

Year 3 — Number Theory

Based on lectures by Professor Henri Johnston

Notes taken by James Arthur

Autumn Term 2021

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine (especially the typos!).

Contents

1	Divisibility	2
1.1	Division Algorithm	2
1.2	Greatest Common Divisor	2
1.3	Euclids Algorithm	4
1.4	Extended Euclidean Algorithm	5
2	Primes and Congruences	6
2.1	Fundamental Theorem of Arithmetic	6
2.2	Congruences	8
3	Residue Classes	11
3.1	Complete Residue Systems	11
3.2	Linear Congruences	12
4	$\mathbb{Z}/n\mathbb{Z}$, Chinese Remainder Theorem and $\varphi(n)$	14
4.1	$\mathbb{Z}/n\mathbb{Z}$ and it's units	14
4.2	Chinese Remainder Theorem	14
4.3	Euler φ function	15
5	Modular Exponentiation	17
5.1	Reduced Residue Systems	17
5.2	Euler- Fermat Theorem	18
5.3	Modular Exponentiation	18
5.4	Polynomial Congruence	19
6	Hensel Lifting, Primitive Roots and Wilson's Theorem	21
6.1	Hensel Lifting	21
6.2	Primitive Roots	22
6.3	Wilson's Theorem	24
7	Quadratic Residues, Legendre Symbols, Euler Criterion and Gauss' Lemma	25
7.1	Legendre Symbol	25
7.2	Eulers Criterion	26
7.3	Gauss' Lemma	27
8	Law of Quadratic Reciprocity	31
9	Jacobi Symbol	34
10	Sums of squares	37
10.1	Pythagorean Triples	37
10.2	Sums of Squares	39
10.3	Sums of two squares	40
10.4	Sums of Four Squares	42

1 Divisibility

1.1 Division Algorithm

Definition 1.1 (Well Ordering Principle). Every non-empty subset of \mathbb{N}_0 contains a least element

Theorem 1.2 (Division Algorithm). Given a $a \in \mathbb{Z}$ and a $b \in \mathbb{N}_1$ there exists unique integers q and r satisfying $a = bq + r$ and $0 \leq r < b$.

The proof splits into uniqueness and existence.

Proof. We shall first prove existence, define $S := \{a - xb : x \in \mathbb{Z} \text{ and } a - xb \geq 0\}$. We know $S \neq \emptyset$ since,

- if $a \geq 0$, then choose $m = 0$, then $a - mb = a \geq 0$
- if $a < 0$, then let $a = m$, so $a - mb = a - ab = (-a)(b - 1) \geq 0$ since $-a > 0$ and $b > 0$ ¹

Hence S is non-empty subset of \mathbb{N}_0 and so by the well ordering principle S must contain a least element $r \geq 0$. Since $r \in S$, then we have there exists a $q \in \mathbb{Z}$ such that $a - qb = r$ and so $a = qb + r$. Now it remains to check that $r < b$, so assume for a contradiction that $r \geq b$, then let there be a $r_1 = r - b \geq 0$. Then,

$$a = qb + r = qb + (r_1 + b) = (q + 1)b + r_1$$

and so $a - (q + 1)b = r_1 \in S$ and is smaller than r , a contradiction.

Now let us show uniqueness, assume that there exist another pair q', r' such that $a = q'b + r'$ where $0 \leq r' < b$. Then from $a = a + qb + r = q'b + r'$ we have that, $(q - q')b = r' - r$. If $q = q'$, then we must have $r = r'$, suppose for a contradiction that this isn't true, then,

$$b \leq |q - q'|b = |r - r'|$$

However, since $0 \leq r, r' < b$ and so $|r - r'| < b$ which gives a contradiction. □

Here's a definition that I feel is useful that wasn't covered in the lectures,

Definition 1.3 (Divisible). We say that some $a \in \mathbb{Z}$ is divisible by some $b \in \mathbb{Z}$ if and only is,

$$\exists n \in \mathbb{Z}, \text{ such that } b = na$$

and denote it, $a \mid b$

1.2 Greatest Common Divisor

Let us start with a theorem.

