Quadratic Reciprocity Proofs

Karim El Shenawy

February 2021

Introduction

This course notebook is the collection of theorem proofs, exercises and answers from Unit 7 of the Number Theory Through Inquiry (Mathematical Association of America Textbooks).

Theorems to Mark

7.1 Theorem

Let p be a prime and let a, b, and c be integers with a not divisible by p. Then there are integers b' and c' such that the set of solutions to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ *is equal to the set of solutions to a congruence of the form* $x^2 + b'x + c' \equiv 0 \pmod{p}$

Proof. Suppose p is a prime and let a, b, and c $\in \mathbf{Z}$ with a not divisible by p. Assume that there are integers b' and c' such that the set of solutions to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$. This implies that the value of $ax^2 + bx + c \in \mathbf{Z_p}$. Now, we know that $p \nmid a \implies (a, p) = 1 \implies a \equiv 1 \pmod{p}$. This also implies that the inverse of a exists $a^{-1} \in \mathbf{Z_p}$. Now by direct proof we can express $ax^2 + bx + c \equiv 0 \pmod{p}$ as

$$\begin{aligned}
ax^2 + bx + c &\equiv 0 \pmod{p} \\
a^{-1}(ax^2 + bx + c) &\equiv 0 \times a^{-1} \pmod{p} \\
x^2 + a^{-1}bx + a^{-1}c &\equiv 0 \pmod{p} \\
x^2 + b'x + c' &\equiv 0 \pmod{p} \qquad \textbf{where } b' = a^{-1}b, c' = a^{-1}c
\end{aligned}$$

Thus, if there are integers b' and c' such that the set of solutions to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is equal to the set of solutions to a congruence of the form $x^2 + b'x + c' \equiv 0 \pmod{p}$. □

7.8 Theorem

Suppose p is an odd prime and p does not divide either a or b. Then

$$(\tfrac{ab}{p}) = (\tfrac{a}{p})(\tfrac{b}{p}).$$

Proof. Suppose p is an odd prime and p does not divide either a or b.

- Case 1: a and b are quadratic residues modulo p. Then by 7.7, ab is a quadratic residue. Thus by direct proof,

$$\begin{aligned}(\frac{ab}{p}) &= (\frac{a}{p})(\frac{b}{p})\\ 1 &= 1 \times 1\\ 1 &= 1\end{aligned}$$

- Case 2: a is quadratic residue modulo p and b is a quadratic non-residue modulo p. Then by 7.7, ab is a quadratic non-residue. Thus by direct proof,

$$\begin{aligned}(\frac{ab}{p}) &= (\frac{a}{p})(\frac{b}{p})\\ -1 &= 1 \times -1\\ 1 &= 1\end{aligned}$$

- Case 3: a and b are quadratic non-residues modulo p. Then by 7.7, ab is a quadratic residue. Thus by direct proof,

$$\begin{aligned}(\frac{ab}{p}) &= (\frac{a}{p})(\frac{b}{p})\\ 1 &= -1 \times -1\\ 1 &= 1\end{aligned}$$

□

7.9 Theorem (Euler's Criterion)

Suppose p is an odd prime and p does not divide the natural number a. Then a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$*; and a is quadratic non-residue modulo p if and only if* $a^{(p-1)/2} \equiv -1 \pmod{p}$*. This criterion can be abbreviation using the Legendre symbol:*

$$a^{(p-1)/2} \equiv (\tfrac{a}{p}) \pmod{p}.$$

Proof. Suppose p is an odd prime and p does not divide the natural number a.

- Case 1: a is a quadratic residue modulo p. By definition, $\frac{a}{p} = 1$. Then by direct proof,

$$\Longrightarrow x^2 \equiv a \pmod p (\Longrightarrow (x^2, p) = 1)$$
$$\Longrightarrow {x^2}^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod p$$
$$\Longrightarrow {x^2}^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod p$$
$$\Longrightarrow x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod p$$

Since $(x^2, p) = 1$, then$(x, p) = 1$

$(x, p) = 1 \Longrightarrow x^{p-1} \equiv 1 \pmod p$ **By Fermat's Little Theorem**

$$\Longrightarrow x^{p-1} \equiv 1 \equiv a^{\frac{p-1}{2}} \pmod p$$
$$\Longrightarrow 1 \equiv a^{\frac{p-1}{2}} \pmod p$$
$$\Longrightarrow 1 \equiv a^{\frac{p-1}{2}} \pmod p$$
$$\Longrightarrow \frac{a}{p} \equiv a^{\frac{p-1}{2}} \pmod p \textbf{ since } \frac{a}{p} = 1$$

- Case 2: a is a quadratic non-residue modulo p. By definition, $\frac{a}{p} = -1$. Then $x^2 \equiv a \pmod p$ has no solution. Suppose that for some integer x such that $1 \leq x < p$, there is x^{-1} such that $1 \leq x^{-1} < p$ and $x \cdot x^{-1} \equiv a \pmod p$. Now since we know that $x^2 \equiv a \pmod p$ has no solution, this implies that $x \neq x^{-1}$. Therefore, by direct proof,

$$\prod_{j=1}^{\frac{p-1}{2}} x \cdot x^{-1} \equiv \prod_{j=1}^{\frac{p-1}{2}} a \pmod p \qquad (p-1)! \quad \equiv a^{\frac{p-1}{2}} \pmod p$$
$$-1 \equiv a^{\frac{p-1}{2}} \pmod p \quad \textbf{By Wilson's Theorem}$$
$$\frac{a}{p} \equiv a^{\frac{p-1}{2}} \pmod p$$

Therefore, for any natural number a while p is an odd prime and p does not divide a, then

$$a^{(p-1)/2} \equiv (\tfrac{a}{p}) \pmod p.$$

□

7.16 Theorem

Let p be an odd prime, then

$$(\tfrac{2}{p}) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}.$$

Proof. Let p be an odd prime, then

$$(\tfrac{2}{p}) = \begin{cases} 1 & \text{if}\, p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if}\, p \equiv 3 \text{ or } 5 \pmod 8). \end{cases}.$$

The above can be then expressed as

$$(\tfrac{2}{p}) = (-1)^{\frac{p^2-1}{8}}.$$

Then, by direct proof,

- Case 1: $\frac{2}{p} = 1$ when 2 is a quadratic residue modulo p

$$\begin{aligned}
(-1)^{\frac{p^2-1}{8}} &= (\frac{2}{p}) \\
(-1)^{\frac{p^2-1}{8}} &= 1 && \textbf{By definition} \\
&\implies \frac{p^2-1}{8} \equiv 0 \pmod 2 \\
&\implies \frac{p^2-1}{8} = 2k && \exists k \in \mathbf{Z} \\
&\implies p^2 = 16k + 1 \\
&\implies p^2 \equiv 1 \pmod{16} \\
&\implies p \equiv \sqrt{1} \pmod{16} \\
&\implies p \equiv \pm 1 \pmod{16} \\
&\implies p \equiv \pm 1 \pmod 8
\end{aligned}$$

