$. Note that when 10^i is divided by p, we get quotient $M(i)$ and remainder r_i, and $r_i = 10^i - pM(i)$. It follows that
$$\begin{aligned} r_i C(p-1) &= C(p-1) \cdot 10^i - M(i)pC(p-1) \\ &= C(p-1) \cdot 10^i - M(i)(10^{p-1}-1) = C(p-1,i). \end{aligned}$$