Theorem 1.4. Let $a, b \in \mathbb{Z}$, $\exists d \in \mathbb{N}_0$ and non-unique $x, y \in \mathbb{Z}$ such that,

1. $d \mid a$ and $d \mid b$
2. and if $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$, then $e \mid d$
3. $d = ax + by$

¹You absolute plank, there doesn't exist any numbers between 0 and 1 in \mathbb{Z} , so $b > 0$ is the same as $b \geq 1$

Proof. If $a = b = 0$, then $d = 0$
 Suppose that $a \neq b \neq 0$, then let

$$S := \{am + bn : m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$$

Now $a^2 + b^2 > 0$ so S is non-empty and a subset of \mathbb{N}_1 . Hence, by the Well ordering principle then there must be some minimum element d . Then we can write $d = ax + by$ by definition of S .

By the division Algorithm, $a = qs + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Suppose for a contradiction that $r \neq 0$. Then,

$$0 < r = a - qd = a - q(ax + by) = (1 - qx)a - qby$$

Hence, $r \in S$. But $r < d$, contradicting the minimality of d in S . So we must have $r = 0$, i.e. $d \mid a$. The same works for $d \mid b$.

Suppose that $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$. Then e divides any linear combination of a and b , so $e \mid d$. Suppose that $e \in \mathbb{N}_1$ also satisfies (i) and (ii). Then, $e \mid d$ and $d \mid e$ and so $d = \pm e$, but $d, e \geq 0$ and so $d = e$. Thus d is unique. \square

Note that this is a standard trick to prove that integers divide, by just proving that $r = 0$ by contradiction.

Corollary 1.5. If $a, b \in \mathbb{Z}$ then there exists a unique $d \in \mathbb{N}_1$ such that.

1. $d \mid a$ and $d \mid b$
2. if $e \in \mathbb{Z}$, then $e \mid a$ and $e \mid b$ then $e \mid d$

Proof. The existence of a d is given by the theorem. In the proof of uniqueness we only use (i) and (ii). \square

Definition 1.6 (Greatest Common Divisor). Let $a, b \in \mathbb{Z}$. Then d of the previous corollary is just the greatest common divisor of a and b , written $\gcd(a, b)$. Also sometimes seen as $\text{hcf}(a, b)$.

If $\gcd(a, b) = 1$, then a and b are coprime.

Identity (Bezouts Identity). Given $a, b \in \mathbb{Z}$ there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

Proposition 1.7. Let $a, b, c \in \mathbb{Z}$, then,

1. $\gcd(a, b) = \gcd(b, a)$
2. $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$
3. $\gcd(ac, bc) = |c| \gcd(a, b)$
4. $\gcd(1, a) = \gcd(a, 1) = 1$
5. $\gcd(0, a) = \gcd(a, 0) = |a|$
6. $c \mid \gcd(a, b)$ if and only if $c \mid a$ and $c \mid b$
7. $\gcd(a + cb, b) = \gcd(a, b)$

Then we can consider the following remark,

Remark. Note that $\gcd(a, b) = 0$ if and only if, $a = b = 0$. Otherwise, $\gcd(a, b) \geq 1$.

Proof. Checking these properties are pretty simple, for (vi) just use Bezouts.

We shall prove (iii), so let $d = \gcd(a, b)$ and $e = \gcd(ac, bc)$. By (vi), $cd \mid e = \gcd(ac, bc)$ since $cd \mid ac$ and $cd \mid bc$. Then by Bezouts, there exists $x, y \in \mathbb{Z}$ such that $d = ax + by$. Then,

$$cd = acx + bcy$$

and as $e \mid ac$ and $e \mid bc$ and so by linearity we have $e \mid cd$. Therefore, $|e| = |cd|$ and so, $e = |c|d$.

