Chapter 9 of Number Theory with Computer Applications
by Kumanduri and Romero;
University of Windsor 62-322 Notes by W.L. Yee.

QUADRATIC CONGRUENCES

9.1 Quadratic Residues

Question: Solve $ax^2+bx+c \equiv 0 \pmod{m}$ where a, b, c are integers and $(2a, m) = 1$. Multiplying by $4a$,

$$4a^2x^2 + 4abx + 4ac \equiv (2ax + b)^2 + 4ac - b^2 \equiv 0 \pmod{m}.$$

Letting $y = 2ax + b$, we are solving the congruence

$$y^2 \equiv b^2 - 4ac \equiv D \pmod{m}.$$

This leads to:

Definition 9.1.1 Let $(a, m) = 1$. If $x^2 \equiv a \pmod{m}$ has an integer solution, then a is a **quadratic residue modulo** m. Otherwise, a is a **quadratic nonresidue modulo** m.

Examples: 1) $m = 5$.

$$\begin{aligned} 1^2 &\equiv 4^2 \equiv 1 \pmod{5} \\ 2^2 &\equiv 3^2 \equiv 4 \pmod{5} \end{aligned}$$

Therefore 1 and 4 are quadratic residues modulo 5 and 2 and 3 are quadratic nonresidues modulo 5.

2) Let $m = 15$.

$$\begin{aligned} 1^2 &\equiv 4^2 \equiv 11^2 \equiv 14^2 \equiv 1 \pmod{15} \\ 2^2 &\equiv 7^2 \equiv 8^2 \equiv 13^2 \equiv 4 \pmod{15} \end{aligned}$$

Therefore 1 and 4 are the only quadratic residues modulo 15.

If $m = p_1^{e_1} \cdots p_k^{e_k}$, then if $x^2 \equiv a \pmod{m}$, then $x^2 \equiv a \pmod{p_i^{e_i}}$ for each $1 \leq i \leq k$.

Conversely, if we solve each congruence $x^2 \equiv a \pmod{p_i^{e_i}}$ to get solutions x_i for $1 \leq i \leq k$, then a solution x to the system of congruences $x \equiv x_i \pmod{p_i^{e_i}}$ is a solution to $x^2 \equiv a \pmod{m}$ by the Chinese Remainder Theorem.

Thus it suffices to solve quadratic congruences modulo p^e.

By Reduction of Exponent, when p is an odd prime, we can solve $x^2 \equiv a \pmod{p^e}$ if we can solve $x^2 \equiv a \pmod{p}$.

Lemma 9.1.3 Let p be an odd prime and a an integer such that $(a, p) = 1$. Then:

a) The equation $x^2 \equiv a \pmod{p}$ has either no solution or exactly two solutions. If x_0 is one solution, then $-x_0 \equiv p - x_0 \pmod{p}$ is the other solution.

b) There are exactly $\frac{p-1}{2}$ quadratic residues modulo p and hence exactly $\frac{p-1}{2}$ quadratic nonresidues modulo p.

Proof: a) Let x, y be solutions to $x^2 \equiv a \pmod{p}$. Then $x^2 \equiv y^2 \pmod{p} \iff p | x^2 - y^2 = (x + y)(x - y) \iff x \equiv \pm y \pmod{p}$.

b) Consider the $p - 1$ equations:

$$\begin{aligned} x^2 &\equiv 1 \pmod{p} \\ x^2 &\equiv 2 \pmod{p} \\ &\vdots \quad\quad \vdots \\ x^2 &\equiv p-1 \pmod{p}. \end{aligned}$$

Each invertible element satisfies exactly one equation. Therefore the total number of solutions is $p-1$. Each equation has no solution or two solutions. Therefore exactly half the equations have solutions, so there are $\frac{p-1}{2}$ quadratic residues modulo p.

We can also prove b) using primitive roots.

Lemma 9.1.4 Let p be a prime and g a primitive root modulo p. Then the

quadratic residues are the even powers $g^2, g^4, \ldots, g^{p-1}$, and the quadratic nonresidues are the odd powers $g, g^3, \ldots, g^{p-2}$.