- Case 2: $\frac{2}{p} = 1$ when 2 is a quadratic non-residue modulo p

$$\begin{aligned}
(-1)^{\frac{p^2-1}{8}} &= (\frac{2}{p}) \\
(-1)^{\frac{p^2-1}{8}} &= -1 && \textbf{By definition} \\
&\implies \frac{p^2-1}{8} \equiv 1 \pmod 2 \\
&\implies \frac{p^2-1}{8} = 2k + 1 && \exists k \in \mathbf{Z} \\
&\implies p^2 = 16k + 9 \\
&\implies p^2 \equiv 9 \pmod{16} \\
&\implies p \equiv \sqrt{9} \pmod{16} \\
&\implies p \equiv \pm 3 \pmod{16} \\
&\implies p \equiv \pm 3 \pmod 8
\end{aligned}$$

Therefore,

$$(\tfrac{2}{p}) = \begin{cases} 1 & \text{if}\, p \equiv \pm 1 \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if}\, p \equiv \pm 3 \equiv 3 \text{ or } 5 \pmod 8). \end{cases}.$$

$\square$

7.23 Theorem

Let p be a prime congruent to 3 modulo 4. Let a be a natural number with $1 < a < p-1$*. Then a is quadratic residue modulo p if and only if* $p-a$ *is a quadratic non-residue modulo p.*

Proof. Let p be a prime congruent to 3 modulo 4. Let a be a natural number with $1 < a < p-1$. Thus, $(p, a) = 1$. Suppose a is a quadratic residue modulo p, then

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv 1 \pmod{p} && \textbf{By Euler's Criterion} \\ a^{\frac{4k+2}{2}} &\equiv 1 \pmod{p} && p = 4k+3, \exists k \in \mathbf{Z} \\ a^{2k+1} &\equiv 1 \pmod{p} \\ a^{2k+1} &\equiv 1 \pmod{p} \end{aligned}$$

Similarly, suppose a is a quadratic non-residue modulo p, then

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv -1 \pmod{p} && \textbf{By Euler's Criterion} \\ a^{\frac{4k+2}{2}} &\equiv -1 \pmod{p} && p = 4k+3, \exists k \in \mathbf{Z} \\ a^{2k+1} &\equiv -1 \pmod{p} \\ a^{2k+1} &\equiv -1 \pmod{p} \end{aligned}$$

Now,

$$\begin{aligned} (p-a)^{\frac{p-1}{2}} &\equiv (p-a)^{2k+1} \pmod{p} \\ &\equiv (0-a)^{2k+1} \pmod{p} && p \equiv 0 \pmod{p} \\ &\equiv -1^{2k+1} a^{2k+1} \pmod{p} \\ &\equiv -1(1) \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

From this result we can conclude that (p-a) is quadratic non-residue modulo p. Now, conversely, suppose that (p-a) is quadratic non-residue modulo p, then

$$\begin{aligned} (p-a)^{\frac{p-1}{2}} &\equiv -1 \pmod{p} \\ (p-a)^{2k+1} &\equiv -1 \pmod{p} \\ -1^{2k+1} a^{2k+1} &\equiv -1 \pmod{p} \\ -a^{2k+1} &\equiv -1 \pmod{p} \\ a^{2k+1} &\equiv 1 \pmod{p} \\ a^{\frac{p-1}{2}} &\equiv 1 \pmod{p} \end{aligned}$$

Thus, by Euler's Criterion, a is a quadratic residue modulo p when (p-a) is quadratic non-residue modulo p. $\square$

7.27 Theorem

Let p be a prime and let i and j be natural numbers with $i \neq j$ satisfying $1 < i, j < \frac{p}{2}$. Then $i^2 \not\equiv j^2 \pmod{p}$.

Proof. Let p be a prime and let i and j be natural numbers with $i \neq j$ satisfying $1 < i, j < \frac{p}{2}$. Suppose by contradiction, $i^2 \equiv j^2 \pmod{p} \implies i^2 - j^2 \equiv (i-j)(i+j) \equiv 0 \pmod{p}$. Thus, $p \mid (i-j)(i+j) \implies p \mid (i-j)$ or $p \mid (i+j)$. However, since $1 < i, j < \frac{p}{2}$, then $i + j < p$ and $|i - j| < p$ which implies that p can not divide $(i + j)$ or $(i - j)$. Therefore $i^2 \not\equiv j^2 \pmod{p}$ holds. $\square$

Practice Theorems from The Golden Rule: Quadratic Reciprocity

7.1 Theorem

Let p be a prime and let a, b, and c be integers with a not divisible by p. Then there are integers b' and c' such that the set of solutions to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is equal to the set of solutions to a congruence of the form $x^2 + b'x + c' \equiv 0 \pmod{p}$

Proof. Suppose p is a prime and let a, b, and c $\in \mathbf{Z}$ with a not divisible by p. Assume that there are integers b' and c' such that the set of solutions to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$. This implies that the value of $ax^2 + bx + c \in \mathbf{Z_p}$. Now, we know that $p \nmid a \implies (a, p) = 1 \implies a \equiv 1 \pmod{p}$. This also implies that the inverse of a exists $a^{-1} \in \mathbf{Z_p}$. Now by direct proof we can express $ax^2 + bx + c \equiv 0 \pmod{p}$ as

$$\begin{aligned}
ax^2 + bx + c &\equiv 0 \pmod{p} \\
a^{-1}(ax^2 + bx + c) &\equiv 0 \times a^{-1} \pmod{p} \\
x^2 + a^{-1}bx + a^{-1}c &\equiv 0 \pmod{p} \\
x^2 + b'x + c' &\equiv 0 \pmod{p} \qquad \textbf{where } b' = a^{-1}b, c' = a^{-1}c
\end{aligned}$$

Thus, if there are integers b' and c' such that the set of solutions to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is equal to the set of solutions to a congruence of the form $x^2 + b'x + c' \equiv 0 \pmod{p}$. $\square$

7.2 Theorem

Let p be a prime, and let b and c be integers. Then there exists a linear change of variable, $y = x + \alpha$ with α an integer, transforming the congruence $x^2 + bx + c \equiv 0 \pmod{p}$ into a congruence of the form $y^2 \equiv \beta \pmod{p}$ for some integer β.

Proof. Given $p \in \mathbf{Z_p}$, and $b, c \in \mathbf{Z}$. By theorem 7.1, we know that $x^2 + bx + c \equiv 0 \pmod{p}$. Now suppose that

- $p \neq 2$. Then by direct proof,

$$\begin{aligned} x^2 + bx + c &\equiv 0 \pmod{p} \\ 4 \times (x^2 + bx + c) &\equiv 0 \times 4 \pmod{p} \\ 4x^2 + 4bx + 4c + b^2 - b^2 &\equiv 0 \pmod{p} \\ 4x^2 + 4bx + b^2 + 4c - b^2 &\equiv 0 \pmod{p} \\ (2x+b)^2 + 4c - b^2 &\equiv 0 \pmod{p} \\ (2x+b)^2 &\equiv b^2 - 4c \pmod{p} \\ y' &\equiv b^2 - 4c \pmod{p} \quad \textbf{let } y' = (2x+b)^2 \end{aligned}$$

  Since, $y' = 2x + b$ and $p \nmid 2 \implies (2, p) = 1 \implies 2 \equiv 1 \pmod{p}$, this also implies that the inverse of a exists $2^{-1} \in \mathbf{Z_p}$. Now let $y = y'2^{-1} = (2x+b)(2^-1) = x + 2^{-1}b, \alpha = 2^{-1}b \in \mathbf{Z_p}$. Then α is an integer modulo p. This results to $y^2 \equiv \beta \pmod{p}$ for some integer $\beta = b^2 - 4c$.

