Number theory and Cryptography May 28th, 2024

Lecture 7: Quadratic Reciprocity

Instructor: Chao Qin *Notes written by: Wenhao Tong and Yingshu Wang*

Definition (Quadratic Residue)**.** *Fix a prime p. An integer a not divisible by p is a* quadratic residue *modulo p if a is a square modulo p; otherwise, a is a* quadratic nonresidue*.*

For example, the squares modulo 5 are

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 4, \quad 4^2 = 1, \qquad \pmod 5$$

so 1 and 4 are both quadratic residues and 2 and 3 are quadratic nonresidues.

Definition (Legendre Symbol)**.** *Let p be an odd prime and let a be an integer. Set*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } \gcd(a,p) \neq 1, \\ +1 & \text{if } a \text{ is a quadratic residue, and} \\ -1 & \text{if } a \text{ is a quadratic nonresidue.} \end{cases}$$

We call this symbol the Legendre Symbol*.*

For example, we have

$$\left(\frac{1}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = -1, \quad \left(\frac{3}{5}\right) = -1, \quad \left(\frac{4}{5}\right) = 1, \quad \left(\frac{5}{5}\right) = 0.$$

Lemma. *The map $\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ given by $\psi(a) = \left(\frac{a}{p}\right)$ is a surjective group homomorphism.*

Theorem (Gauss's Quadratic Reciprocity Law)**.** *Suppose p and q are distinct odd primes. Then*

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

Also

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{and} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

In our example, Gauss's theorem implies that

$$\left(\frac{5}{p}\right) = (-1)^{2\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv 1,4 \pmod 5 \\ -1 & \text{if } p \equiv 2,3 \pmod 5. \end{cases}$$

Example 1. *Is* 69 *a square modulo the prime* 389*? We have*

$$\left(\frac{69}{389}\right) = \left(\frac{3\cdot 23}{389}\right) = \left(\frac{3}{389}\right)\cdot\left(\frac{23}{389}\right) = (-1)\cdot(-1) = 1.$$

Here

$$\left(\frac{3}{389}\right) = \left(\frac{389}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

and

$$\begin{aligned}\left(\frac{23}{389}\right) &= \left(\frac{389}{23}\right) = \left(\frac{21}{23}\right) = \left(\frac{-2}{23}\right) \\ &= \left(\frac{-1}{23}\right)\left(\frac{2}{23}\right) = (-1)^{\frac{23-1}{2}}\cdot 1 = -1.\end{aligned}$$

Thus 69 *is a square modulo* 389*.*

Proposition (Euler's Criterion)**.** *We have* $\left(\frac{a}{p}\right) = 1$ *if and only if*

$$a^{(p-1)/2} \equiv 1 \pmod p.$$

Corollary. *The equation* $x^2 \equiv a \pmod p$ *has no solution if and only if* $a^{(p-1)/2} \equiv -1 \pmod p$*. Thus* $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$*.*

Proof. This follows from Euler's Criterion and the fact that the polynomial $x^2 - 1$ has no roots besides $+1$ and -1. □

Example 2. *Suppose* $p = 11$*. By squaring each element of* $(\mathbb{Z}/11\mathbb{Z})^*$*, we see that the squares modulo* 11 *are* $\{1,3,4,5,9\}$*. We compute* $a^{(p-1)/2} = a^5$ *for each* $a \in (\mathbb{Z}/11\mathbb{Z})^*$ *and get*

$$\begin{aligned}&1^5 = 1,\ 2^5 = -1,\ 3^5 = 1,\ 4^5 = 1,\ 5^5 = 1, \\ &6^5 = -1,\ 7^5 = -1,\ 8^5 = -1,\ 9^5 = 1,\ 10^5 = -1.\end{aligned}$$

Thus the a *with* $a^5 = 1$ *are* $\{1,3,4,5,9\}$*, just as Euler's Criterion predicts.*

Lemma (Gauss's Lemma)**.** *Let p be an odd prime and let a be an integer $\not\equiv 0 \pmod{p}$. Form the numbers*

$$a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a$$

and reduce them modulo p to lie in the interval $(-\frac{p}{2},\ \frac{p}{2})$, i.e., for each of the above products $k \cdot a$ find a number in the interval $(-\frac{p}{2},\ \frac{p}{2})$ that is congruent to $k \cdot a$ modulo p. Let ν be the number of negative numbers in the resulting set. Then

$$\left(\frac{a}{p}\right) = (-1)^{\nu}.$$

Lemma. *Let $a, b \in \mathbb{Q}$. Then for any integer n,*

$$\#\left((a,b) \cap \mathbb{Z}\right) \equiv \#\left((a, b+2n) \cap \mathbb{Z}\right) \pmod{2}$$

and

$$\#\left((a,b) \cap \mathbb{Z}\right) \equiv \#\left((a-2n, b) \cap \mathbb{Z}\right) \pmod{2},$$

provided that each interval involved in the congruence is nonempty.