Proof: $g, g^2, g^3, \ldots, g^{p-1}$ are the invertible elements. $g^{2r} \equiv (g^r)^2$ is a quadratic residue. If $x^2 \equiv g^i$ has a solution g^k, $g^{2k} \equiv g^i$ implies that $2k \equiv i \pmod{p-1}$. $p-1$ is even, so the above equation implies i is even. Therefore the even powers are quadratic residues and the odd powers are quadratic nonresidues.

Definition 9.1.5 Let p be an odd prime and a an integer. The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined by:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \\ 0 & \text{if } p|a \end{cases}$$

Proposition 9.1.7 Let p be an odd prime, and a, b two integers such that $(p, ab) = 1$. Then:

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

b) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

Proof: a) and b) are clear.

c) If $(p, ab) = 1$, let $a \equiv g^i \pmod{p}$ and $b \equiv g^j \pmod{p}$ where g is a primitive root of p. Then $ab \equiv g^{i+j} \pmod{p}$ so that by Lemma 9.1.4 $\left(\frac{a}{p}\right) = (-1)^i$, $\left(\frac{b}{p}\right) = (-1)^j$ and $\left(\frac{ab}{p}\right) = (-1)^{i+j} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

If $(p, ab) \neq 1$, then $p|ab$ so $\left(\frac{ab}{p}\right) = 0$. p divides ab, so either $p|a$ or $p|b$ so that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0$.

Example: Let $a = q_1^{e_1} \cdots q_k^{e_k}$ be a positive integer such that $(a, p) = 1$. Then

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)^{e_1} \cdots \left(\frac{q_k}{p}\right)^{e_k}.$$

Thus determining the Legendre symbol is reduced to determing $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, and $\left(\frac{q}{p}\right)$ for odd primes q.

Proposition 9.1.9: Euler's Criterion Let p be an odd prime and a an integer such that $(a,p)=1$. Then

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

Proof: Let g be a primitive root modulo p. If a is a quadratic residue, then $a \equiv g^{2i} \pmod{p}$ so

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

If a is not a quadratic residue, then $a \equiv g^{2i+1} \pmod{p}$ so

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

Example: Does $x^2 \equiv 8 \pmod{31}$ have a solution?
$\left(\frac{8}{31}\right) = \left(\frac{2}{31}\right)^3$.
$\left(\frac{2}{31}\right) \equiv 2^{15} \equiv (2^5)^3 \equiv 1 \pmod{31}$. Thus $\left(\frac{8}{31}\right) = 1^3 = 1$. Therefore 8 is a quadratic residue modulo 31, so the equation has a solution.

Proposition 9.1.11 Let p be an odd prime. Then

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

Proof: By Euler's Criterion, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ which is 1 if $\frac{p-1}{2}$ is even, i.e. $p \equiv 1 \pmod{4}$, and -1 if $\frac{p-1}{2}$ is odd, i.e. $p \equiv 3 \pmod{4}$.

Example: If an odd prime p is a sum of two squares, then $p \equiv 1 \pmod{4}$.

Proof: Let $x^2+y^2=p$. Then $x^2 \equiv -y^2 \pmod{p}$. Since y is invertible, multiply by $(y^{-1})^2$ to get $(xy^{-1})^2 \equiv -1 \pmod{p}$. Then -1 is a quadratic residue modulo p, so $p \equiv 1 \pmod{4}$ by Proposition 9.1.11.

Example: If a prime p satisfies $p \equiv 1 \pmod 4$, then p is a sum of two squares.

