Elementary Number Theory Course Notes

Isaac Holt

February 7, 2023

Contents

1 Quadratic Residues and Non-Residues

Consider the equation $x^2 \equiv a \pmod{p}$.

Definition 1.0.1. Let $a \in \mathbb{Z}$, p be an odd prime, $p \not| a$. $a \pmod{p}$ is a **quadratic residue (QR) mod** p if for some $x \in \mathbb{Z}$, $x^2 \equiv a \pmod{p}$.

If there doesn't exist such an x, $a \pmod{p}$ is a **quadratic non-residue (NQR)**.

Lemma 1.0.2. For p an odd prime, there are $\frac{p-1}{2}$ QRs and $\frac{p-1}{2}$ NQRs.

Proof. Define the map $f : \{1, \ldots, \frac{p-1}{2}\} \to Q$, $f(x) := x^2 \pmod{p}$, where $Q := \{x^2 \pmod{p}\}$ is the set of all QRs.

f is clearly surjective, since $\{x^2 \pmod{p} : 1 \leq x \leq p-1\} = \{x^2 \pmod{p} : 1 \leq x \leq \frac{p-1}{2}\}$, since if $\frac{p+1}{2} \leq x \leq p-1$, $-x \pmod{p} \in \{1, \ldots, \frac{p-1}{2}\}$ and $x^2 \equiv (-x)^2 \pmod{p}$.

Suppose that $f(a) = f(b)$, so $a^2 \equiv b^2 \pmod{p} \Rightarrow (a-b)(a+b) \equiv \pmod{p}$. $2 \leq a+b \leq p-1$ so $a+b \not\equiv 0 \pmod{p}$, hence $a \equiv b \pmod{p} \Rightarrow a = b$.

So f surjective and injective so is bijective, so $|Q| = \frac{p-1}{2}$. The remaining $\frac{p-1}{2}$ elements are the NQRs. $\square$

Lemma 1.0.3. Let $a \in \mathbb{Z}$, $a \in \mathbb{Z}$, p be an odd prime, $p \not| ab$. Let Q denote the QRs mod p and N denote the NQRs mod p.

1. If $a \in Q$ and $b \in Q$ then $ab \in Q$.
2. If $a \in Q$ and $b \in N$, then $ab \in N$.
3. If $a \in N$ and $b \in N$, then $ab \in Q$.

Proof.

1. If $a \in Q$ and $b \in Q$, for some $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, $x^2 \equiv a \pmod{p}$ and $y^2 \equiv b \pmod{p}$, so $ab \equiv x^2y^2 \pmod{p} \equiv (xy)^2 \pmod{p}$ so for some z, $z^2 \equiv ab \pmod{p}$ $(z = xy)$. So $ab \in Q$.
2. Suppose $ab \notin N$, for $a \in Q$, $\in N$. Since $ab \not\equiv 0 \pmod{p}$, $ab \in Q$. So for some $w \in \mathbb{Z}$, $ab \equiv w^2 \pmod{p}$. Since $a \in Q$, for some $t \in \mathbb{Z}$, $a \equiv t^2 \pmod{p}$ so $t^2 b \equiv w^2 \pmod{p}$. Cancelling t^2 on both sides, $b \equiv w^2\bar{t}^2 \pmod{p} \equiv (w\bar{t})^2 \pmod{p}$. But $b \in N$, so we have a contradiction.
3. We write $a^{-1} \cdot Q := \{1 \leq b \leq p-1 : a \cdot b \in Q\} = \{a^{-1}x : x \in Q$ (a^{-1} is such that $a^{-1}a \equiv 1 \pmod{p}$)).

   As $a \in N$, $a^{-1} \in N$ (if $a^{-1} \in Q$ then as $a \in N$, 2. implies that $a^{-1}a \equiv 1 \in N \pmod{p}$ which is not true since $1 \equiv 1^2 \pmod{p}$).

