Chapter 7

Date: Mar 27 Made by Eric

In this note, n is always a natural number, and $\mathbb{Z}_n$ is always a ring, containing congruence classes of $\equiv_n$, or the cosets of $\mathbb{Z}/n\mathbb{Z}$ if you wish

In this note, p_i is always a prime for each $i \in \mathbb{Z}$

Definitions

Definition 1. *Let $[a] \in U_n$. $[a]$ is a **quadratic residue** mod (n), if $[a] = [s]^2$ for some $s \in U_n$*

Theorem 1. *The set of all quadratic residue constitute a subgroup of U_n*

Proof. Let $[a]$ and $[b]$ be two quadratic residue mod (n), and suppose $[a] = [x]^2, [b] = [y]^2$ for some $[x], [y] \in U_n$

$[a][b] = [xy]^2$

$[1] = [1]^2$

$[a]^{-1} = ([x]^2)^{-1}([x^{-1}])^2$ ■

Definition 2. *The subgroup of all quadratic residue mod n is written Q_n*

Definition 3. *Suppose p is an odd prime. The **Legendre** symbol of any integer $a \in \mathbb{Z}$ is*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \in Q_p \\ -1 & \text{if } a \in U_p \setminus Q_p \end{cases} \tag{1}$$

Theorems

Theorem 2. *Let $n > 2$, and suppose that there is a primitive root g mod (n)*

$$Q_n \text{ is a cyclic group of order } \frac{\varphi(n)}{2}\text{, generated by } g^2$$

Proof. That Q_n is a cyclic group follows immediately from that U_n is a cyclic group

Let $a \in Q_n$

We know $a = (g^j)^2$ for some $j \in \mathbb{Z}$

So every elements in Q_n can be and can only be expressed by even power of g

Then we see $Q_n = \langle g^2 \rangle$ and $|Q_n| = \frac{\varphi(n)}{2}$ ■

Corollary 2.1. *Let p be an odd prime and g be a primitive rood mod (p)*

$$\left(\frac{g^i}{p}\right) = (-1)^i$$

Proof. Notice that if i is even, then $g^i \in Q_n$, and if i is odd, then $g^i \notin Q_n$ ∎

Theorem 3. *Let p be an odd prime*

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

Proof. Notice if any of a or b is divided by p, then both $\left(\frac{ab}{p}\right)$ and $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ are 0

We know U_p is cyclic, so we pick a primitive root g mod p

Express a and b in the form of $a = g^i$ and $b = g^j$

By the following equation, our proof is completed

$$\left(\frac{ab}{p}\right) = \left(\frac{g^{i+j}}{p}\right) = (-1)^{i+j} = (-1)^i(-1)^j = \left(\frac{g^i}{p}\right)\left(\frac{g^j}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

∎

Theorem 4. ***(Euler's Criterion)*** *Let p be an odd prime and a be an integer*

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

Proof. If $p|a$, then both side of the equation is 0

Let g be a primitive rood mod p

If $a \in Q_n$, then we can express a in the form of $a = g^{2n}$ where $n \in \mathbb{Z}$, and we see

$$a^{\frac{p-1}{2}} \equiv_p g^{n(p-1)} \equiv_p (g^{p-1})^n \equiv_p 1 \equiv_p \left(\frac{a}{p}\right)$$

If $a \notin Q_n$, then we can express a in the form of $a = g^{2n+1}$ where $n \in \mathbb{Z}$, and we have the

$$a^{\frac{p-1}{2}} \equiv_p g^{(2n+1)\frac{p-1}{2}} \equiv_p g^{n(p-1)} g^{\frac{p-1}{2}} \equiv_p g^{\frac{p-1}{2}}$$

$\mathbb{Z}_p$ is a field, so $x^2 \equiv_p 1$ can have at most two solution. Obviously, 1 and -1 are the two solutions.