- $p = 2$. Then either $x^2 \equiv 0 \pmod{p}$ or $x^2 \equiv 1 \pmod{p}$. This then implies that suppose $x = y$ then $y^2 \equiv \beta \pmod{p}$ for some integer β.

□

7.3 Theorem

Let p be an odd prime. Then half the numbers not congruent to 0 in any complete residue system modulo p are perfect square modulo p and half are not.

Proof. Suppose p $p \in \mathbf{Z_p}, p \neq 2$. Then by Theorem 6.6 and 6.17, we know that every prime p has $\phi(p-1)$ primitive roots and that we can have a primitive root g for each p which forms a complete residue system modulo p as follows,

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

Now since $p \neq 2$, then we can rewrite the above set $\{0, 1, g^2, g^4, g^6, ..., g^{p-3}, g^{p-1}\}$ as $\{0, 1, g^2, (g^2)^2, (g^3)^2, ..., g^{\frac{(p-3)}{2}^2}, g^{\frac{(p-1)}{2}^2}\}$. This implies that there $\frac{p-1}{2}$ numbers in the set $\{0, 1, 2, ..., p-1\}$ that are perfect square and each odd power of g can not be a perfect square. Thus, if g^{2k+1} is perfect square then we have some $x \in \{1, 2, ..., p-1\}$ such that $g^{2k+1} = x^2, 0 < 2k+1 < p-1$.
Now since $x \in \{1, 2, ..., p-1\}$, then $x = g^i, 0 < i \leq p-1$. Thus we have $g^{2k+1} = g^{2i} \implies g^{2k+1-2i} \equiv 1 \pmod{p} \implies p-1 \mid 1$. However, this is a contradiction since p-1 is even and $2k + 1 - 2i = 2(k+1) - i$ is odd. So, no odd power of g is a perfect square modulo p. Since $\{g^0, g, g^2, ..., g^{p-1}\}$ are the result of the powers of $\{0, 1, 2, ..., p-1\}$. We can deduce that $\{0, 1, 2, ..., p-1\}$ is half odd and half even. Thus, there are half the numbers not congruent to 0 in any complete residue system modulo p are perfect square modulo p and half are not. □

7.4 Exercise

Determine which of the numbers $1, 2, 3, ..., 12$ *are perfect squares modulo 13. For each such perfect square, list the number or numbers in the set whose square is that number.*

- $1^2 \equiv 1 \pmod{13}$
- $2^2 \equiv 4 \pmod{13}$
- $3^2 \equiv 9 \pmod{13}$
- $4^2 \equiv 3 \pmod{13}$
- $5^2 \equiv 12 \pmod{13}$
- $6^2 \equiv 10 \pmod{13}$
- $7^2 \equiv 10 \pmod{13}$
- $8^2 \equiv 12 \pmod{13}$
- $9^2 \equiv 3 \pmod{13}$
- $10^2 \equiv 9 \pmod{13}$
- $11^2 \equiv 4 \pmod{13}$
- $12^2 \equiv 1 \pmod{13}$

Thus, the numbers that are perfect squares are 1, 4, 9, 3, 12, 10.

7.5 Question

Can you characterize perfect squares modulo a prime p in terms of their representation as a power of a primitive prime.

Solution. We know that for every prime p, there are $\phi(p-1)$ primitive roots, by Theorem 6.17. Suppose tha the set of all primitive roots modulo p is $\{a_0, a_1, a_2, ..., a_{p-1}\}$.
Any number that is a perfect square can not be primitve root modulo p since a_i is a square of any x thrn x can be written as power of $a_i \pmod{p}$. Hence for each x (perfect square), there exists $b_i \in \mathbf{Z}$ such that

$$a_i^{b_i} \equiv x \pmod{p} \text{ if } b_i \mid \phi(p-1).$$

7.6 Theorem

Let p be a prime. Then half the numbers not congruent to 0 modulo p in any complete residue system modulo p are quadratic residues modulo p and half are quadratic non-residues modulo p.

Proof. Suppose $p \in \mathbf{Z_p}$. By Theorem 6.8, we know that for every prime, there exist at least 1 primitive root modulo p. Suppose that for p, that primitive root is g. Also we know that $(\frac{a}{b}) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Thus,

$$(\frac{a}{b}) \equiv a^{\frac{p-1}{2}} \pmod{p}$$
$$(\frac{g^k}{b}) \equiv g^{k\frac{p-1}{2}} \pmod{p} \qquad \exists k \in \mathbf{Z}$$

Now, g is not a quadratic residue, hence $g^{p-1} \equiv 1 \pmod{p}$. Therefore, $(\frac{a}{b}) \equiv (-1)^k \pmod{p}$.
Moreover, we can suggest that

$$\textstyle\sum_{a=1}^{b-1}(\frac{a}{b}) = \sum_{a=1}^{b-1}(-1)^k = 0.$$

Therefore, half the numbers not congruent to 0 modulo p in any complete residue system modulo p are quadratic residues modulo p and half are quadratic non-residues modulo p. □

7.7 Theorem

Suppose p is an odd prime and p does not divide either of the two integers a or b. Then

1. If a and b are both quadratic residues modulo p, then ab is a quadratic residue modulo p;

   Proof. Given that p is an odd prime and p does not divide either of the two integers a or b. We know that $(\frac{a}{b}) = 1$ if and only if $(\frac{a}{b}) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Therefore, $a \equiv x^k \pmod{p}, \exists k \in \mathbf{Z}$ and $b \equiv y^k \pmod{p}$. This implies that $ab \equiv (xy)^k \pmod{p}$ then ab is a quadratic residue. □

2. If a is quadratic residue modulo p and b is a quadratic non-residue modulo p, then ab is a quadratic non-residue modulo p;

   Proof. Given that p is an odd prime and p does not divide either of the two integers a or b. We know that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. This implies that $(ab)^{\frac{p-1}{2}} \equiv (-1) \pmod{p}$ then ab is a not quadratic residue. □

3. If a and b are both quadratic non-residues modulo p, then ab is a quadratic residue modulo p.

Proof. Given that p is an odd prime and p does not divide either of the two integers a or b. We know that $a^{\frac{p-1}{2}} \equiv -11 \pmod{p}$ and $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. This implies that $(ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then ab is a quadratic residue. □

7.8 Theorem

Suppose p is an odd prime and p does not divide either a or b. Then

$$(\tfrac{ab}{p}) = (\tfrac{a}{p})(\tfrac{b}{p}).$$

Proof. Suppose p is an odd prime and p does not divide either a or b.