Proof: Let $0 < x < p$ satisfy $x^2 \equiv -1 \pmod p$. We show there exist a and b, $0 \leq a, b < \sqrt{p}$ such that $bx \equiv a \pmod p$. There are $\lfloor \sqrt{p} \rfloor + 1$ choices for each of a and b, so there are $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$ numbers of the form $bx - a$ where $0 \leq a, b < \sqrt{p}$. Therefore two of these are congruent modulo p, say $b_1 x - a_1 \equiv b_2 x - a_2 \pmod p$. Then $(b_1 - b_2)x \equiv (a_1 - a_2) \pmod p$. Since $b_1 \neq b_2$ or $a_1 \neq a_2$, both are nonzero. Let $b = b_1 - b_2$ and $a = a_1 - a_2$. Since $x^2 \equiv -1 \pmod p$, therefore $b^2 x^2 \equiv a^2 \equiv -b^2 \pmod p$ so $p | a^2 + b^2$. Since $0 < a, b < \sqrt{p}$, therefore $p = a^2 + b^2$.

Exercise p. 222 # 7) Show that there are infinitely many primes of the form $4k + 1$ using the properties of $\left(\frac{-1}{p}\right)$. (Recall that the infinitude of primes of the form $4k + 3$ was proved in Exercise 2.2.6, but that method does not apply to primes of the form $4k + 1$.)

Suppose, by contradiction, there are finitely many primes of the form $4k + 1$. Let them be $p_1, \ldots, p_k$. Consider

$$n = (2p_1 p_2 \cdots p_k)^2 + 1.$$

Let p be a prime divisor of n. Then $p \neq p_i$. $-1 \equiv (2p_1 p_2 \cdots p_k)^2 \pmod p$ so by Proposition 9.1.11 p is of the form $4k + 1$–contradiction. Thus there are infinitely many primes of the form $4k + 1$.

Exercises

Exercise p. 221 # 1) Find all quadratic residues and quadratic nonresidues in a complete residue system modulo each of the following integers.

a) 11

$1^2 \equiv (-1)^2 \equiv 1 \pmod{11}$, $2^2 \equiv (-2)^2 \equiv 4 \pmod{11}$, $3^2 \equiv (-3)^2 \equiv 9 \pmod{11}$,

$4^2 \equiv (-4)^2 \equiv 5 \pmod{11}$, $5^2 \equiv (-5)^2 \equiv 3 \pmod{11}$

Therefore the quadratic residues modulo 11 are $1, 4, 9, 5, 3$ and the quadratic nonresidues modulo 11 are $2, 6, 7, 8, 10$.

b) 29

$1^2 \equiv (-1)^2 \equiv 1 \pmod{29}$, $2^2 \equiv (-2)^2 \equiv 4 \pmod{29}$,

$3^2 \equiv (-3)^2 \equiv 9 \pmod{29}$, $4^2 \equiv (-4)^2 \equiv 16 \pmod{29}$,

$5^2 \equiv (-5)^2 \equiv 25 \pmod{29}$, $6^2 \equiv (-6)^2 \equiv 36 \equiv 7 \pmod{29}$,

$7^2 \equiv (-7)^2 \equiv 49 \equiv 20 \pmod{29}$, $8^2 \equiv (-8)^2 \equiv 64 \equiv 6 \pmod{29}$,

$9^2 \equiv (-9)^2 \equiv 81 \equiv 23 \pmod{29}$, $10^2 \equiv (-10)^2 \equiv 100 \equiv 13 \pmod{29}$,

$11^2 \equiv (-11)^2 \equiv 121 \equiv 5 \pmod{29}$, $12^2 \equiv (-12)^2 \equiv 144 \equiv 28 \pmod{29}$,

$13^2 \equiv (-13)^2 \equiv 169 \equiv 24 \pmod{29}$, $14^2 \equiv (-14)^2 \equiv 196 \equiv 22 \pmod{29}$

Therefore the quadratic residues modulo 29 are $1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22$.

The quadratic nonresidues modulo 29 are $2, 3, 8, 10, 11, 12, 13, 14, 17, 18, 19, 21, 26, 27$.

Exercise p. 221 # 2) Evaluate the following Legendre symbols.

c) $\left(\frac{7}{31}\right)$

By Euler's Criterion, $\left(\frac{7}{31}\right) \equiv 7^{15} \pmod{31}$.