   Thus for every $x \in Q$, $a^{-1}x \in N \Rightarrow a^{-1}Q \subseteq N$.

   $a^{-1}x \equiv a^{-1}y \pmod{p} \Rightarrow x \equiv y \pmod{p}$. AS $1 \leq x, y \leq p-1$, $x = y$. Thus, the map $Q \to a^{-1}Q$ given by $x \to a^{-1}x$ is injective and bijective.

   Therefore $|a^{-1}Q| = |Q| = |N| \Rightarrow a^{-1}Q = N$ so if $b \in N$, $b \in a^{-1}Q$ so $ab \in Q$.

$\square$

Definition 1.0.4. Let p be an odd prime. The **Legendre symbol** written as $(\frac{a}{p})$ is defined for $a \in \mathbb{Z}$ as

$$(\frac{a}{p}) := \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } p \in Q \\ -1 & \text{if } p \in N \end{cases} \tag{1}$$

Properties of the Legendre symbol:

- (multiplicativity): if $a, b \in \mathbb{Z}$ then

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

- (periodicity mod p): if $a \equiv b \pmod{p}$ then

$$(\frac{a}{p}) = (\frac{b}{p})$$

Theorem 1.0.5. (Euler's criterion): if p is an odd prime and $a \in \mathbb{Z}$ with $p \not| a$ then

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

Proof. Let g be a primitive root mod p.

$\{g^r \pmod{p} : 1 \leq r \leq p-1\} = 1, \dots, p-1 \Rightarrow \{g^{2r} : 1 \leq r \leq \frac{p-1}{2}\}$ gives the QRs uniquely. There are the following cases:

1. a is a QR. Then for some $1 \leq r \leq \frac{p-1}{2}$, $g^{2r} \equiv a \pmod{p}$. Then

$$a^{\frac{p-1}{2}} \equiv (g^{2r})^{\frac{p-1}{2}} \equiv (g^r)^{p-1} \equiv (g^{p-1})^r \equiv 1^r \equiv 1 \equiv (\frac{a}{p}) \pmod{p}$$

2. a is not a QR. Then for some $1 \leq r \leq \frac{p-1}{2}$, $a \equiv g^{2r-1} \pmod{p}$. So $a^{\frac{p-1}{2}} \equiv (g^{2r})^{\frac{p-1}{2}} g^{\frac{p-1}{2}}$.

   But $x = g^{-\frac{p-1}{2}} \equiv -1 \pmod{p}$, since $x^2 \equiv 1 \pmod{p} \Rightarrow x \equiv \pm 1 \pmod{p}$ and since g is primitive, $x \not\equiv 1 \pmod{p}$.

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

□

Remark. Euler's crtierion is hard to use if p is large.

Corollary 1.0.6. -1 is a QR mod p iff $p \equiv 1 \pmod{4}$.

Proof. $(-1)^{\frac{p-1}{2}} \equiv (\frac{-1}{p}) \pmod{p}$ by Euler's criterion. The power $\frac{p-1}{2}$ is even iff $p \equiv 1 \pmod{4} \Rightarrow (-1)^{\frac{p-1}{2}} = 1$ iff $p \equiv 1 \pmod{4}$. □

Theorem 1.0.7. (Law of quadratic reciprocity - QRL): Let p, q be distinct odd primes. Then

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

Proof. TODO □

Corollary 1.0.8.

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

1.1 Algorithm for computing $(\frac{a}{p})$

p is an odd prime, $a \in \mathbb{Z}$. TODO: make this clearer.