- Case 1: a and b are quadratic residues modulo p. Then by 7.7, ab is a quadratic residue. Thus by direct proof,

$$\begin{aligned}(\frac{ab}{p}) &= (\frac{a}{p})(\frac{b}{p})\\ 1 &= 1 \times 1\\ 1 &= 1\end{aligned}$$

- Case 2: a is quadratic residue modulo p and b is a quadratic non-residue modulo p. Then by 7.7, ab is a quadratic non-residue. Thus by direct proof,

$$\begin{aligned}(\frac{ab}{p}) &= (\frac{a}{p})(\frac{b}{p})\\ -1 &= 1 \times -1\\ 1 &= 1\end{aligned}$$

- Case 3: a and b are quadratic non-residues modulo p. Then by 7.7, ab is a quadratic residue. Thus by direct proof,

$$\begin{aligned}(\frac{ab}{p}) &= (\frac{a}{p})(\frac{b}{p})\\ 1 &= -1 \times -1\\ 1 &= 1\end{aligned}$$

□

7.9 Theorem (Euler's Criterion)

Suppose p is an odd prime and p does not divide the natural number a. Then a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$*; and a is quadratic non-residue modulo p if and only if* $a^{(p-1)/2} \equiv -1 \pmod{p}$*. This criterion can be abbreviation using the Legendre symbol:*

$$a^{(p-1)/2} \equiv (\tfrac{a}{p}) \pmod{p}.$$

Proof. Suppose p is an odd prime and p does not divide the natural number a.

- Case 1: a is a quadratic residue modulo p. By definition, $\frac{a}{p} = 1$. Then by direct proof,

$$\begin{aligned}
&\Longrightarrow x^2 \equiv a \pmod{p} (\Longrightarrow (x^2, p) = 1) \\
&\Longrightarrow x^{2^{\frac{p-1}{2}}} \equiv a^{\frac{p-1}{2}} \pmod{p} \\
&\Longrightarrow x^{2^{\frac{p-1}{2}}} \equiv a^{\frac{p-1}{2}} \pmod{p} \\
&\Longrightarrow x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p} \\
&\text{Since } (x^2, p) = 1, \text{ then} (x, p) = 1 \\
&(x, p) = 1 \Longrightarrow x^{p-1} \equiv 1 \pmod{p} \qquad \textbf{By Fermat's Little Theorem} \\
&\Longrightarrow x^{p-1} \equiv 1 \equiv a^{\frac{p-1}{2}} \pmod{p} \\
&\Longrightarrow 1 \equiv a^{\frac{p-1}{2}} \pmod{p} \\
&\Longrightarrow 1 \equiv a^{\frac{p-1}{2}} \pmod{p} \\
&\Longrightarrow \frac{a}{p} \equiv a^{\frac{p-1}{2}} \pmod{p} \ \textbf{since } \frac{a}{p} = 1
\end{aligned}$$

- Case 2: a is a quadratic non-residue modulo p. By definition, $\frac{a}{p} = -1$. Then $x^2 \equiv a \pmod{p}$ has no solution. Suppose that for some integer x such that $1 \leq x < p$, there is x^{-1} such that $1 \leq x^{-1} < p$ and $x \cdot x^{-1} \equiv a \pmod{p}$. Now since we know that $x^2 \equiv a \pmod{p}$ has no solution, this implies that $x \neq x^{-1}$. Therefore, by direct proof,

$$\begin{aligned}
\prod_{j=1}^{\frac{p-1}{2}} x \cdot x^{-1} &\equiv \prod_{j=1}^{\frac{p-1}{2}} a \pmod{p} \qquad (p-1)! \ \equiv a^{\frac{p-1}{2}} \pmod{p} \\
-1 &\equiv a^{\frac{p-1}{2}} \pmod{p} \quad \textbf{By Wilson's Theorem} \\
\frac{a}{p} &\equiv a^{\frac{p-1}{2}} \pmod{p}
\end{aligned}$$

Therefore, for any natural number a while p is an odd prime and p does not divide a, then

$$a^{(p-1)/2} \equiv (\tfrac{a}{p}) \pmod{p}.$$

□

7.10 Theorem

Let p be an odd prime. Then −1 is a quadratic residue modulo p if and only if p is of the form $4k + 1$ for some integer k. Or, equivalently,

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

Proof. Suppose $p \in \mathbf{Z_p}$. Then by Theorem 7.9, $a^{(p-1)/2} \equiv (\frac{a}{p}) \pmod p$ if p does not divide natural number a. Now we know that p does not divide -1, then $-1^{(p-1)/2} \equiv (\frac{-1}{p}) \equiv -1 \pmod p$ if and only if -1 is a quadratic residue modulo p. This holds if and only if the exponent $\frac{p-1}{2}$ is an even integer which can be expressed as $\frac{p-1}{2} \equiv 0 \pmod 2$ or $\frac{p-1}{2} \equiv 0 \pmod 4$. Now by direct proof,

$$\begin{aligned} &\frac{p-1}{2} \equiv 0 \pmod 4 \\ &p \equiv 1 \pmod 4 \\ &\implies p = 4k+1, \exists k \in \mathbf{Z} \end{aligned}$$

Therefore, p is of the form $4k+1$ for some integer k when -1 is a quadratic residue modulo p. □

7.11 Theorem

Let k be a natural number and $p = 4k + 1$ be a prime congruent to 1 modulo 4. Then

$$(\pm(2k)!)^2 \equiv -1 \pmod p.$$

Proof. Suppose k is a natural number and $p = 4k+1$ is a prime congruent to 1 modulo 4. By Wilson's Theorem, we know that $(p-1)! \equiv -1 \pmod p$. Now suppose residue classes in the interval of $[-2k, 2k]$, then by Wilson's Theorem, $(-1)^{2k}(2k)!(2k)! \equiv -1 \pmod p$ or $((2k)!)^2 \equiv -1 \pmod p$. We also know that the negative square root of -1 is also the square root of -1 thus both of the following holds $(-(2k)!)^2 \equiv ((2k)!)^2 \equiv -1 \pmod p$, thus $(\pm(2k)!)^2 \equiv -1$ (mod p). □

7.12 Theorem (Infinitude of $4k + 1$ Primes Theorem)

There are infinitely many primes congruent to 1 modulo 4.
Hint: if $p_1, p_2, ..., p_r$ are primes each congruent to 1 modulo 4, what can you say about each prime factor of the number $N = (2p_1p_2 \cdots p_r)^2 + 1$?