Notice $(g^{\frac{p-1}{2}})^2 \equiv_p g^{p-1} \equiv_p 1$, so we deduce $g^{\frac{p-1}{2}} \equiv_p 1$ or -1

Because U_p is cyclic and $|U_p| = p-1$, we deduce $g^{\frac{p-1}{2}} \not\equiv_p 1$, which give us $g^{\frac{p-1}{2}} \equiv_p -1 \equiv_p \left(\frac{a}{p}\right)$

∎

Corollary 4.1. *Let p be an odd prime*

$$-1 \in Q_p \iff p \equiv_4 1$$

Proof. $(-1) \in Q_p \iff (-1)^{\frac{p-1}{2}} \equiv_p 1 \iff \frac{p-1}{2}$ is even $\iff 2|\frac{p-1}{2} \iff 4|p-1 \iff p \equiv_4 1$ ∎

Theorem 5. ***(Gauss' Lemma)*** *Let p be an odd prime and suppose $a \in U_p$. Let $P = \{1, \ldots, \frac{p-1}{2}\} \subset U_p$ and $N = \{-1, \ldots, -\frac{p-1}{2}\} \subset U_p$*

$$\left(\frac{a}{p}\right) = (-1)^{|aP \cap N|}$$

Proof. We first prove the following fact that is intuitive numerically, yet obscure algebraicly.

$$aP = \{\varepsilon_i i | i \in P\}, \varepsilon_i = 1 \text{ or } -1 \text{(fact)}$$

Arbitrarily pick two elements from aP and express them in the form of ax and ay, where $x, y \in P$

$ax \not\equiv_p ay$ follows immediately from its construction

Assume $ax \equiv_p -ay$

$a(x+y) \equiv_p 0 \implies p|a(x+y)$

Because $a \in U_p$, so we deduce $p|x+y$

Notice $1 \leq x, y \leq \frac{p-1}{2} \implies x + y \leq p - 1$ CaC

Now we have concluded $ax \not\equiv_p \pm ay$

This tell us that each element of aP lies in one of the following cells and no two elements of aP lies in the same cell. (done)

$$\{\pm 1\}, \{\pm 2\}, \ldots, \{\pm \frac{p-1}{2}\}$$

With fact, we deduce

$$a^{\frac{p-1}{2}}(\frac{p-1}{2})! = a^{|P|}\Pi P = \Pi aP = \Pi_{i \in P}\varepsilon_i i$$

Notice $\varepsilon_i = -1 \iff \varepsilon_i i \in N$, so we deduce there are $|aP \cap N|$ number amount of ε_i satisfy $\varepsilon_i = -1$

We further deduce

$$a^{\frac{p-1}{2}}(\frac{p-1}{2})! = \Pi_{i \in P}\varepsilon_i i = (-1)^{|aP \cap N|}(\frac{p-1}{2})!$$

Cancelling $(\frac{p-1}{2})!$, we deduce

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}} \equiv_p (-1)^{|aP\cap N|}$$

Notice both $\left(\frac{a}{p}\right)$ and $(-1)^{|aP\cap N|}$ can only be 1 or -1, so we see

$$\left(\frac{a}{p}\right) = (-1)^{|aP\cap N|}$$

■

Corollary 5.1. $2 \in Q_p \iff p \equiv_8 \pm 1$

Proof. By **Gauss' Lemma**, we know $\left(\frac{2}{p}\right) = (-1)^{|2P\cap N|}$

$2P = \{2, 4, \ldots, p-1\}$

Notice $2P$ contains all even number smaller than p, which enable us to directly express $2P \cap N$ in the fashion below

We now split our proof into two cases, $\frac{p-1}{2}$ is even, and $\frac{p-1}{2}$ is odd.

Case: $\frac{p-1}{2}$ is even

Notice $N = \{\frac{p-1}{2}+1, \frac{p-1}{2}+2, \ldots, p-1\}$

$2P \cap N = \{\frac{p-1}{2}+2, \frac{p-1}{2}+4, \ldots, p-1\}$

$|2P \cap N| = \frac{p-1}{4} \implies \left(\frac{2}{p}\right) = (-1)^{|2P\cap N|} = (-1)^{\frac{p-1}{4}}$

$\left(\frac{2}{p}\right) = 1 \iff 2|\frac{p-1}{4} \iff 8|p-1 \iff p \equiv_8 1$

Case: $\frac{p-1}{2}$ is odd

$2P \cap N = \{\frac{p-1}{2}+1, \frac{p-1}{2}+3, \ldots, p-1\}$

$|2P \cap N| = \frac{p+1}{4} \implies \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$

$\left(\frac{2}{p}\right) = 1 \iff 2|\frac{p+1}{4} \iff 8|p+1 \iff p \equiv_8 -1$ ■

