QUADRATIC RECIPROCITY

MAX STEINBERG FOR THE OLGA RADKO MATH CIRCLE
ADVANCED
BASED ON A PACKET BY FRANCISC BOZGAN

1. Warmup: Modular Arithmetic

Let us recall some basics of modular arithmetic.

Definition 1 (modulo)**.** Let a, b be integers and n a positive integer. We say that a is congruent to b modulo n (and we write $a \equiv b \mod p$) if n divides $a - b$. We write $a \mod n$ to denote the remainder of a divided by n.

Problem 1. Let a, b be integers and n a positive integer. Show that $a + b \mod n \equiv (a \mod n) + (b \mod n) \mod n$. Is it true that $a + b \mod n \equiv (a \mod n) + (b \mod n)$?

Problem 2. Let a, b be integers and n a positive integer. Prove that $(a \mod n)(b \mod n) \mod n = ab \mod n$. Is it true that $(a \mod n)(b \mod n) = ab \mod n$?

Problem 3.
(1) To what number between 0 and 6 inclusive is the product $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$ congruent modulo 7?
(2) To what number between 0 and 12 inclusive is the product $3 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 29 \cdot 113$ congruent modulo 13?

Problem 4. Let z be a positive integer. We can write z as a sum $z = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^n a_n$, where each a_i is the i-th digit of a (in base 10).
(1) Show that z is divisible by 3 if and only if the sum $a_0 + a_1 + \cdots + a_n$ is divisible by 3.
(2) Show that z is divisible by 11 if and only if the sum $a_0 - a_1 + a_2 - a_3 \cdots \pm a_n$ is divisible by 11.

2. Quadratic Reciprocity

Now we can start talking about Quadratic Reciprocity. This method was developed intuitively (not actually in the modern form you will see here) by some great number theorists of the 17th and 18th century including Fermat, Euler, Lagrange, and Legendre. They began by looking at the quadratic polynomials modulo a prime p and trying to solve it in the most general forms. Namely, they did not try to solve

$$ax^2 + bx + c = 0$$

in the real or complex numbers, which was already known, but rather

$$ax^2 + bx + c \equiv 0 \mod p \text{ where } p \text{ is a prime number.}$$

We will call such an equation solvable if there exists an integer x_0 such that $ax_0^2 + bx_0 + c \equiv 0 \mod p$. Although they had little success solving this problem, these mathematicians stated some important conjectures in this field that would broadened the field of number theory. A major breakthrough in this direction came when Gauss (in 1798) proved what is now called the Quadratic Reciprocity Law: if p, q are prime numbers and if $p \equiv 1 \mod 4$, then

$$x^2 - p \equiv 0 \mod q \text{ is solvable if and only if } x^2 - q \equiv 0 \mod p \text{ is solvable}$$

and if $p, q \equiv 3 \mod 4$, then

$$x^2 - p \equiv 0 \mod q \text{ is solvable if and only if } x^2 - q \equiv 0 \mod p \text{ is } \textbf{not} \text{ solvable}$$

We will prove this theorem later, but in a more modern formulation. Now let's discuss some of the basics that will lead up to the proof of this theorem.

Theorem (Fundamental Theorem of Arithmetic)**.** Every nonzero integer n can be written uniquely as $n = \pm p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ where r is a positive integer greater than or equal to $1, p_1, \dots p_r$ distinct prime numbers and $a_1, \dots a_r$ are positive integers.

The last (and non-trivial) result that we have to recall in order to proceed further is Fermat's Little Theorem:

Theorem (Fermat's Little Theorem)**.** If a is an integer and p is a prime, then $a^p \equiv a \mod p$.

Problem 5. Prove Fermat's Little Theorem. *Hint: use induction on a and the binomial theorem.*

Definition 2 (quadratic residue)**.** Let a be an integer and p a prime. We say a is a **quadratic residue mod** p if $x^2 - a \mod p$ is solvable, and a **quadratic nonresidue mod** p if $x^2 - a \mod p$ is not solvable.

Now we state our first theorem:

Theorem. Given a prime p and an integer a, the equation $x^2 \equiv a$ has zero, one, or two solutions modulo p.