1. Use the division algorithm to divide $a = kp + r$, $0 \leq r \leq p-1$, hence $(\frac{a}{p}) = (\frac{r}{p})$.
2. If $r = 0$ or $r = 1$, $(\frac{0}{p}) = 0$, $(\frac{1}{p}) = 1$ so we are done.
3. If $r \neq 0$ and $r \neq 1$, factor $r = {p_1}^{a_1} \dots {p_k}^{a_k}$, then $(\frac{r}{p}) = (\frac{p_1}{p})^{a_1} \dots (\frac{p_k}{p})^{a_k}$
4. If $2|a_i$, then $(\frac{p_i}{p})^{a_i} = 1$.
5. If $2 \not| a_i$, $(\frac{p_i}{p})^{a_i} = (\frac{p_i}{p})$
6. If $p_i = 2$, use the above corollary: $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.
7. If $p_i \neq 2$, use QRL to write $(\frac{p_i}{p}) = (\frac{p}{p_i})(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ and go to step 1 to calculate $(\frac{p}{p_i})$

1.2 Application of Legendre Symbols

Theorem 1.2.1. There are infinitely many primes of the form $4n + 1$.

Proof. Assume the contrary, so let $p_1 < \dots < p_k$ be a finite list of primes, with $p_i \equiv 1 \pmod 4$ for every i.

Let $N = (2p_1 \dots p_k)^2 + 1$. Since $N > 1$, for some prime p, $p|N$. $p \neq p_i$ for every i. $N \equiv 0 \pmod p$, hence $(2p_1 \dots p_k)^2 \equiv -1 \pmod p$. Thus -1 is a QR mod p.

By Euler's criterion, $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$, so $p \equiv 1 \pmod 4$.

But $p \notin \{p_1, \dots, p_k\}$ and $p \equiv 1 \pmod 4$ so we have a contradiction. $\square$

2 Sums of two squares

2.1 Sums of two squares

Given $n \in \mathbb{N}_0$, can we represent n as a sum of two squares, i.e. do there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = n$.

Equivalently, find solutions $x, y \in \mathbb{Z}$ to the equation

$$x^2 + y^2 = n$$

Lemma 2.1.1. If n, m are both sums of two squares, so is $n \cdot m$.

Proof. Let $n = a^2 + b^2$, $m = c^2 + d^2$, $a, b, c, d \in \mathbb{Z}$. Then $nm = (a^2 + b^2)(c^2 + d^2) = (a^2c^2 + b^2d^2) + (b^2c^2 + a^2d^2) = (ac+bd)^2 - b^2c^2 + a^2d^2 - 2acbd = (ac+bd)^2 - (ad-bc)^2$ $\square$

Corollary 2.1.2. If $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ and all the powers ${p_i}^{e_i}$ are sums of two squares then n is also.

We focus on prime powers: $n = p^a$.
If $a = 2b$, $b \in \mathbb{N}$, then $n = p^{2b} = (p^b)^2 = (p^b)^2 + 0^2$ so n is a sum of two squares.
If $a = 2b + 1$, $n = (p^b)^2 \cdot p$.
If $n = p$ is a prime, is n a sum of two squares.

Theorem 2.1.3. A prime p is a sum of two squares iff either $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. ($\Rightarrow$): For every n, $n^2 \equiv 0$ or $1 \pmod 4$

Therefore if $p = x^2 + y^2$, $p = x^2 + y^2 \bmod 4 \in \{0, 1, 2\}$. The only p equivalent to 0 or $2 \pmod 4$ is $p = 2$, otherwise, $p \equiv 1 \pmod 4$.

($\Leftarrow$): Suppose $p = 2$ or $p \equiv 1 \pmod 4$. If $p = 2$, $p = 1^2 + 1^2$. If $p \equiv 1 \pmod 4$, $\left(\frac{-1}{p}\right) = 1$, so we can solve $u^2 + 1 \equiv 0 \pmod 4$, $1 \leq u \leq \frac{p-1}{2}$. We will find small $A, B \in \mathbb{N}_0$ suvh that $A^2 + B^2 \equiv 0 \pmod p$ using u. If $0 < A^2 + B^2 < 2p$, $A^2 + B^2 = p$.

