A Bad Intro to Quadratic Reciprocity

Royce Yao

11 June 2023

Formatting done by *evan.sty*

§1 Units

We know that for each positive integer $n \geq 2$, taking $\pmod n$ allows us to get a group $\mathbb{Z}n/\mathbb{Z}$ under addition.

Elements of this group are representation for the entire set of elements with the same remainder under division. This can be checked to be well-defined

$$[a]_n = \{\dots, a-k, a, a+k, \dots\}.$$
$$[a]_n + [b]_n = [a+b]_n$$

holds.

However, it can also be seen that

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

This raise a natural question: when we can do something similar for residues under multiplication?

§1.1 Construction

Suppose that we naively take the case of $\mathbb{Z}6/\mathbb{Z}$ and endow it with multiplication. While $[1]_6$ is an indentity element, and multiplication being associative carries over, we run into a problem with inverses.

Both

$$[1]_6 \cdot [0]_6 = [0]_6$$
$$[2]_6 \cdot [0]_6 = [0]_6$$

hold, so there isn't an inverse to $[0]_6$. As such, this isn't a group. However, it turns getting rid of the elements without these **modular inverses** gives a group.

Definition 1.1 (Modular Inverses)**.** Let the **modular inverse**, if it exists, of $[a]_n$ be some $[b]_n$ such that

$$[a]_n \cdot [b]_n = [1]_n.$$

An element with a modular inverse is called a **unit**.

Example 1.2
Find the units when $n = 6$.

For this, we can construct the multiplication table

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

It turns out that only 1 and 5 seem to be units. They are also the only residues relatively prime to 6. As a matter of fact, we can prove this.

Theorem 1.3 (Unit $\iff$ Relatively Prime)
An element $[a]_n$ is a unit if and only if $\gcd(a, n) = 1$ where a is any representative.

Proof. Suppose that $\gcd(a, n) = 1$. Then consider the infinite sequence

$$a, a^2, a^3, \cdots$$

All elements of this are also relatively prime with n. Since there are only finitely many residues, there must exist integers $p < q$ such that $a^p \equiv a^q \pmod{n}$. However, then

$$n \mid a^p(a^{q-p} - 1)$$

which in turn means that $a^{q-p} \equiv 1 \pmod{n}$. As such, a^{q-p-1} is an inverse of a.

Now suppose that $\gcd(a, n) = d > 1$. Then, for any residue b, $d \mid ab$. Since $d \mid n$, it follows that ab can not be $1 \pmod{n}$. □

Thus, we remain only with the $\phi(n)$ relatively prime residues that form a group. This group is called the **group of units** U_n.

Exercise 1.4. Compute U_4, U_5, U_7 and U_9.

§1.2 Primitive Roots

This raises the question of how U_n decomposes. As a matter of fact, Group Theory gives us the following classification theorem for decomposing finite Abelian groups such as U_n.

Theorem 1.5 (Fundamental Theorem of Finite Abelian Groups)
If G is a finite Abelian group, then

$$G \cong C_{a_1} \times C_{a_2} \times C_{a_3} \cdots \times C_{a_k}$$

for some integers a_i such that $a_1 \cdot a_2 \cdot \ldots a_k = |G|$.

However, this does not give us actual decompositions, it just guarenteeds the existence of one.

A subcase is when U_n is directly isomorphic to a cyclic group.

Theorem 1.6 (Primitive Roots)

If n is a prime odd power, then

$$U_n \cong C_{\phi(n)}$$

In other words, there exists a $g \in U_n$ such that for each $u \in U_n$, $u = g^k$ for some k. Proofs of this can be decently elementary.

Lemma 1.7 (U_n decomposition)

If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is a prime factorization, then

$$U_n \cong U_{p_1^{e_1}} \times U_{p_2^{e_2}} \times \cdots \times U_{p_k^{e_k}}$$

.

Proof. Take a isomorphism $a \to (a \pmod{p_1^{e_1}}, a \pmod{p_2^{e_2}}, \dots)$. □

Proposition 1.8 (U_{2^k} decomposition)

For $k = 0, 1, 2$ it follows that

$$U_{2^k} \cong C_{2^{k-1}}$$

or in other words they have primitive roots.

For $k \geq 3$,

$$U_{2^k} \cong C_2 \times C_{2^{k-2}}$$

This allows us to decompose units. Considering U_{2^k} in a bit more detail allows us to get the cyclic group decomposition as promised.