Now, let's prove (vii), let $e = \gcd(a + bc, b)$ and $f = \gcd(a, b)$. Then $e \mid (a + bc)$ and $e \mid b$. Thus by linearity, we have $e \mid a$. Hence, $e \mid a$ and $e \mid b$ so by property (vi), we have $e \mid f$. Similarly we can get that $f \mid a + bc$ and $f \mid b$ and so again by (vi) we have $e = f$ as $f, e \geq 0$. \square

Lemma 1.8 (Euclids Lemma). Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Proof. Suppose that $a \mid bc$ and $\gcd(a, b) = 1$. By Bezouts, we get that for some $x, y \in \mathbb{Z}$ we get $1 = ax + by$. Hence, $c = acx + bcy$, but $a \mid acx$ and $a \mid bcy$, so $a \mid c$ by linearity. \square

Theorem 1.9 (Solubility of linear equations in \mathbb{Z}). Let $a, b, c \in \mathbb{Z}$. The equation,

$$ax + by = c$$

is soluble with $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b) \mid c$

Proof. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$ so if there exists $x, y \in \mathbb{Z}$ such that $c = ax + by$ then $d \mid c$ by linearity of divisibility. Now, suppose that $d \mid c$. Then we can write $c = qd$ for some $q \in \mathbb{Z}$. By Bezouts, there exists some $x', y' \in \mathbb{Z}$ such that $d = ax' + by'$. Hence, $c = qd = aqx' + byq'$ and so $x = qx'$ and $y = qy'$ gives a suitable solution. \square

1.3 Euclids Algorithm

Theorem 1.10 (Euclids Algorithm). Let $a, b \in \mathbb{N}_1$ with $a > b > 0$ and $b \nmid a$. Let $r_0 = a$, $r_1 = b$ and apply the division Algorithm repeatedly to obtain a sequence of remainders defined sucessively,

$$\begin{array}{ll} r_0 = r_1 q_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2 q_2 + r_3 & 0 < r_3 < r_2 \\ \vdots & \\ r_{n-2} = r_{n-1} q_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_n + r_{n+1} & r_{n+1} = 0 \end{array}$$

Then the last non-zero remainder, r_n is the $\gcd(a, b)$.

Proof. There is a stage at which $r_{n+1} = 0$ because the r_i are strictly decreasing non-negative integers. We have,

$$\begin{aligned} \gcd(r_i, r_{i+1}) &= \gcd(r_{i+1} q_{i+1} + r_{i+2} r_{i+1}) \\ &= \gcd(r_{i+2} r_{i+1}) \\ &= \gcd(r_{i+1}, r_{i+2}) \end{aligned}$$

Applying this result repeatedly,

$$\begin{aligned} \gcd(a, b) &= \gcd(r_0, r_1) \\ &= \gcd(r_2, r_3) \\ &= \dots \\ &= \gcd(r_{n-1}, r_n) \\ &= r_n \end{aligned}$$

Where the last equality is because $r_n \mid r_{n-1}$ □

Remark. One can also use Euclids Algorithm to find the $x, y \in \mathbb{Z}$ Bezouts Identity state to exist by working backwards. These aren't unique.

1.4 Extended Euclidean Algorithm

Instead of doing Euclids, and working backwards we can compute our bezouts x, y during euclids. This is the extended Euclids Algorithm. This time we are going to define sequences of integers x_i and y_i , such that $r_i = ax_i + by_i$. Recall that r_n is the last non-zero remainder and that $r_n = \gcd(a, b)$. Therefore $\gcd(a, b) = r_n = ax_n + by_n$ and so $(x, y) := (x_n, y_n)$.

We have that $r_0 = a$ and $r_1 = b$. Hence, we see $r_0 = 1 \times a + 0 \times b$ and $r_1 = 0 \times a + 1 \times b$, and so we set $(x_0, y_0) := (1, 0)$ and $(x_1, y_1) := (0, 1)$. So, now we consider for $i \geq 2$ we have a pair (x_j, y_j) for $j < i$. Then $r_{i-2} = r_{i-1}q_{i-1} + r_i$ and so,

$$\begin{aligned} r_i &= r_{i-2} - r_{i-1}q_{i-1} \\ &= (ax_{i-2} + by_{i-2}) - (ax_{i-1} + by_{i-1})q_{i-1} \\ &= a(x_{i-2} - x_{i-1}q_{i-1}) + b(y_{i-2} - y_{i-1}q_{i-1}) \end{aligned}$$

Thus we set $x_i := x_{i-2} - x_{i-1}q_{i-1}$ and $y_i := y_{i-2} - y_{i-1}q_{i-1}$. These can be defined recursively this way.