Theorem 6. ***(Law of Quadratic Reciprocity)*** *Let p and q be two distinct odd primes*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Theorem 7. *Let p be an odd prime, let $e \geq 1$, and let $a \in \mathbb{Z}$*

$$a \in Q_{p^e} \iff a \in Q_p$$

Proof. Let g be a primitive root mod p^e

We first prove g is also a primitive root mod p

Let g be of order q in $U_{p^{e-1}}$

$g^q \equiv_{p^{e-1}} 1$ so we can express g^q in the form of $g^q = kp^{e-1} + 1$

$g^{pq} \equiv_{p^e} (g^q)^p \equiv_{p^e} kp^{e-1}\binom{p}{1} + 1 \equiv_{p^e} 1 \implies g$ have order smaller than pq in U_{p^e}, which is only possible if $q = p^{e-1}$, so g is of the order p^{e-1} in $U_{p^{e-1}}$; that is, g is a primitive root mod p^{e-1}

By repeatedly using the same argument, we know g is a primitive root mod p (done)

Notice Q_{p^e} and Q_p both contain exactly the even power of g, so $a \in Q_{p^e} \iff a \in Q_p$

■

Theorem 8. *Let a be an odd integer and $e \geq 3$*

$$a \in Q_{2^e} \iff a \equiv_8 1$$

Proof. We first express U_{2^e} in the form of $\{\pm 5^i | 0 \leq i < 2^{e-2}\}$

We first show $Q_{2^e} = \{5^{2i} | 0 \leq i < 2^{e-2}\}$

Let $x \in Q_{2^e}$ and express x in the form of $x \equiv_{2^e} c^2$. Express c in the form of $\pm 5^i$, and we see $x \equiv_{2^e} 5^{2i} \in \{5^{2i} | 0 \leq i < 2^{e-2}\}$

$5^{2i} \equiv_{2^e} (5^i)^2 \implies \{5^{2i} | 0 \leq i < 2^{e-2}\} \subseteq Q_{2^e}$ (done)

And then we show $\{a \in U_{2^e} : a \equiv_8 1\} = \{5^{2i} | 0 \leq i < 2^{e-2}\} = Q_{2^e}$

Notice $5^2 \equiv_8 1$

So $\pm 5^i \equiv_8 1 \iff i$ is even and the sign is positive. (done)

■

Summary

1. Let p be an odd prime. $-1 \in Q_p \iff p \equiv_4 1$ **and** $2 \in Q_p \iff p \equiv_8 \pm 1$ **and** $a \in Q_{p^e} \iff a \in Q_p$

2. $a \in Q_{2^{c_0} p_1^{c_1} \cdots p_k^{c_k}} \iff a \in Q_{p_i}, \forall p_i$ **and** $a \in Q_{2^{c_0}}$

3. Let $e \geq 3$ **and** a **be odd. Then** $a \in Q_{2^e} \iff a \equiv_8 1$

Exercises

7.6

Use a primitive root to find the elements of Q_{25}

Proof. To find a primitive root mod (5^2), we first find a primitive root mod (5)

Notice 2 is a primitive root mod (5)

$\varphi(25) = 5 * 4$

$2^{10} \equiv_{25} -1$ and $2^4 \equiv_{25} 16 \implies 2$ is a primitve root mod (25)

By Theorem 2, we know $Q_{25} = \langle 2^2 \rangle = \langle 4 \rangle = \{4, 16, 14, 6, 24, 21, 9, 11, 19, 1\}$ ■

7.7

Prove $-1 \in Q_{29}$ by factorizing 28

Proof. $-1 \equiv_{29} 28 \equiv_{29} 4 * 7 \implies \left(\frac{-1}{29}\right) = \left(\frac{4}{29}\right)\left(\frac{7}{29}\right) = \left(\frac{4}{29}\right)\left(\frac{36}{29}\right) = 1$

■

7.8

Determine whether 3 and 5 are quadratic residues mod (29)

Proof. $\frac{29-1}{2} = 14$

$3^{14} \equiv_{29} (3^3)^4 3^2 \equiv_{29} (-2)^4 3^2 \equiv_{29} 144 \equiv_{29} -1 \implies 3$ is not a quadratic residues mod (29)

$5^{14} \equiv_{29} (5^2)^7 \equiv_{29} (-4)^7 \equiv_{29} -(4^3)^2(4) \equiv_{29} -6^2(4) \equiv_{29} -28 \equiv_{29} 1 \implies 5$ is a quadratic residues mod (29) ■

7.9

Use Gauss' Lemma to determine whether 3 and 5 are quadratic residues mod (29) and whether $10 \in Q_{29}$