Let $k = \text{floor}(\sqrt{p})$, so $k \in \mathbb{N}$ and $k < \sqrt{p} < k + 1$. Consider the set $\{a + b \cdot u \pmod p : 0 \leq a, b \leq k\}$. There are $(k + 1)^2$ pairs (a, b). Since $(k + 1)^2 > (\sqrt{p})^2 = p$. By the pigeon-hole principle, we can find two pairs $(a_1, b_1) \neq (a_2, b_2)$ such that $a_1 + b_1u \equiv a_2 + b_2u \pmod p$.

So $(b_2 - b_1)u \equiv a_1 - a_2 \pmod p \Rightarrow Bu \equiv \pm A \pmod p$ where $B = |b_2 - b_1| \leq k < \sqrt{p}$, $A = |a_1 - a_2| \leq k < \sqrt{p}$ and at least one of A and B is > 0.

So $A^2 + B^2 \equiv (Bu)^2 + B^2 \equiv B^2(u^2 + 1) \equiv 0 \pmod p$

Since at least one of A and B is > 0, $A^2 + B^2 > 0$. Since $A, B < \sqrt{p}$, $A^2 + B^2 < 2p$. Also, $p | (A^2 + B^2)$, hence $A^2 + B^2 = p$. $\square$

Corollary 2.1.4. A positive integer $n > 1$ written as $n = m^2 p_1 \cdots p_k$, with $p_1, \cdots p_k$ distinct primes (n can always be written in this way) is a sum of two squares iff for every p_i either $p_i = 2$ or $p_i \equiv 1 \pmod 4$.

Remark. There is a theorem due to Lagrange that says that every $n \in \mathbb{N}_0$ can be represented as the sum of four squares.

3 Continued Fractions

3.1 Pell equations

Definition 3.1.1. A **Pell equation** is an equation of the form $x^2 - dy^2 = \pm 1$, where $d \geq 1$ is not a square.

Remark. If $x, y \neq 0$ and both are large, then as $(x - \sqrt{d}y)(x + \sqrt{d}y) = x^2 - dy^2 = \pm 1$,

$$\left|\frac{x}{y} - \sqrt{d}\right| \left|\frac{x}{y} + \sqrt{d}\right| = \left|\left(\frac{x}{y}\right)^2 - d\right| = \frac{1}{y^2}$$

So if $x^2 - dy^2 = \pm 1$ has a solution $(x, y) \in \mathbb{N}_0^2$, then $\frac{x}{y}$ approximates $\pm\sqrt{d}$.

3.2 Continued fractions

Definition 3.2.1. A **finite continued fraction (finite CF)** is an expression of the form

$$[a_0; a_1, \ldots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_n}}$$

where $a_j \in \mathbb{R}$, $n \geq 0$.

Mostly, $a_0 \in \mathbb{Z}$ and $a_1, \ldots, a_n \in \mathbb{N}$. In this case, $[a_0, \ldots, a_n]$ is called an **ellipse**.

Proposition 3.2.2. Any $\frac{a}{b} \in \mathbb{Q}$ can be expressed as a finite CF.

Proof. (Not a full proof). Suppose for simplicity that $a \geq b$ (if not, take $a_0 = 0$). By the division algorithm, $a = a_0 b + r_1$, $0 \leq r_1 < b$ hence $\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{b/r_1}$.

Now divide b by r_1: $b = a_1 r_1 + r_2$, $0 \leq r_2 < r_1$, so $\frac{b}{r_1} = a_1 + \frac{r_2}{r_1}$ so

$$\frac{a}{b} = a_0 + \frac{1}{a_1 + \frac{1}{r_1/r_2}}$$

We continue with this: $r_i = a_{i+1} r_{i+1} + r_{i+2}$ until r_{i+1} divides r_1 (i.e. $r_{i+2} = 0$). This must occur as $0 \leq r_{i+1} < r_i$.