You can use this theorem without proof. Now we are ready to define the Legendre's symbol:

Definition 3 (Legendre Symbol)**.** Given a prime number p and an integer a, the **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined as

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

Problem 6. Show that $\left(\frac{x^2}{p}\right) = 1$ for each prime p and integer $x, p \nmid x$.

From now on, unless otherwise stated, p is always an odd prime and a an integer.

Problem 7. Show that if a is a quadratic residue modulo p, then $a + kp$ is as well for any integer k.

Thus we may regard Legendre's Symbol as a function from the integers $0 \leq a < p$ to the set $\{-1, 0, 1\}$. Fermat's Little Theorem asserts that if $a^p \equiv a \mod p$, so $a^{p-1} \equiv 1 \mod p$[1], which implies $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. More precisely:

Theorem (Euler's Criterion)**.** If a is an integer and p a prime, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$.

You may use this without proof.

Problem 8. Prove that

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

for all integers a, b and prime numbers p.

We also have a corollary:

Corollary 1 (First Supplement of the Quadratic Reciprocity Law)**.** For every prime number $p \geq 3, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Problem 9. Prove this corollary.

Before we can get to quadratic reciprocity itself, we have to state another intermediate theorem:

Theorem (Second Supplement of the Quadratic Reciprocity Law)**.** We have $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. In other words, 2 is a quadratic residue modulo a prime $p \geq 3$ if and only if $p \equiv \pm 1 \mod 8$.

With all this being said, we conclude with the most important theorem of this part, the Gauss' Law of Quadratic Reciprocity:

Theorem. For any different odd primes p and q,

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

The proof of this fact is pretty tricky, and it will be ommitted. Nevertheless, this won't stop us from using it frequently to deduce other properties about Legendre's symbol.

3. Exercises

(1) What is $\left(\frac{1}{p}\right)$ if p is a prime number of the form $19k + 3$? Is 25 a quadratic residue modulo 79? Is 26 a quadratic residue modulo 79? Is 11718 a quadratic residue modulo 11719 (trust me, this number is indeed prime)?

(2) Compute the following Legendre symbols: $\left(\frac{2}{17}\right), \left(\frac{13}{59}\right), \left(\frac{2012}{103}\right)$,

$$\left(\frac{2^{2012} \cdot 3^{2013} \cdot 5^{2014} \cdot 7^{2015}}{19}\right)$$

(3) In fact, what Gauss proved was $\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$. Prove that

$$(-1)^{\left(\frac{p^2-1}{8}\right)} \equiv \left[\frac{p+1}{4}\right] (\text{mod} 2)$$

for any odd prime number p, using the theorem that Gauss proved. (Note that $[x]$ is the greatest integer smaller or equal to x)

(4) Is 23 a square mod 41? Is 15 a square mod 41? (CHMMC, Winter 2010)

(5) Compute the number of primes p less than 100 such that p divides $n^2 + n + 1$ for some integer n. (CHMMC, Winter 2010)

[1] this requires us to know p is prime, as then a is invertible mod p for any a

(6) Find all the primes p with the property that $7p + 3^p - 4$ is a perfect square. (Junior Balkan MO 2007)(Hint: Use Fermat's Little Theorem)
(7) Prove the following statements:
   (a) -2 is a quadratic residue modulo p if and only if $p \equiv 1$ or $p \equiv 3 \mod 8$;
   (b) -3 is a quadratic residue modulo p if and only if $p \equiv 1 \mod 6$;
   (c) 3 is quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 12$;
   (d) 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 10$.
(8) Show that there exist infinitely many prime numbers of the form $10k + 9$.
(9) Prove that for $n \in \mathbb{N}$, every prime divisor p of number $n^4 - n^2 + 1$ is of the form $12k + 1$ for some integer k.
(10) If p is a prime of the form $4k+1$, prove that $x = \left(\frac{p-1}{2}\right)!$ is a solution of the congruence $x^2 + 1 \equiv 0 \mod p$.
(11) Show there exists a natural number $a < \sqrt{p} + 1$ that is a quadratic nonresidue modulo p. (Hint: Suppose a is a quadratic nonresidue. What can you say about $\left[\frac{p}{a}\right] + 1$?)
(12) (Challenge problem) Prove that an integer a is a quadratic residue modulo every prime number if and only if a is a perfect square.
(13) Evaluate

$$\left[\frac{1}{2003}\right] + \left[\frac{2}{2003}\right] + \left[\frac{2^2}{2003}\right] + \cdots + \left[\frac{2^{2001}}{2003}\right]$$

