Elementary Number Theory
Math 175, Section 30, Autumn 2010
Shmuel Weinberger (shmuel@math.uchicago.edu)
Tom Church (tchurch@math.uchicago.edu)
www.math.uchicago.edu/~tchurch/teaching/175/

Script 4: Quadratic Reciprocity

Fix a field R, and let $P(x)$ be a polynomial with coefficients in R; that is,

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

with each $a_i \in R$. For any $r \in R$, we can evaluate the polynomial $P(x)$ at r to give a value $P(r) \in R$, defined by

$$P(r) = a_n r^n + a_{n-1} r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \in R.$$

Theorem 4.1 (Division algorithm for linear polynomials)**.** For any $u \in R$, we can write $P(x) = (x - u) \cdot Q(x) \ + \ P(u)$ for some polynomial $Q(x)$.

An element $r \in R$ is called a *root* of the polynomial $P(x)$ if $P(r) = 0$.

Theorem 4.2. If r is a root of $P(x)$, then $P(x) = (x - r) \cdot Q(x)$ for some polynomial $Q(x)$.

Exercise 4.3. If $r_1, \ldots, r_k$ are distinct roots of $P(x)$, then

$$P(x) = (x - r_1)(x - r_2) \cdots (x - r_k) \cdot Q(x)$$

for some polynomial $Q(x)$.

Theorem 4.4. If $P(x)$ is a polynomial of degree n, then $P(x)$ has at most n distinct roots.

Definition 4.5. Fix $m > 1$ and suppose $(a, m) = 1$. If there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{m}$, then a is called a *quadratic residue (mod m)*. If there does not exist such an $x \in \mathbb{Z}$, then a is called a *quadratic nonresidue (mod m)*.

Definition 4.6. If p is an odd prime and $(a, p) = 1$, then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

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

Theorem 4.7. Let p be an odd prime. Then:

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

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

iii. If $(a, p) = 1$, then $\left(\frac{a^2}{p}\right) = 1$ and $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

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

Definition 4.8. Fix an odd integer $n > 0$. We say that a subset $S \subset \{1, \ldots, n-1\}$ is a *half-set* (modulo n) if

1. every element of S is invertible modulo n, and
2. for every y which is invertible modulo n, either there exists $x \in S$ s.t. $y \equiv x \pmod{n}$ or there exists $x \in S$ s.t. $-y \equiv x \pmod{n}$, but not both.

A half-set's purpose in life is to have all of its elements multiplied together: we write $\prod_S$ for the product $\prod_{s \in S} s$.

Theorem 4.9. If S and T are both half-sets modulo n, then $\prod_S \equiv \pm \prod_T \pmod{n}$.

Lemma 4.10. Let p be an odd prime. Let S be the half-set $S = \{1, \ldots, \frac{p-1}{2}\}$, and let $T = \{2, 4, \ldots, p-1\}$. Then T is a half-set modulo p , and $\prod_T \equiv \left(\frac{2}{p}\right) \prod_S \pmod{p}$.

Theorem 4.11. Let p be an odd prime. Then $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1$ or $p \equiv 7 \pmod{8}$, while $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3$ or $p \equiv 5 \pmod{8}$. This can be summarized as $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Lemma 4.12. Let q be an odd prime. Then $\left[\left(\frac{q-1}{2}\right)!\right]^2 \equiv (-1)^{\frac{q-1}{2}}(-1) \pmod{q}$.

In the remainder of this script, we prove Quadratic Reciprocity:

Theorem 4.13 (Quadratic reciprocity)**.** Let p and q be distinct odd primes. Then

- if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$,

  p is a quadratic residue $\pmod q$ if and only if q is a quadratic residue $\pmod p$;

- if $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$,

  p is a quadratic residue $\pmod q$ if and only if q is **not** a quadratic residue $\pmod p$.

Lemma 4.14. This theorem can be summarized as:

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

For the rest of the sheet, fix odd primes p and q. Let

$$\begin{aligned} S &= \left\{1 \le k \le \frac{pq-1}{2} \,\middle|\, (k, pq) = 1\right\}, \\ A &= \left\{1 \le k \le \frac{pq-1}{2} \,\middle|\, (k, p) = 1\right\}, \\ \text{and } B &= \left\{1 \le k \le \frac{pq-1}{2} \,\middle|\, q|k\right\}. \end{aligned}$$

Lemma 4.15. S is a half-set modulo pq, the set B is contained in the set A, and the set S is the difference $A \setminus B$. Moreover we can write

$$A = \left\{a + px \,\middle|\, 1 \le a \le p-1, 0 \le x < \frac{q-1}{2}\right\} \cup \left\{a + px \,\middle|\, 1 \le a \le \frac{p-1}{2}, x = \frac{q-1}{2}\right\}$$

and

$$B = \left\{qa \,\middle|\, 1 \le a \le \frac{p-1}{2}\right\}.$$

Lemma 4.16. We have:[1]

$$\begin{aligned} \textstyle\prod_A &\equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p \\ \text{and } \textstyle\prod_B &\equiv q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p \end{aligned}$$

Lemma 4.17. Show that

$$\begin{aligned} \textstyle\prod_S &\equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p \\ \text{and } \textstyle\prod_S &\equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod q \end{aligned}$$

[1]Both are mod p, this is not a typo.

Let

$$T = \left\{ k \in \mathbb{Z} \;\middle|\; \begin{array}{l} 1 \le k < pq \\ k \equiv a \pmod{p} \text{ for } 1 \le a \le p-1 \\ k \equiv b \pmod{q} \text{ for } 1 \le b \le \frac{q-1}{2} \end{array} \right\}$$

Lemma 4.18. T is a half-set modulo pq, with

$$\begin{aligned} \textstyle\prod_T &\equiv \left[(p-1)!\right]^{\frac{q-1}{2}} && \pmod{p} \\ \text{and} \quad \textstyle\prod_T &\equiv \left[\left(\frac{q-1}{2}\right)!\right]^{p-1} && \pmod{q}. \end{aligned}$$

Conclude that

$$\begin{aligned} \textstyle\prod_T &\equiv (-1)^{\frac{q-1}{2}} && \pmod{p} \\ \text{and} \quad \textstyle\prod_T &\equiv (-1)^{\frac{q-1}{2}\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} && \pmod{q}. \end{aligned}$$

Theorem 4.19.

$$\begin{aligned} &\text{If } \left(\frac{q}{p}\right) \equiv 1 \pmod{p}, \quad \text{then} \quad \left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod{q}, \\ &\text{while if } \left(\frac{q}{p}\right) \equiv -1 \pmod{p}, \quad \text{then} \quad -\left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod{q}. \end{aligned}$$

Theorem 4.13 (Quadratic reciprocity)**.** Let p and q be distinct odd primes. Then

- if $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$,

  p is a quadratic residue $\pmod{q}$ if and only if q is a quadratic residue $\pmod{p}$;

- if $p \equiv 3 \pmod{4}$ and $q \equiv 3 \pmod{4}$,

  p is a quadratic residue $\pmod{q}$ if and only if q is **not** a quadratic residue $\pmod{p}$.