Proposition (Euler)**.** *Let p be an odd prime and let a be a positive integer with $p \nmid a$. If q is a prime with $q \equiv \pm p \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Proposition (Legendre Symbol of 2)**.** *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Proof. When $a = 2$, the set $S = \{a, 2a, \ldots, \frac{p-1}{2}a\}$ is

$$\{2, 4, 6, \ldots, p-1\}.$$

We must count the parity of the number of elements of S that lie in the interval $I = (\frac{p}{2}, p)$. Writing $p = 8c + r$, we have

$$\begin{aligned} \#\left(I \cap S\right) &= \#\left(\frac{1}{2}I \cap \mathbb{Z}\right) = \#\left(\left(\frac{p}{4}, \frac{p}{2}\right) \cap \mathbb{Z}\right) \\ &= \#\left(\left(2c + \frac{r}{4}, 4c + \frac{r}{2}\right) \cap \mathbb{Z}\right) \equiv \#\left(\left(\frac{r}{4}, \frac{r}{2}\right) \cap \mathbb{Z}\right) \pmod{2}, \end{aligned}$$

where the last equality comes from Lemma . The possibilities for r are $1, 3, 5, 7$. When $r = 1$, the cardinality is 0; when $r = 3, 5$ it is 1; and when $r = 7$ it is 2. □

Definition (Root of Unity)**.** *An nth* root of unity *is a complex number ζ such that $\zeta^n = 1$. A root of unity ζ is a* primitive *nth root of unity if n is the smallest positive integer such that $\zeta^n = 1$.*

For example, -1 is a primitive second root of unity, and $\zeta = \frac{\sqrt{-3}-1}{2}$ is a primitive cube root of unity. More generally, for any $n \in \mathbb{N}$ the complex number

$$\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$$

is a primitive nth root of unity (this follows from the identity $e^{i\theta} = \cos(\theta) + i\sin(\theta)$). For the rest of this section, we fix an odd prime p and the primitive pth root $\zeta = \zeta_p$ of unity.

Definition (Gauss Sum)**.** *Fix an odd prime p. The* Gauss sum *associated to an integer a is*

$$g_a = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^{an},$$

where $\zeta = \zeta_p = \cos(2\pi/p) + i\sin(2\pi/p) = e^{2\pi i/p}$.

Proposition (Gauss Sum)**.** *For any a not divisible by p,*

$$g_a^2 = (-1)^{(p-1)/2} p.$$

Lemma. *For any integer a,*

$$\sum_{n=0}^{p-1} \zeta^{an} = \begin{cases} p & \text{if } a \equiv 0 \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $a \equiv 0 \pmod{p}$, then $\zeta^a = 1$, so the sum equals the number of summands, which is p. If $a \not\equiv 0 \pmod{p}$, then we use the identity

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$$

with $x = \zeta^a$. We have $\zeta^a \neq 1$, so $\zeta^a - 1 \neq 0$ and

$$\sum_{n=0}^{p-1} \zeta^{an} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = \frac{1-1}{\zeta^a - 1} = 0.$$

□

Lemma. *If x and y are arbitrary integers, then*

$$\sum_{n=0}^{p-1} \zeta^{(x-y)n} = \begin{cases} p & \text{if } x \equiv y \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This follows from last Lemma by setting $a = x - y$. □

Lemma. *We have $g_0 = 0$.*

Proof. By definition

$$g_0 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right). \tag{1}$$

the map

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$$

is a surjective homomorphism of groups. Thus, half the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ map to +1 and half map to −1 (the subgroup that maps to +1 has index 2). Since $\left(\frac{0}{p}\right) = 0$, the sum is 0. □

Lemma. *For any integer a,*

$$g_a = \left(\frac{a}{p}\right) g_1.$$

Proof. When $a \equiv 0 \pmod{p}$, the lemma follows from last Lemma, so suppose that $a \not\equiv 0 \pmod{p}$. Then,

$$\left(\frac{a}{p}\right) g_a = \left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{an} = \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta^{an} = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta^{m} = g_1.$$

Here, we use that multiplication by a is an automorphism of $\mathbb{Z}/p\mathbb{Z}$. Finally, multiply both sides by $\left(\frac{a}{p}\right)$ and use that $\left(\frac{a}{p}\right)^2 = 1$. □