(Note that $[x]$ is the greatest integer smaller or equal to x)

4. Generalization: The Jacobi Symbol

Definition 4 (Jacobi Symbol)**.** Let a be an integer and b an odd number, and let $b = p_1^{\alpha_1} p_2^{\alpha_1} \dots p_r^{\alpha_r}$ be the factorization of b onto primes. Jacobis symbol $\left(\frac{a}{b}\right)$ is defined as a product of Legendre's symbols, namely

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}$$

If a is a quadratic residue modulo n, then clearly $\left(\frac{a}{n}\right) = 1$. However the converse is not true.

Problem 10. Find a counterexample to this theorem. That is, find some positive integers a, n so that $\left(\frac{a}{n}\right) = 1$ but a is not a quadratic residue modulo n.

Nevertheless, if $\left(\frac{a}{n}\right) = -1$, then a is not a quadratic residue modulo n. All this discussion can be summarized in the following statement:

Theorem. Let a be an integer and b a positive integer, and let $b = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ be the factorization of b onto primes. Then a is a quadratic residue modulo b if and only if a is a quadratic residue modulo $p_i^{\alpha_i}$ for each $i = 1, 2, \dots, r$.

We will not see the proof of this theorem here. One direction is trivial, namely if there exists an x such that $x^2 \equiv a \mod n$, then clearly the same x satisfies $x^2 \equiv a \,(\mathrm{mod} p_i^{\alpha_i})$.

Problem 11. (Challenge problem). If you know the Chinese Remainder Theorem, prove the other direction of t his theorem.

The most beautiful thing about the Jacobi symbol is that it obeys most of the laws that the Legendre's Symbol does.

Theorem. For all integers a, b and odd numbers c, d the following equalities hold:

$$\left(\frac{a+bc}{c}\right) = \left(\frac{a}{c}\right)$$
$$\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$$
$$\left(\frac{a}{cd}\right) = \left(\frac{a}{c}\right)\left(\frac{a}{d}\right)$$

Problem 12. Prove the previous theorem.

We also have that the Jacobi symbol obeys the three reciprocity laws, namely

Theorem. For every odd integer a,

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}, \quad \left(\frac{2}{a}\right) = (-1)^{\left(\frac{a^2-1}{8}\right)}$$

and for any two coprime odd integers a, b it holds that

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

5. Exercises

(1) Show that if $\gcd(ab, nm) = 1$, then $\left(\frac{ab^2}{nm^2}\right) = \left(\frac{a}{n}\right)$.
(2) Let $F(x) = \left(x^2 - 17\right)\left(x^2 - 19\right)\left(x^2 - 323\right)$. Prove that for each m positive integer, the equation

$$F(x) \equiv 0 \mod m$$

has a solution x in $\mathbb{N}$. Show that $F(x) = 0$ doesn't have any integer solutions.
(3) Let $m, n \geq 3$ be positive odd integers. Prove that $2^m - 1$ doesn't divide $3^n - 1$.
(4) Show that if $2n + 1$ and $3n + 1$ are perfect squares, then n is divisible by 40.
(5) Is a natural number uniquely determined by the product of its (positive) divisors?
(6) Show that there are no positive integers x, y, z, t such that $x + y + t^2 = 4xyz$. (Hint: Write the equation as $4zt^2 + 1 = (4zy - 1)(4zx - 1)$; now look at the Jacobi symbol $\left(\frac{-z}{4yz-1}\right)$).
(7) (Challenge Problem) Show that the number of quadratic residues modulo $p^n (n \geq 1)$ is equal to

$$\left[\frac{2^{n-1} - 1}{3}\right] + 2 \text{ for } p = 2, \quad \text{and} \quad \left[\frac{p^{n+1} - 1}{2(p+1)}\right] + 1 \text{ for } p \geq 3$$

(8) (Challenge Problem) Prove that the equation $x^2 = y^3 - 5$ has no integer solutions (x, y).
(9) (Challenge Problem) Prove that $4kxy - 1$ does not divide the number $x^m + y^n$ for any positive integers x, y, k, m, n.