Proof. Let $P = \{1, \ldots, 14\} \subset U_{29}$ and $N = -P \subset U_{29}$

$3P \cap N = 3 * \{5, 6, 7, 8, 9\} \implies \left(\frac{3}{29}\right) = (-1)^5 = -1 \implies 3$ is not a quadratic residues mod (29)

$5P \cap N = 5 * \{3, 4, 5, 9, 10, 11\} \implies \left(\frac{5}{29}\right)(-1)^6 = 1 \implies 5$ is a quadratic residues mod (29)

$10P \cap N = 10 * \{2, 5, 8, 11, 14\} \implies 10 \notin Q_{29}$

■

7.10

For which prime p is $-2 \in Q_p$

Proof.

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

$\left(\frac{-2}{p}\right) = 1$ if and only if

$$\left(\frac{-1}{p}\right) = 1 = \left(\frac{2}{p}\right) \text{ and } \left(\frac{-1}{p}\right) = -1 = \left(\frac{2}{p}\right)$$

We know $-1 \in Q_p \iff p \equiv_4 1$ and $2 \in Q_p \iff p \equiv_8 \pm 1$

$$\text{Case: } \left(\frac{-1}{p}\right) = 1 = \left(\frac{2}{p}\right)$$

$p \equiv_4 1$ and $p \equiv_8 \pm 1 \implies p \equiv_8 1$

$$\text{Case: } \left(\frac{-1}{p}\right) = -1 = \left(\frac{2}{p}\right)$$

$p \not\equiv_4 1$ and $p \not\equiv_8 \pm 1$ and p is odd $(-2 \notin Q_2) \implies p \equiv_8 3$

■

7.11

Is 219 a quadratic residue mod (383)?

Proof. $\left(\frac{219}{383}\right) = \left(\frac{-164}{383}\right)$

$383 \equiv_4 3 \implies \left(\frac{-1}{383}\right) = -1 \implies \left(\frac{219}{383}\right) = \left(\frac{-164}{383}\right) = -\left(\frac{164}{383}\right) = -\left(\frac{4}{383}\right)\left(\frac{41}{383}\right) = -\left(\frac{41}{383}\right)$

$\frac{(41-1)(383-1)}{4}$ is even, so $\left(\frac{41}{383}\right) = \left(\frac{383}{41}\right) = \left(\frac{14}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{7}{41}\right)$

$41 \equiv_4 1 \implies \left(\frac{2}{41}\right) = 1$

$\left(\frac{219}{383}\right) = -\left(\frac{7}{41}\right)$

$\frac{(7-1)(41-1)}{4}$ is even, so $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{-1}{7}\right)$

$\left(\frac{219}{383}\right) = -\left(\frac{-1}{7}\right)$

$7 \equiv_4 3 \implies \left(\frac{-1}{7}\right) = -1$

So $\left(\frac{219}{383}\right) = 1$ ■

7.12

For each of the following integer a, characterize the primes p for which $a \in Q_p$: $a = -3, 5, 6, 7, 10, 169$

Proof. All and only odd a satisfy $a \in Q_2$

$-3 \in Q_p \iff p \equiv_{12} 1$

$5 \in Q_p \iff p \equiv_5 \pm 1$

$6 \in Q_p \iff p \equiv_{24} \pm 1$ or ± 5

$7 \in Q_p \iff p \equiv_{28} \pm 1$ or ± 3 or ± 9

$10 \in Q_p \iff p \equiv_{40} \pm 1$ or ± 9 or ± 3 or ± 13

$169 \in Q_p \iff p \neq 13$ ■

7.14

Solve $x^2 \equiv_{5^4} 6$

Proof. $6 \equiv_5 1^2$

So 1 is a square root of 6 mod (5)

Let s be a square root of 6 mod (5^2); that is, $s^2 \equiv_{5^2} 6$

Express s in the form of $m + 5k$ where $m < 5$

$$s^2 \equiv_{5^2} 6 \implies s^2 \equiv_5 6 \implies m^2 \equiv_5 6 \implies m = \pm 1$$

We deduce

$$6 \equiv_{5^2} s^2 \equiv_{5^2} (m+5k)^2 \equiv_{5^2} m^2 + 2(5mk) + 5^2k^2 \equiv_{5^2} m^2 + 2(5mk)$$

Then we can solve this congruence equation from $m = \pm 1$ and have solution $(m,k) = \pm(1,3)$; that is, $s = \pm 16$

So 16 is a square root of 6 mod (5^2)

Wash away the variable name we used.