$$(x_i, y_i) := (x_{i-2}, y_{i-2}) - q_{i-1}(x_{i-1}, y_{i-1})$$

Example. We compute $\gcd(841, 160)$ use Extended Euclidean Algorithm.

i	r_{i-2}	r_{i-1}	q_{i-1}	r_i	x_i	y_i
0				841	1	0
1				160	0	1
2	841	= 160	× 5	+ 41	1	-5
3	160	= 41	× 3	+ 37	-3	16
4	41	= 37	× 1	+ 4	4	-21
5	37	= 4	× 9	+ 1	-39	205
6	4	= 1	× 4	+ 0		

Therefore, $\gcd(841, 160) = 1 = 841 \times (-39) + 160 \times 205$.

2 Primes and Congruences

We start by defining primes and composite numbers,

Definition 2.1 (Prime). A number $p \in \mathbb{N}_1$ with $p > 1$ is prime if and only if its only divisors are 1 and p , i.e.

$$n \mid p \implies n = 1 \text{ or } n = p$$

Definition 2.2 (Composite Numbers). A number $n \in \mathbb{N}_1$ with $n > 1$ is composite if and only if it is not prime, i.e.

$$n = ab \quad 1 < a, b \in \mathbb{N}$$

One is neither composite nor prime.

Proposition 2.3. If $n \in \mathbb{N}_1$ with $n > 1$, then n has a prime factor.

Proof. Use strong induction, so assume for $1 < m < n$ where $m \in \mathbb{N}_1$ that m has a prime factor.

Case (i): If n is prime, then n is a prime factor of n .

Case (ii): If n is composite, then $n = ab$ where $a, b > 1$ and so, $1 < a < n$. By the induction hypothesis, there is a prime p such that $p \mid a$. Hence, $p \mid a$ and $a \mid n$ so, by transitivity $p \mid n$. \square

Proposition 2.4. If $1 < n \in \mathbb{N}_1$, then we can write $n = p_1 p_2 \dots p_k$ where $k \in \mathbb{N}_1$ and p_i are primes.

Proof. If n is prime, then the result is clear. So suppose that n is composite. Then n must have a prime factor, so $n = p_1 n_1$ where $1 < n_1 \in \mathbb{N}_1$. If n_1 is prime, we are done. If n_1 is composite, then we can write $n_1 = p_2 n_2$ and so on... This process terminates as $n > n_1 > n_2 > \dots > 1$. Hence after at least n steps we obtain a prime factorisation of n . \square

Example.

$$666 = 3 \times 222 = 3 \times 2 \times 111 = 3 \times 2 \times 3 \times 37$$

Theorem 2.5. There are infinitely many primes

Euclid's Proof. For a contradiction, assume there are finitely many primes, $\{p_1, p_2, p_3, \dots, p_n\}$ and that is a complete list. Consider $N := p_1 p_2 \dots p_n + 1 \in \mathbb{N}$. Then $N > 1$ so by the first proposition, N has a prime factor p . However, every prime is one of the elements of the list, so $p = p_i$. Hence, $p_i \mid (p_1 p_2 \dots p_n)$ so $p \mid (N - 1)$. However, $p \mid N$ and we can write $1 = N - (N - 1)$, so $p \mid 1$, which is a contradiction. \square

2.1 Fundamental Theorem of Arithmetic

Lemma 2.6. Let $n \in \mathbb{Z}$, then if $p \nmid n$ then $\gcd(p, n) = 1$

Proof. Let $d = \gcd(p, n)$. Then $d \mid p$ so by definition of prime either $d = 1$ or $d = p$. But $d \mid n$ so $d \neq p$ because $p \nmid n$. Hence, $d = 1$. \square

Theorem 2.7 (Euclid's Lemma for Primes). Let $a, b \in \mathbb{Z}$ and p be a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Assume $p \mid ab$ and that $p \nmid a$. We shall prove $p \mid b$. By Lemma, $\gcd(p, a) = 1$, so by Euclid's lemma, $p \mid b$. \square

Remark. Euclid's Lemma for primes immediately generalises to several factors.