Proof. Assume that there are primes each congruent to 1 modulo 4, $p_1, p_2, ..., p_r$. Consider $N = (2p_1p_2...p_r)^2 + 1$. Let p be a prime that divides N. The prime p is relative prime to $2, p_1, p_2, ...p_r$, so it is not 2 and is not congruent to 1 modulo 4. But $(2, p_1, p_2, ...p_r)^2 \equiv -1 \pmod p$, so -1 is a quadratic residue modulo p. This contradicts Theorem 7.9, so there cannot be finitely many primes congruent to 1 modulo 4. □

7.13 Lemma

Let p be a prime, a an integer not divisible by p, and $r_1, r_2, ..., r_{\frac{(p-1)}{2}}$ *the representative of* $a, 2a, ..., \frac{p-1}{2}a$ *in the complex residue system*

$$\{-\tfrac{p-1}{2}, ..., -1, 0, 1, ..., \tfrac{p-1}{2}\}.$$

Then

$$a \cdot 2a \cdot ... \cdot \tfrac{p-1}{2}a \equiv (-1)^g (\tfrac{p-1}{2})! \pmod p$$

where g is the number of r_i*'s which are negative.*
Hint: It suffices to show that we never have $r_i \equiv -1 r_j \pmod p$ *for some i and j.*

Proof. Let p be a prime, a an integer not divisible by p, and $r_1, r_2, ..., r_{\frac{(p-1)}{2}}$ the representative of $a, 2a, ..., \frac{p-1}{2}a$ in the complex residue system

$$\{-\tfrac{p-1}{2}, ..., -1, 0, 1, ..., \tfrac{p-1}{2}\}.$$

Suppose $\exists i, j \in \mathbf{Z}$ where $1 \leq i, j \leq \frac{p-1}{2}$ then with $ia \not\equiv ja \pmod p$ implies that $i - j \leq \frac{p-1}{2} < p$. Now, suppose that $r_i \equiv -r_j \pmod p$ for some i and j. Then $ax \equiv ay \pmod p$ where $r_i \equiv ax \pmod p$ and $-r_j \equiv ay \pmod p$, where $-\frac{p-1}{2} \leq k, a \leq \frac{p-1}{2}$. This implies that $p \mid (x-y)a$ but this is a contradiction since $p \nmid a$ and $p \nmid x - y$ since $x - y < p$. Therefore, $r_i \not\equiv -r_j \pmod p$ for some i and j.
Thus,

$$\begin{aligned} r_1 r_2 \cdot ... \cdot r_{\frac{p-1}{2}} &= (-1)^g (1 \cdot 2 \cdot ... \cdot \frac{p-1}{2}) \\ &\textbf{g is number of negative } r_i \\ &= (-1)^g (\frac{p-1}{2})! \pmod p \\ &\textbf{Since, there are } \frac{p-1}{2} \textbf{ and } r_i \not\equiv -r_j \pmod p \end{aligned}$$

□

7.14 Theorem (Gauss' Lemma)

Let p be a prime and a an integer not divisible by p. Let g be the number of representatives of $a, 2a, ..., \frac{p-1}{2}a$ *in the complex system residue* $\{-\frac{p-1}{2}, ..., -1, 0, 1, ..., \frac{p-1}{2}\}$*. Then*

$$(\tfrac{a}{p}) = (-1)^g.$$

Proof. Given that p is be a prime and a an integer not divisible by p, a is relatively prime to p, $a_i \equiv \pm a_j \pmod p$ if and only if $i \neq \pm j \pmod p$. Since $1 \leq i, j \leq \frac{p-1}{2}$, this congruence can only hold if $i = j$. Therefore, $a \cdot 2a \cdot ... \cdot$

$\frac{p-1}{2}a \equiv (-1)^g(\frac{p-1}{2})!$ (mod p), where g is the number of representatives that are negative. Since $(\frac{p-1}{2})!$ is relatively prime to p, $a^{\frac{p-1}{2}}(-1)^g$ (mod p). By Theorem 7.9, a is a quadratic residue if and only if $(-1)^g = 1$. $\square$

7.15 Question

Does the prime's residue class modulo 4 determine whether or not 2 is a quadratic residue? Consider the primes' residue class modulo 8 and see whether the residue class seems to correlate with whether or not 2 is a quadratic residue. Make a conjecture.

Conjecture. *Let p be a prime and a an integer not divisible by p. Then the prime's residue class modulo 4 determine whether or not 2 is a quadratic residue* Incomplete

7.16 Theorem

Let p be an odd prime, then

$$(\tfrac{2}{p}) = \begin{cases} 1 & \text{if}\, p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if}\, p \equiv 3 \text{ or } 5 \pmod 8). \end{cases}.$$

Proof. Let p be an odd prime, then

$$(\tfrac{2}{p}) = \begin{cases} 1 & \text{if}\, p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if}\, p \equiv 3 \text{ or } 5 \pmod 8). \end{cases}.$$

The above can be then expressed as

$$(\tfrac{2}{p}) = (-1)^{\frac{p^2-1}{8}}.$$

Then, by direct proof,

- Case 1: $\frac{2}{p} = 1$ when 2 is a quadratic residue modulo p

$$\begin{aligned}
(-1)^{\frac{p^2-1}{8}} &= (\frac{2}{p}) \\
(-1)^{\frac{p^2-1}{8}} &= 1 && \textbf{By definition} \\
&\implies \frac{p^2-1}{8} \equiv 0 \pmod 2 \\
&\implies \frac{p^2-1}{8} = 2k && \exists k \in \mathbf{Z} \\
&\implies p^2 = 16k+1 \\
&\implies p^2 \equiv 1 \pmod{16} \\
&\implies p \equiv \sqrt{1} \pmod{16} \\
&\implies p \equiv \pm 1 \pmod{16} \\
&\implies p \equiv \pm 1 \pmod 8
\end{aligned}$$

- Case 2: $\frac{2}{p} = 1$ when 2 is a quadratic non-residue modulo p

$$
\begin{aligned}
(-1)^{\frac{p^2-1}{8}} &= (\frac{2}{p}) \\
(-1)^{\frac{p^2-1}{8}} &= -1 && \textbf{By definition} \\
&\implies \frac{p^2-1}{8} \equiv 1 \pmod 2 \\
&\implies \frac{p^2-1}{8} = 2k+1 && \exists k \in \mathbf{Z} \\
&\implies p^2 = 16k+9 \\
&\implies p^2 \equiv 9 \pmod{16} \\
&\implies p \equiv \sqrt{9} \pmod{16} \\
&\implies p \equiv \pm 3 \pmod{16} \\
&\implies p \equiv \pm 3 \pmod 8
\end{aligned}
$$

Therefore,

$$
(\tfrac{2}{p}) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \equiv 3 \text{ or } 5 \pmod 8). \end{cases}.
$$

□

7.17 Exercise

Table 1 shows $(\frac{p}{q})$ for the first several odd primes. For example, the table indicates $(\frac{7}{3}) = 1$, but that $(\frac{3}{7}) = -1$. Make another table that shows when $(\frac{p}{q}) = (\frac{q}{p})$ and when $(\frac{p}{q} \neq (\frac{q}{p})$.

Done manually on book.

7.18 Exercise

Make a conjecture about the relationship between $(\frac{p}{q})$ and $(\frac{q}{p})$ depending on p and q.