The continued fraction is $[a_0; a_1, \ldots, a_n]$ where $r_{n+1} = 0$. $\square$

Definition 3.2.3. Given a finite CF $\alpha = [a_0; a_1, \ldots, a_n]$, the a_i are called **partial quotients** of α.

The truncated CF's $[a_0; a_1, \ldots a_j] = \frac{p_j}{q_j}$, with $0 \leq j \leq n$, $p_j \in \mathbb{Z}$, $q_j \in \mathbb{N}$, are called the **convergents** of α.

For $j = 0, j = 1$ we have $\frac{p_0}{q_0} = [a_0] = a_0 \Rightarrow p_0 = a_0, q_0 = 1$.

$\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1} \Rightarrow p_1 = q_1 a_0 + 1, q_1 = a_1$.

Proposition 3.2.4. Given a finite CF, $[a_0; a_1, \ldots, a_n]$, $n \geq 1$, $[[p_k, p_{k-1}], [q_k, q_{k-1}]] = [[a_1, 1], [1, 0]] \cdots [[a_k, 1], [1, 0]]$ TODO: make these matrices.

Hence $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$, $q_1 = a_1$, $p_k = a_k p_{k-1} + p_{k-2}$, $q_k = a_k q_{k-1} + q_{k-2}$.

Lemma 3.2.5. Let $\alpha = [a_0; a_1, \ldots, a_n]$ be a finite CF with convergents $\frac{p_k}{q_k}$, $0 \leq k \leq n$.

For every $k \geq 0$, $q_{k+1} \geq q_k$ and if $k \geq 1$ then $q_{k+1} > q_k$.

Proof. If $k = 0$, $q_1 = a_1 \geq 1 = q_0$. Inductively, if $q_{k-1} > 0$ for $k \geq 1$ then $q_{k+1} = a_{k+1} q_k + q_{k-1} \geq a_{k+1} q_k \geq q_k$ since $a_{k+1} \geq 1$. $\square$

Lemma 3.2.6. For every $k \geq 1$, $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}$.

Proof. By the previous proposition,

$$[[p_k, p_{k-1}], [q_k, q_{k-1}]] = [[a_1, 1], [1, 0]] \cdots [[a_k, 1], [1, 0]]$$

$p_k q_{k-1} - q_k p_{k-1} = \det[[p_k, p_{k-1}], [q_k, q_{k-1}]] = \det[[a_1, 1], [1, 0]] \cdots \det[[a_k, 1], [1, 0]] = (-1)^{k+1}$. □

Corollary 3.2.7. $\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{p_k q_{k-1} - p_{k-1} q_k}{q_k q_{k-1}} = \frac{(-1)^{k+1}}{q_k q_{k-1}}$

So the convergents get closer as k increases.

Proposition 3.2.8. The even-numbered convergents are growing: $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots$ and the odd-numbered convergents are decreasing: $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \cdots$.

Moreover, for every $k \geq 1$ such that $2k + 1 \leq n$,

$$\frac{p_{2k}}{q_{2k}} \leq \alpha \leq \frac{p_{2k+1}}{q_{2k+1}}$$

and

$$\left| \alpha - \frac{p_m}{q_m} \right| \leq \frac{1}{q_m q_{m-1}}$$

for every $m \leq n - 1$.

Proof. TODO □

Definition 3.2.9. In general, if $\alpha \in \mathbb{R}$ (not necessarily rational), for $j > 0$:

1. $a_j := \text{floor}(\alpha_j)$ where $\{a_j\} := \alpha_j - a_j$
2. Define $\alpha_{j+1} := \frac{1}{\{\alpha_j\}}$. $(\alpha_0 = \alpha)$

The continued fraction for α is $[a_0; a_1, a_2, \ldots]$.

This could continue indefinitely if $a \notin \mathbb{Q}$.