Let s be a square root of 6 mod (5^3); that is, $s^2 \equiv_{5^3} 6$

Express s in the form of $m + 5^2k$ where $m < 5^2$

$$s^2 \equiv_{5^3} 6 \implies s^2 \equiv_{5^2} 6 \implies m^2 \equiv_{25} 6 \implies m = \pm 16$$

We deduce

$$6 \equiv_{5^3} s^2 \equiv_{5^3} (m+5^2k)^2 \equiv_{5^3} m^2 + 2(5^2mk) + 5^4k^2 \equiv_{5^3} m^2 + (2mk)5^2$$

Then we can solve the congruence equation from $m = \pm 15$ and have solution $(m,k) = \pm(16,0)$

So 16 is a square root of 6 mod (5^3)

Wash away the variable name we used.

Let s be a square root of 6 mod (5^4); that is, $s^2 \equiv_{5^4} 6$

Express s in the form of $m + 5^3k$ where $m < 5^3$

$$s^2 \equiv_{5^4} 6 \implies s^2 \equiv_{5^3} 6 \implies m^2 \equiv_{5^3} 6 \implies m = \pm 16$$

We deduce

$$6 \equiv_{5^4} s^2 \equiv_{5^4} (m+5^3k)^2 \equiv_{5^4} m^2 + (2mk)5^3 + 5^6k^2 \equiv_{5^4} m^2 + (2mk)5^3$$

Then we can solve the congruence equation from $m = \pm 15$ and have solution $(m,k) = \pm(16,39)$

$\blacksquare$

7.15

Solve $x^2 \equiv_{7^2} -3$ and $x^2 \equiv_{7^3} -3$

Proof. $-3 \equiv_7 2^2$

So 2 is a square root of -3 mod (7)

Let s be a square root of -3 mod (7^2)

Express s in the form of $s = m + 7k$ where $m < 7$

$$s^2 \equiv_{7^2} -3 \implies s^2 \equiv_7 -3 \implies m^2 \equiv_7 -3 \implies m = \pm 2$$

We deduce

$$-3 \equiv_{7^2} s^2 \equiv_{7^2} m^2 + (2mk)7 + 7^2k^2 \equiv_{7^2} m^2 + (2mk)7$$

From $m = \pm 2$, we can solve the congruence equation by solution $(m,k) = \pm(2,12)$

So we know 86 is a square root of -3 mod (7^2)

± 12 are also square roots of -3 mod (7^2)

Wash away the variable name we used.

Express s in the form of $s = m + 7^2k$ where $m < 7^2$

$$s^2 \equiv_{7^3} -3 \implies s^2 \equiv_{7^2} -3 \implies m^2 \equiv_{7^2} -3 \implies m = \pm 12$$

We deduce

$$-3 \equiv_{7^3} s^2 \equiv_{7^3} m^2 + (2mk)7^2 + 7^4k^2 \equiv_{7^3} m^2 + (2mk)7^2$$

From $m = \pm 12$, we can solve the congruence equation by solution $(m,k) = \pm(12, 300)$ ∎

7.16

Find the square root of 41 mod (2^6)

Proof. $\pm 19, \pm 51$ ∎

7.25

Is 43 a quadratic residue mod (923)

Proof. $923 = 13 * 71$

$$\left(\frac{43}{13}\right) = \left(\frac{4}{13}\right) = 1$$

So $43 \in Q_{13}$

$$\left(\frac{43}{71}\right) = \left(\frac{43}{71}\right) = -\left(\frac{71}{43}\right) = -\left(\frac{28}{71}\right) = -\left(\frac{7}{43}\right) = \left(\frac{43}{7}\right) = \left(\frac{1}{7}\right) = 1$$

So $43 \in Q_{71}$, then $43 \in Q_{923}$ ■

7.20

Let $r \geq 1$, show that there are infinitely many primes p such that $p \equiv_{2^r} 1$

Proof. Assume there are only finitely many primes $p_1, \ldots, p_k$ satisfy $p \equiv_{2^r} 1$

Let $a = 2p_1 \cdots p_k$

Prime factorize $a^{2^{(r-1)}} + 1$ and pick any appearing prime p_c so $p_c | a^{2^{(r-1)}} + 1$