$7^2 \equiv 49 \equiv 18 \pmod{31}$

$7^4 \equiv 18^2 \equiv 324 \equiv 14 \pmod{31}$

$7^8 \equiv 14^2 \equiv 196 \equiv 10 \pmod{31}$

Therefore $7^{15} \equiv 7^8 7^4 7^2 7^1 \equiv 10 \times 14 \times 18 \times 7 \equiv 17640 \equiv 1 \pmod{31}$

Therefore $\left(\frac{7}{31}\right) = 1$.

d) $\left(\frac{60}{79}\right)$

First, $\left(\frac{60}{79}\right) = \left(\frac{4}{79}\right)\left(\frac{15}{79}\right) = \left(\frac{15}{79}\right)$. By Euler's Criterion, $\left(\frac{15}{79}\right) \equiv 15^{39} \pmod{79}$.

$15^2 \equiv 225 \equiv 67 \pmod{79}$

$15^4 \equiv 67^2 \equiv 4489 \equiv 65 \pmod{79}$

$15^8 \equiv 65^2 \equiv 4225 \equiv 38 \pmod{79}$

$15^{16} \equiv 38^2 \equiv 1444 \equiv 22 \pmod{79}$

$15^{32} \equiv 22^2 \equiv 484 \equiv 10 \pmod{79}$

Therefore $15^{39} \equiv 15^{32} 15^4 15^2 15^1 \equiv 10 \times 65 \times 67 \times 15 \equiv 653250 \equiv -1 \pmod{79}$.

Therefore $\left(\frac{15}{79}\right) = -1$, so $\left(\frac{60}{79}\right) = -1$.

Exercise p. 221 # 5) Determine all prime numbers p such that $p|n^2+1$ for some integer n.

$p|n^2+1$ for some integer n

if and only if $n^2+1 \equiv 0 \pmod{p}$ for some $n \in \mathbb{Z}$

if and only if $n^2 \equiv -1 \pmod{p}$ for some $n \in \mathbb{Z}$

if and only if $\left(\frac{-1}{p}\right) = 1$

if and only if p is a prime of the form $4k+1$ or $p=2$

Exercise p. 222 # 12) Show that a primitive root modulo p is never a quadratic residue. Determine all primes p for which every quadratic nonresidue is also a primitive root.

Let g be a primitive root modulo p. Then $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Thus by Euler's Criterion, $\left(\frac{g}{p}\right) \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Thus a primitive root modulo p is never a quadratic residue.

There are $\frac{p-1}{2}$ quadratic nonresidues modulo p. There are $\phi(p-1)$ primitive roots in a complete residue system modulo p: if g is a primitive root and $(a, p-1) = 1$, then g^a is also a primitive root. Thus $\phi(p-1) = \frac{p-1}{2}$. Thus $p-1 = 2^k$ for some positive integer k. Thus p is a prime of the form 2^k+1.

If p is a prime of the form 2^k+1, then consider g a primitive root modulo p. Then $g^2, g^4, \cdots, g^{p-1}$ are quadratic residues modulo p and $g, g^3, g^5, \cdots, g^{p-2}$ are quadratic nonresidues modulo p by Lemma 9.1.4. Further, $(2i+1, p-1) = (2i+1, 2^k) = 1$, so the quadratic nonresidues are all primitive roots modulo p.

Note: If $p = 2^k+1$ is a prime, then $k = 2^a$ for some a. $p = 2^{2^a}+1$ is called a Fermat prime.

Proof: Let $k = 2^a\ell$ where ℓ is odd. We show that $\ell = 1$.

$$2^k+1 = 2^{2^a\ell} - (-1)^\ell = (2^{2^a} - (-1))(2^{2^a(\ell-1)} - 2^{2^a(\ell-2)} + \cdots - 2^{2^a} + 1).$$

If $\ell > 1$, then both factors are bigger than 1 making the product composite. Therefore $\ell = 1$ so p is of the form $2^{2^a}+1$.

The only known Fermat primes are $F_0 = 2^{2^0}+1$, $F_1 = 2^{2^1}+1$, F_2, F_3, and F_4.