Number theory and Cryptography

Chao Qin

School of Mathematical Sciences

May 28th, 2024

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*.

Quadratic Reciprocity

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.

Quadratic Reciprocity

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

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

Quadratic Reciprocity

Lemma

The map $\psi : (\mathbf{Z}/p\mathbf{Z})^* \to \{\pm 1\}$ *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

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

Quadratic Reciprocity

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

Is 69 a square modulo the prime 389? We have

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

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

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

Thus 69 is a square modulo 389.

Quadratic Reciprocity

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

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 . □

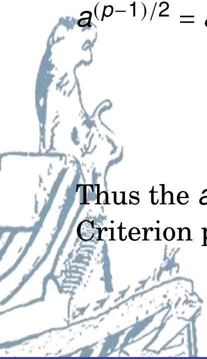
Quadratic Reciprocity

Example

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

$$1^5 = 1,\ 2^5 = -1,\ 3^5 = 1,\ 4^5 = 1,\ 5^5 = 1,$$
$$6^5 = -1,\ 7^5 = -1,\ 8^5 = -1,\ 9^5 = 1,\ 10^5 = -1.$$

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



Quadratic Reciprocity

Lemma (Gauss's Lemma)

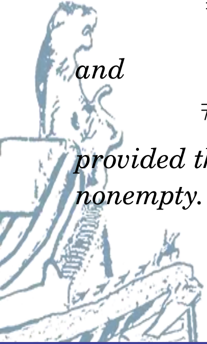
Let p *be an odd prime and let* a *be an integer* $\not\equiv 0 \pmod{p}$*. Form the numbers*

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

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*

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

Quadratic Reciprocity



Lemma

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

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

and

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

provided that each interval involved in the congruence is nonempty.

Quadratic Reciprocity

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

Quadratic Reciprocity

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*

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

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

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

where the last equality comes from Lemma 9. 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 $\zeta^n = 1$.

Quadratic Reciprocity

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 $n \in \mathbf{N}$ 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.