Conjecture. *Let p and q be odd primes, then $(\frac{p}{q})$ and $(\frac{q}{p})$ if p is a quadratic residue modulo q and q is a quadratic residue modulo p. Also if p is a quadratic non-residue modulo q and p is a quadratic non-residue modulo p.*

7.19 Theorem (Quadratic Reciprocity Theorem-Reciprocity Part)

Let p and q be odd primes, then

$$
(\tfrac{p}{q}) = \begin{cases} (\tfrac{q}{p}) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -(\tfrac{q}{p}) & \text{if } p \equiv q \equiv 3 \pmod 4). \end{cases}.
$$

Hint: Try to use the techniques used in the case of $(\frac{2}{p})$.

Proof. Let p and q be odd primes. Suppose x is the number of pairs $(a, b), 1 \leq a \leq \frac{q-1}{2}$ such that $-\frac{q}{2} < ap - bq < 0$. Also, for each a, if there is a b for which $ap - bq$ satisfies this pairs of inequalities, then b is unique and $0 \leq a \leq \frac{p}{2}$. By Gauss' Lemma, $(p \mid q) = (-1)^x$.

Similarly, let y be the number of pairs $(a, b), 1 \leq b \leq \frac{p-1}{2}$ such that $-\frac{p}{2} < bq - ap < 0$. For each b, there is at most one value of a for which $bq - ap$ satisfies this pair of inequalities, and $0 < a < \frac{q}{2}$. By Gauss's Lemma, $(b \mid a) = (-1)^y$. Therefore, $(a \mid b)(b \mid a) = (-1)^{x+y}$ where $x + y$ is the number of pairs (a, b) such that $0 < a < \frac{q}{2}, 0 < n < \frac{p}{2}$, and $-\frac{2}{2} < ap - bq < \frac{p}{2}$.

If (a, b) is such a pair, then $(\frac{q-1}{2} - a, \frac{p-1}{2} - b)$ also satisfies these inequalities. These two pairs are distinct unless $a = \frac{q+1}{4} and b = \frac{p+1}{4}$, which can happen if and only if $p \equiv q \equiv 3 \pmod 4$. Therefore, $x + y$ is even unless $p \equiv q \equiv 3 \pmod 4$, in which case $x + y$ is odd. □

7.20 Exercise (Computational Technique)

Given a prime p, show how you can determine whether a number a is quadratic residue modulo p. Equivalently, show how to find $(\frac{a}{p})$. *To illustrate your method, compute* $(\frac{1248}{93})$ *and some other examples.*

Proof. Let p be a prime and a be an integer such that $p \nmid a$. a is said to be a quadratic residue modulo p if there exists some integer x such that

$$x^2 \equiv a \pmod p.$$

We also know that the Legendre Symbol pf a mod p is

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

Also by definition, we know that $(\frac{a}{p}) = 1$ if a is quadratic residue modulo p and $(\frac{a}{p}) = -1$ if a is quadratic non-residue modulo p. Moreover, by the fundamental theorem of arithmetic, we can express a natural number say n as a product of primes such as $n = p_1^{r_1} p_2^{r_2} ... p_t^{r_t}$. Then $(\frac{a}{n}) = (\frac{a}{p_1})^{r_1} (\frac{a}{p_2})^{r_2} ... (\frac{a}{p_t})^{r_t}$. This is called Jacobi Symbol.
If $(\frac{a}{n}) = -1$, then a is a quadratic non-residue modulo n. Thus,

$$(\frac{1248}{93}) = (\frac{1248}{31})(\frac{1248}{3}) = (\frac{8}{31})(\frac{0}{3}) = 0.$$

Therefore, 1248 is a quadratic non-residue modulo 93. □

7.21 Exercise

Find all the quadratic residues modulo 23.

$$x^2 \equiv a \pmod{23}$$

- $1^2 \equiv 1 \pmod{23}$
- $2^2 \equiv 4 \pmod{23}$
- $3^2 \equiv 9 \pmod{23}$
- $4^2 \equiv 16 \pmod{23}$
- $5^2 \equiv 2 \pmod{23}$
- $6^2 \equiv 13 \pmod{23}$
- $7^2 \equiv 3 \pmod{23}$
- $8^2 \equiv 18 \pmod{23}$
- $9^2 \equiv 12 \pmod{23}$
- $10^2 \equiv 8 \pmod{23}$
- $11^2 \equiv 6 \pmod{23}$
- $12^2 \equiv 6 \pmod{23}$
- $13^2 \equiv 8 \pmod{23}$
- $14^2 \equiv 12 \pmod{23}$
- $15^2 \equiv 18 \pmod{23}$
- $16^2 \equiv 3 \pmod{23}$
- $17^2 \equiv 13 \pmod{23}$
- $18^2 \equiv 2 \pmod{23}$
- $19^2 \equiv 16 \pmod{23}$
- $20^2 \equiv 9 \pmod{23}$
- $21^2 \equiv 4 \pmod{23}$
- $22^2 \equiv 1 \pmod{23}$

Thus the set of quadratic residue modulo 23 is $\{1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6\}$

7.22 Theorem

Let p be a prime of the form $p = 2q + 1$ where q is a prime. Then every natural number a, $0 < a < p - 1$, is either a quadratic residue or a primitive root modulo p.

Proof. $\square$

7.23 Theorem

Let p be a prime congruent to 3 modulo 4. Let a be a natural number with $1 < a < p - 1$. Then a is quadratic residue modulo p if and only if $p - a$ is a quadratic non-residue modulo p.

Proof. Let p be a prime congruent to 3 modulo 4. Let a be a natural number with $1 < a < p - 1$. Thus, $(p, a) = 1$. Suppose a is a quadratic residue modulo p, then

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv 1 \pmod{p} && \textbf{By Euler's Criterion} \\ a^{\frac{4k+2}{2}} &\equiv 1 \pmod{p} && p = 4k + 3, \exists k \in \mathbf{Z} \\ a^{2k+1} &\equiv 1 \pmod{p} \\ a^{2k+1} &\equiv 1 \pmod{p} \end{aligned}$$

Similarly, suppose a is a quadratic non-residue modulo p, then

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv -1 \pmod{p} && \textbf{By Euler's Criterion} \\ a^{\frac{4k+2}{2}} &\equiv -1 \pmod{p} && p = 4k + 3, \exists k \in \mathbf{Z} \\ a^{2k+1} &\equiv -1 \pmod{p} \\ a^{2k+1} &\equiv -1 \pmod{p} \end{aligned}$$

Now,

$$\begin{aligned} (p-a)^{\frac{p-1}{2}} &\equiv (p-a)^{2k+1} \pmod{p} \\ &\equiv (0-a)^{2k+1} \pmod{p} && p \equiv 0 \pmod{p} \\ &\equiv -1^{2k+1} a^{2k+1} \pmod{p} \\ &\equiv -1(1) \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

From this result we can conclude that (p-a) is quadratic non-residue modulo p.