Example 1.9

Find the number of integers $1 \leq a \leq 600$ such $600 \mid a^{10} - 1$.

Note that this is equivalent to the number of elements in U_{600} with order dividing 10. We first decompose

$$U_{600} \cong U_8 \times U_3 \times U_{25} \cong C_2 \times C_2 \times C_2 \times C_4 \times C_5$$

The order of an element is the same as the lcm of its order in each of the cyclic groups. Thus, the order in each cyclic group componentwise divides 10. The answer is thus $2 \cdot 2 \cdot 2 \cdot 2 \cdot 1 = \boxed{16}$

§2 Quadratic Residues

A quadratic residue is the following

Definition 2.1 (Quadratic Residue)**.** A residue is q is **quadratic** $\pmod{n}$ if there exists x such

$$x^2 \equiv q \pmod{n}$$

Else, a residue is nonquadratic.

We use the abbreviations QR and NQR here.

Let Q_n be the subset of U_n which is a QR.

Exercise 2.2. Find Q_9.

§2.1 Quadratic Residues mod p

Take p as an odd prime here, and let g be a primitive root of p. The units $\pmod p$ are then

$$g^0, g^1, g^2, \dots, g^{p-2}$$

in some order.

It's easy enough to find the quadratic units then, its just every other power of g (as $p-1$ is even)

$$g^0, g^1, g^2, \dots, g^{p-2}$$

This gives us that there are $\frac{p-1}{2}$ primitive roots.

Proposition 2.3

The product of two residues is a NQR if and only if exactly one of them is a NQR. As such, Q_n is a subgroup of U_n.

Proof. Express as primitive roots. □

§2.2 General Quadratic Residues

Proposition 2.4

$a \in Q_p$ if and only if $a \in Q_{p^k}$ for odd primes p.

Proof. The converse follows immediately. Else, if $a \in Q_{p^k}$ such $b^2 \equiv a \pmod{p^k}$, considering

$$b^2, (b+p^k)^2, (b+2p^k)^2 \dots$$

gives that $a \in Q_{p^{k+1}}$ (as $p \neq 2$) □

Proposition 2.5 (Q_n decomposition)

Once again, we can decompose

$$Q_n \cong Q_{p_1^{e_1}} \times Q_{p_2^{e_2}} \times \cdots \times Q_{p_k^{e_k}}$$

§2.3 Legendre Symbol

Definition 2.6 (Legendre Symbol)**.** Let a be an number and p an odd prime. Then the **Legendre symbol** is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ -1 & a \notin Q_n, a \neq 0 \\ 1 & a \in Q_n \end{cases}$$

Using multiplication properties of QRs and NQRs, we get the following.

Proposition 2.7 (Legendre Symbol is Multiplicative)
It follows that

$$\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$$

.

SImilarily, we get a simple criterion for whether a root is quadratic.

Proposition 2.8 (Euler's Criterion)
We have that

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

As a matter of fact, a surprising relation holds.

Theorem 2.9 (Quadratic Reciprocity)

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

Using this and the multiplication property allows us to simplify large Legendre symbols.

§3 Applications

Problem 3.1 (AIME I 2016/12)**.** Find the least positive integer m such that m^2-m+11 is a product of at least four not necessarily distinct primes.

Problem 3.2 (IMO 1986/1)**.** Let d be any positive integer not equal to $2, 5$ or 13. Show that one can find distinct a, b in the set $\{2, 5, 13, d\}$ such that $ab-1$ is not a perfect square.

Problem 3.3 (IMO 2005/4)**.** Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n=2^n+3^n+6^n-1,\quad n\geq 1.$$

Problem 3.4 (Christmas Theorem)**.** Show that an odd prime p can be expressed as the sum of two squares if and only if p is $1 \pmod 4$.

Problem 3.5. Let p be a prime and n a positive integer. Determine the remainder when $1^n+2^n+\cdots+(p-1)^n$ is divided by p, as a function of n and p.

Problem 3.6 (ARML 2022 I-10)**.** The decimal expansion of the fraction $\frac{1}{664349}=\frac{1}{27343\cdot 243}$ consists of an infinitely repeating block of n digits. Compute the least possible value of n.

Problem 3.7 (OMMC 2023 Final P8)**.** Let p be a prime. Suppose the mean of the nonzero quadratic residues mod p is less than $\frac{p}{2}$. Show that the median of the nonzero quadratic residues mod p is less than $\frac{p}{2}$.