Definition 3.2.10. An **infinite CF** is the limit, if it exists, of a sequence of finite CF's: $\{[a_0; a_1, \ldots, a_n]\}_{n \geq 0}$ given a $\{a_i\}_{i \geq 0}$ with $\forall i, a_i \geq 1$.

Proposition 3.2.11. If $a_0 \in \mathbb{Z}$ and $\forall ige1, a_i \in \mathbb{N}$, then $\{[a_0; a_1, \ldots, a_n]\}_{n \geq 0} \subset \mathbb{Q}$ converges.

Proof. Use the Cauchy criterion: $[a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}$ are the convergents. $\forall m \geq 1, q_{m+1} > q_m$, $q_m \in \mathbb{N}$. Let $\alpha_n = \frac{p_n}{q_n}$. If $m \leq n$,

$$\left| \alpha_n - \frac{p_m}{q_m} \right| \leq \frac{1}{q_m q_{m+1}}$$

Let $\epsilon > 0$. Then for some N, if $m \geq N$, $q_{m+1} > q_m > \frac{1}{\sqrt{2}}$. Then with $n \geq m \geq N$,

$$\left| \frac{p_n}{q_n} - \frac{p_m}{q_m} \right| \leq \frac{1}{q_m q_{m+1}} < \sqrt{\epsilon}\sqrt{\epsilon} = \epsilon$$

Thus $\{\frac{p_k}{q_k}\}_k$ is a Cauchy sequence. □

Definition 3.2.12. An infinite CF $\alpha = [a_0; a_1, a_2, \ldots]$ is (eventually) periodic if for some $m \in \mathbb{N}_0$ and $k \geq 1$, if $n > m$, $\forall j \in \mathbb{N}_0$, $a_{n+jk} = a_n$. That is,

$$\alpha = [a_0; a_1, \ldots, a_m, a_{m+1}, \ldots, a_{m+k}, \ldots] = [a_0; \ldots, a_m, \overline{a_{m+1}, \ldots, a_{m+k}}]$$

k is the **period** of the CF of α.

Lemma 3.2.13. If $d \in \mathbb{N}$, d is not a square, the CF of $\sqrt{d}$ is eventually periodic with initial part of length 1.

Theorem 3.2.14. The eventually periodic $\alpha \notin \mathbb{Q}$ are preicsely of the form $a + b\sqrt{d}$, $a, b \in \mathbb{Q}$, $d \in \mathbb{N}$, d is not a square.

Example 3.2.15. Find simplified expression for $\alpha = [1; 3, \overline{4, 2}] = [1; 3, \beta]$.

$\beta = [4; 2, \beta]$ so

$$\beta = 4 + \frac{1}{2 + \frac{1}{\beta}} = 4 + \frac{\beta}{2\beta + 1}$$

so simplifying, we get $2\beta^2 - 8\beta - 4 = 0 \Leftrightarrow \beta^2 - 4\beta - 2 = 0$, which has a positive root $2 + \sqrt{6}$ (β must be positive).

This can be used to simplify the expression for α.

3.3 Application to Pell Equations

Theorem 3.3.1. Let $x^2 - dy^2 = \pm 1$, $d \in \mathbb{N}$, d is not a square. Suppose the CF of $\sqrt{d}$ has period k.

If $\{\frac{p_m}{q_m}\}_{m \geq 0}$ are the convergents of $\sqrt{d}$. Then for every $n \in \mathbb{N}$,

$$p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn}$$

In particular, if k is even then $x^2 - dy^2 = 1$ has an infinite collection of solutions

$$(x, y) = (p_{kn-1}, q_{kn-1}), n \in \mathbb{N}_0$$

If k is odd then $x^2 - dy^2 = -1$ has soltuions

$$(x, y) = (p_{(2n-1)k-1}, q_{(2n-1)k-1})$$

and $x^2 - dy^2 = 1$ has soltuions

$$(x, y) = (p_{2kn-1}, q_{2kn-1})$$