Now, conversely, suppose that (p-a) is quadratic non-residue modulo p, then

$$\begin{aligned}
(p-a)^{\frac{p-1}{2}} &\equiv -1 \pmod p \\
(p-a)^{2k+1} &\equiv -1 \pmod p \\
-1^{2k+1}a^{2k+1} &\equiv -1 \pmod p \\
-a^{2k+1} &\equiv -1 \pmod p \\
a^{2k+1} &\equiv 1 \pmod p \\
a^{\frac{p-1}{2}} &\equiv 1 \pmod p
\end{aligned}$$

Thus, by Euler's Criterion, a is a quadratic residue modulo p when (p-a) is quadratic non-residue modulo p. □

7.24 Theorem

Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. Then $p \equiv 3 \pmod 4$.

Proof. Given that p is a prime of the form $p = 2q + 1$ where q is an odd prime. Since q is prime, we can express $q = 2k + 1, \exists k \in \mathbf{Z}$. Then, by direct proof,

$$\begin{aligned}
&p = 2q + 1 && \\
&p = 2(2k + 1) + 1 && \mathbf{q = 2k + 1} \\
&p = 4k + 3 && \\
&p \equiv 4k + 3 \pmod 4 && \\
&p \equiv 3 \pmod 4 && \textbf{since } 4 \mid 4k
\end{aligned}$$

□

7.25 Theorem

Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. Let a be a natural number, $1 < a < p - 1$. Then a is a quadratic residue if and only if $p - a$ is a primitive root modulo p.

Proof. Given that p is a prime of the form $p = 2q + 1$ where q is an odd prime. By Theorem 7.24, $p = 2q+1 \equiv 3 \pmod{4}$. Therefore, if a is a quadratic residue, then $p-a$ is a quadratic non-residue. The order of $p-a$ must divide $p-1 = 2q$, and therefore it must be $1, 2, q$, or $2q$. Since the only residue of order 1 is 1 and the only residue of order 2 is $p-1$ and $1 < p-a < p-1$, the order of $p-a$ must be q or $2q$. Since $p-a$is quadratic non-residue, $(p-a)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Since $\frac{p-1}{2} = q$, the order of $p - a$ is not q. Therefore, the order of $p - a$ is $2q = p - 1$, so $p - a$ is a primitive root.

If $p - a$ is a primitive root, then $(p - a)^{\frac{(p-1)}{2}} 6 \equiv 1 \pmod p$, which implies that $p-a$ is not a quadratic residue. Since $p \equiv 3 \pmod{4}$, a must be a quadratic residue modulo p. □

7.26 Theorem

Let p be a prime and a be an integer. Then a^2 is not a primitive root modulo p.

Proof. Let p be a prime and a be an integer. By contradiction, suppose a^2 is a primitive root modulo p. Then, $ord_p(a^2) = p - 1$, by direct proof,

$$\begin{aligned} (a^2)^{p-1} &\equiv 1 \pmod{p} \quad \textbf{By Fermat's Little Theorem} \\ (a)^{2(p-1)} - 1 &\equiv 0 \pmod{p} \\ (a^{p-1} - 1)(a^{p-1} + 1) &\equiv 0 \pmod{p} \end{aligned}$$

Since p is prime then $p \mid (a^{p-1} - 1)$ or/and $p \mid (a^{p-1} + 1)$.

- Case 1: Suppose $p \mid (a^{p-1} - 1)$. This implies that $a^{p-1} \equiv 1 \pmod{p} \Longrightarrow ord_p(a) \mid p - 1 \Longrightarrow ord_p(a^2) = p - 1$ where p-1 is even. Then $ord_p(a) = p - 1 \not\Longrightarrow ord_p(a^2) = p - 1$ which is a contradiction.
- Case 2: Suppose $p \mid (a^{p-1} + 1)$. This implies that

$$\begin{aligned} a^{p-1} &\equiv -1 \pmod{p} \\ a^{2(p-1)} &\equiv -1^2 \pmod{p} \\ (a^2)^{(p-1)} &\equiv -1 \pmod{p} \end{aligned}$$

Thus, $ord_p(a) = 2(p - 1)$ which is not possible since (p-1, a) = 1.

Therefore. $ord_p(a^2) = p - 1$ is not possible thus a^2 is not a primitive root of p. □

7.27 Theorem

Let p be a prime and let i and j be natural numbers with $i \neq j$ satisfying $1 < i, j < \frac{p}{2}$. Then $i^2 \not\equiv j^2 \pmod{p}$.

Proof. Let p be a prime and let i and j be natural numbers with $i \neq j$ satisfying $1 < i, j < \frac{p}{2}$. Suppose by contradiction, $i^2 \equiv j^2 \pmod{p} \Longrightarrow i^2 - j^2 \equiv (i - j)(i + j) \equiv 0 \pmod{p}$. Thus, $p \mid (i - j)(i + j) \Longrightarrow p \mid (i - j)$ or $p \mid (i + j)$. However, since $1 < i, j < \frac{p}{2}$, then $i + j < p$ and $|i - j| < p$ which implies that p can not divide $(i + j)$ or $(i - j)$. Therefore $i^2 \not\equiv j^2 \pmod{p}$ holds. □

7.28 Theorem

Let p be a prime of the form $p = 2q+1$ where q is an odd prime. Then the complete set of numbers that are not primitive roots modulo p are $1, -1, 2^2, 3^2, ..., q^2$.

Proof. Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. Suppose that the complete set of numbers that are not primitive roots modulo p are $1, -1, 2^2, 3^2, ..., q^2$. Then, by direct proof,

- $(q+1)^2 \equiv q^2 + 2q + 1 \equiv q^2 \pmod{p}$
- $(q+2)^2 \equiv (q+1)^2 + 2(q+1) + 1 \equiv q^2 + 2 \pmod{p}$
- $(q-1)^2 \equiv q^2 - 2q + 1 \equiv q^2 + 2 \pmod{p}$
- Thus, $(q+2)^2 \equiv (q^2-1)^2 \pmod{p}$
- $(q+3)^2 \equiv (q+2)^2 + 2(q+2) + 1 \equiv q^2 + 6 \pmod{p}$
- $(q-2)^2 \equiv q^2 + 4q + 1 \equiv q^2 + 6 \pmod{p}$
- Thus, $(q+3)^2 \equiv (q^2-2)^2 \pmod{p}$

Now,

$$(2q)^2 \equiv 4q^2 \equiv -4q - 1 \equiv 1 \pmod{p}$$

Therefore, $1, -1, 2^2, 3^2, ..., q^2$ are the complete set of numbers that are not primitive roots modulo p. □

Alternate Proof:

Proof. Let p be a prime of the form $p = 2q+1$ where q is an odd prime. Suppose that the complete set of numbers that are not primitive roots modulo p are $1, -1, 2^2, 3^2, ..., q^2$. Since for any $a \in \{2, 3, .., q-1\}$ then $(a^2)^b \equiv a^{2b} \equiv a^{q-1} \equiv 1 \pmod{q}$, thus $ord_p(a^2) = p < q$ which implies that a^2 is not a primitive root modulo q. □

7.29 Theorem

Let p be a prime of the form $p = 2q + 1$ where q is an odd prime. Then the complete set of numbers that are primitive roots modulo are $-2^2, -3^2, ..., -q^2$.