Notice p_c can not be one of the $p_1, \ldots, p_k$

Observe

$$a^{2^{(r-1)}} \equiv_{p_c} -1$$

So we know a have order 2^r in U_{p_c} **(notice this is true because $2^{(r-1)}$ contain only prime 2)**

Then $2^r | p_c - 1$ by theorem of Lagrange, which make $p_c \equiv_{2^r} 1$ CaC

■

7.22

Let q and r be distinct primes, and suppose $q \equiv_4 r \equiv_4 1$. Show that $(x^2 - q)(x^2 - r)(x^2 - qr) \equiv_n 0$ have solution for all $n \in \mathbb{N}$

Proof. Prime factorize $n = 2^{c_0} p_1^{c_1} \cdots p_k^{c_k}$

$(x^2 - q)(x^2 - r)(x^2 - qr) \equiv_n 0 \iff (x^2 - q)(x^2 - r)(x^2 - qr) \equiv_{2^{c_0}} 0$ and $(x^2 - q)(x^2 - r)(x^2 - qr) \equiv_{p_i} 0, \forall p_i$

We show there are solution $x_0, \ldots, x_k$ respectively for the congruence equations $(x_0^2 - q)(x_0^2 - r)(x_0^2 - qr) \equiv_{2^{c_0}} 0$ and $(x_i^2 - q)(x_i^2 - r)(x_i^2 - qr) \equiv_{p_i} 0$

Notice If $x \equiv_{2^{c_0}} x_0$ then $(x^2 - q)(x^2 - r)(x^2 - qr) \equiv_{2^{c_0}} 0$ and, similarly, if $x \equiv_{p_i} x_i$ then $(x^2 - q)(x^2 - r)(x^2 - qr) \equiv_{p_i} 0$

After attaining solutions $x_0, \ldots, x_k$, we want to use Chinese Remainder Theroem to attain an x such that $x \equiv_{2^{c_0}} x_0$ and $x \equiv_{p_i} x_i, \forall p_i$. Notice that it is possible one can run into the problem where $yx_1 \cdots x_k \equiv_{2^{c_0}} x_0$ have no solution for y. To prevent this possibility, we only have to ensure that $x_1, \ldots, x_k$ are all odds, which is doable, since we can add p_i to even x_i if necessary.

Now we shows that the solutions $x_0, \ldots, x_k$ exists.

We first show solution x_0 exists.

Consider the case $c_0 = 1$ or 2. We see $q \equiv_4 1 \implies q \in Q_{2^{c_0}}$. Then we can find a square root of q mod 2^{c_0} to be our x_0.

Now consider the case $c_0 \geq 3$.

If $r \in Q_{2^{c_0}}$ or $q \in Q_{2^{c_0}}$, then we can easily find a square root of one of then to be our x_0. If $r \notin Q_{2^{c_0}}$ and $q \notin Q_{2^{c_0}}$, we see $r \not\equiv_8 1 \not\equiv_8 q$, by which we know $r \equiv_8 5 \equiv_8 q$, so $rq \equiv_8 1$, then we can find a square root of rq to be our x_0.

We now show the solution x_i exists for all p_i.

Notice

$$\left(\frac{r}{p_i}\right)\left(\frac{q}{p_i}\right) = \left(\frac{qr}{p_i}\right)$$

This tell us at least one of the $\left(\frac{r}{p_i}\right), \left(\frac{q}{p_i}\right), \left(\frac{qr}{p_i}\right)$ is 1. Then we can pick the square root of its counterpart r or q or rq to be to be our x_i

■

7.27

Show that $\sum_{a \in Q_p} a \equiv_p 0$

Proof. Let g be a primitive root mod p

Express Q_p in the form of $Q_p = \{g^{p-1} = g^0, g^2, g^4, \ldots, g^{p-3}\}$

$$\sum_{a \in Q_p} a \equiv_p g^{p-3} + \cdots + g^0 \equiv_p \frac{g^{p-1} - g^0}{g^2 - 1} \equiv_p \frac{0}{g^2 - 1} \equiv_p 0$$

■

7.26

Find the square roots of 7 mod (513)

Proof. $x^2 \equiv_{513} 7 \iff x^2 \equiv_{27} 7$ and $x^2 \equiv_{19} 7 \iff x \equiv_{27} \pm 13$ and $x \equiv_{19} \pm 11 \iff [x] \in \{[(\pm 5)19 + (\pm 1)27]\}$ **notice** $\pm$ **have no order relation** ■