Proof. Let p be a prime of the form $p = 2q+1$ where q is an odd prime. Suppose the complete set of numbers that are primitive roots modulo are $-2^2, -3^2, ..., -q^2$. Then p is odd prime so for any $a \in \{2, 3, ..., q-1\}$. Now $(-a)^2 p \equiv -1 \pmod{q}$ so $-a^2$ is a primitive root modulo p.
Now, we must prove that the set $-2^2, -3^2, ..., -q^2$ contains all primitive roots and the set $1, -1, 2^2, 3^2, ..., q^2$ contains all non-primitive roots (By Theorem 7.28). If we prove that the union of both these sets forms $\mathbf{Z_q}$. Then we are done. Now note that for $a \neq b$ then

$$\begin{aligned} &\implies a^2 \equiv b^2 \pmod{q} \qquad\qquad a, b \in \{1, 2, 3, .., q-1\} \\ &\implies a \equiv -b \pmod{q} \end{aligned}$$

So,

$$\{1^2, 2^2, 3^2, .., (q-1)^2\} = \tfrac{q-1}{2} = p.$$

Similarly,

$$\{-2^2, -3^2, .., -(q-1)^2\} = p - 1.$$

Thus, all sets are disjoint. Therefore, the complete set of numbers that are primitive roots modulo are $-2^2, -3^2, ..., -q^2$. $\square$

7.30 Exercise

Verify that the primitive roots modulo 23 that we listed earlier in this section are in fact the same as those given by Miller's Theorem.

- $1^2 \equiv 22^2 \equiv 1 \pmod{23}$
- $2^2 \equiv 21^2 \equiv 4 \pmod{23}$
- $3^2 \equiv 20^2 \equiv 9 \pmod{23}$
- $4^2 \equiv 19^2 \equiv 16 \pmod{23}$
- $5^2 \equiv 18^2 \equiv 2 \pmod{23}$
- $6^2 \equiv 17^2 \equiv 13 \pmod{23}$
- $7^2 \equiv 16^2 \equiv 3 \pmod{23}$
- $8^2 \equiv 15^2 \equiv 18 \pmod{23}$
- $9^2 \equiv 14^2 \equiv 12 \pmod{23}$
- $10^2 \equiv 13^2 \equiv 8 \pmod{23}$
- $11^2 \equiv 12^2 \equiv 6 \pmod{23}$

Thus the set of quadratic residue modulo 23 is $\{1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6\}$

7.31 Exercise

List the primitive roots and quadratic residues modulo 47.

- $1^2 \equiv 46^2 \equiv 1 \pmod{47}$
- $2^2 \equiv 45^2 \equiv 4 \pmod{47}$
- $3^2 \equiv 44^2 \equiv 9 \pmod{47}$
- $4^2 \equiv 43^2 \equiv 16 \pmod{47}$
- $5^2 \equiv 42^2 \equiv 25 \pmod{47}$
- $6^2 \equiv 41^2 \equiv 36 \pmod{47}$
- $7^2 \equiv 40^2 \equiv 2 \pmod{47}$
- $8^2 \equiv 39^2 \equiv 17 \pmod{47}$

- $9^2 \equiv 38^2 \equiv 34 \pmod{47}$
- $10^2 \equiv 37^2 \equiv 6 \pmod{47}$
- $11^2 \equiv 36^2 \equiv 27 \pmod{47}$
- $12^2 \equiv 35^2 \equiv 3 \pmod{47}$
- $13^2 \equiv 34^2 \equiv 28 \pmod{47}$
- $14^2 \equiv 33^2 \equiv 8 \pmod{47}$
- $15^2 \equiv 32^2 \equiv 37 \pmod{47}$
- $16^2 \equiv 31^2 \equiv 21 \pmod{47}$
- $17^2 \equiv 30^2 \equiv 7 \pmod{47}$
- $18^2 \equiv 29^2 \equiv 42 \pmod{47}$
- $19^2 \equiv 28^2 \equiv 32 \pmod{47}$
- $20^2 \equiv 27^2 \equiv 24 \pmod{47}$
- $21^2 \equiv 26^2 \equiv 18 \pmod{47}$
- $22^2 \equiv 25^2 \equiv 14 \pmod{47}$
- $23^2 \equiv 24^2 \equiv 12 \pmod{47}$

Thus the set of quadratic residue modulo 23 is

$$\{1, 4, 9, 16, 25, 36, 2, 17, 34, 6, 27, 3, 28, 8, 37, 21, 7, 42, 32, 24, 18, 14, 12\}$$

7.32 Blank Paper Exercise

- Quadratic Congruences
- Quadratic Residues
- Legendre Symbol
- Euler's Criterion
- Gauss' Lemma
- Quadratic Reciprocity
- Sophie Germain

Diagramming Numbers Modulo a Prime

7.1.1 Exercise

Construct squaring diagrams similar to that of Figure 7.1 for all primes up to p = 31 by hand.

7.1.2 Theorem

Let p be prime. For $0 \leq a \leq p$*, the only solutions to the congruence* $a^2 \equiv 0 \pmod{p}$ *are* $a = 0$ *and* $a = p$*.*

Proof. Let p be prime. For $0 \leq a \leq p$, the only solutions to the congruence $a^2 \equiv 0 \pmod{p}$ are $a = 0$ and $a = p$. Since $p \nmid a$ when $0 \leq a \leq p$. $\square$

7.1.3 Theorem

Let p be an odd prime and let a, b *be integers,* $1 \leq a < b < p$*, such that* $a^2 \equiv b^2 \pmod{p}$*. Then* $a + b = p$*.*

Proof. Let p be an odd prime and let a, b be integers, $1 \leq a < b < p$, such that $a^2 \equiv b^2 \pmod{p}$. Then by direct proof,

$$\begin{aligned} a^2 &\equiv b^2 \pmod{p} \\ a &\equiv b \pmod{p} \\ a + b &\equiv 0 \pmod{p} \end{aligned}$$

Then, $p \mid a + b \implies a + b = kp, \exists k \in \mathbf{Z}$. Thus, $a + b = p$. $\square$

7.1.4 Exercise

Denote the tree rooted at 1 in the squaring diagram as T_1*.*

7.1.5 Theorem

Let $p = 2^k m + 1$*, with m an odd prime.*

Proof. Suppose prime p such that $p = 2^k m + 1$, with m an even prime. Then,

$$\begin{aligned} p &= 2^k(2) + 1 \\ p &= 2^{k+1} + 1 \end{aligned}$$

Now by Fermat's Little Theorem,

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ a^{2^k} &\equiv 1^{0.5} \pmod{p} \\ a^{2^k} &\equiv 1 \pmod{p} \end{aligned}$$

Thus, m must be odd. $\square$

7.1.6 Theorem

If p is a Fermat prime, the squaring diagram for p consists of the single binary tree T_1.

7.1.7 Theorem

Let $p = 2^k m + 1$ be prime.

7.1.8 Question

For p prime, can you make a conjecture about cycle periods in the squaring diagram?

7.1.9 Question

What conjecture can you make about the relation of the squaring diagram for a prime p and for the composite number $2p$?