Definition 2.8. Let $n \in \mathbb{N}_1$ and p be a prime. Then,

$$v_p(n) := \max\{k \in \mathbb{N} \cup \{0\} : p^k \mid n\}$$

In other words, k is the unique non-negative integer such that $p^k \mid n$ but $p^{k+1} \nmid n$. Equivalently, $v_p(n) = k$ if and only if $n = p^k n'$ where $n' \in \mathbb{N}$ and $p \nmid n'$.

Example. We can see that,

- $v_2(720) = 4$ as $2^4 \mid 720$ but $2^5 \nmid 720$
- $v_3(720) = 2$ as $3^2 \mid 720$ but $3^3 \nmid 720$
- $v_5(720) = 1$ as $5^1 \mid 720$ but $5^2 \nmid 720$
- if $p \geq 7$, then $v_p(720) = 0$ as $p \nmid 720$.

Lemma 2.9. Let $n, m \in \mathbb{N}_1$ and p be a prime. Then $v_p(mn) = v_p(m) + v_p(n)$

Proof. Let $k = v_p(m)$ and $\ell = v_p(n)$. Then we write $m = p^k m'$ where $p \nmid m'$ and $n = p^\ell n'$ where $p \nmid n'$. Then $nm = p^{k+\ell} m'n'$ and so by Euclid's lemma $p \nmid m'n'$ as if it did then $p \mid n'$ or $p \mid m'$ but it doesn't. So $v_p(mn) = v_p(m) + v_p(n)$. \square

Theorem 2.10 (Fundamental Theorem of Arithmetic). Let $1 < n \in \mathbb{N}_1$. Then,

1. (Existence) The number n can be written as a product of primes.
2. (Uniqueness) Suppose that,

$$n = p_1 \dots p_r = q_1 \dots q_s$$

where each p_i and q_j are prime. Assume further that,

$$p_1 \leq p_2 \leq \dots \leq p_r \quad \text{and} \quad q_1 \leq q_2 \leq \dots \leq q_s$$

Then $r = s$ and $p_i = q_i$ for all i

Remark. If 1 is a prime, then the Uniqueness here is broken, as,

$$6 = 3 \times 2 = 3 \times 2 \times 1 = \dots$$

Remark. A consequence of the FTA is that the integral domain \mathbb{Z} is in fact a UFD.

Proof. The existence is something we have done before. The harder part is uniqueness. Let ℓ be any prime. Then we have,

$$\begin{aligned} v_\ell(n) &= v_\ell(p_1 \dots p_r) \\ &= v_\ell(p_1) + \dots + v_\ell(p_r) \end{aligned}$$

However,

$$v_\ell(p_i) = \begin{cases} 1 & \text{if } \ell = p_i \\ 0 & \text{if } \ell \neq p_i \end{cases}$$

Therefore,

$$\begin{aligned} v_\ell(n) &= \# \text{ of } i \text{ for which } \ell = p_i \\ &= \# \text{ of times } \ell \text{ appears in the factorisation } n = p_1 \dots p_r \end{aligned}$$

Similarly,

$$v_\ell(n) = \# \text{ of times } \ell \text{ appears in the factorisation } n = q_1 \dots q_s$$

Thus every prime ℓ appears the same number of times in each factorisation, giving the desired result. \square

Remark. Another way of interpreting this result is to say that for $n \in \mathbb{N}_1$,

$$n = p_1^{v_{p_1}(n)} p_2^{v_{p_2}(n)} \dots p_r^{v_{p_r}(n)}$$

where p_1, \dots, p_r are the distinct prime factors of n . Note that we take the empty product to be 1, which covers the case for $n = 1$.

Lemma 2.11. Let $n = \prod_{i=1}^r p_i^{a_i}$ where each $a_i \in \mathbb{N}_0$ and the p_i 's are distinct primes. The set of positive divisors of n is the set of numbers of the form $\prod_{i=1}^r p_i^{c_i}$ where $0 \leq c_i \leq a_i$ for $i = 1, \dots, r$.

Proof. Exercise \square

2.2 Congruences

Definition 2.12. Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}_1$. We write $a \equiv b \pmod{n}$, and say ‘ a is congruent to $b \pmod{n}$ ’, if and only if $n \mid (a - b)$. If $n \nmid (a - b)$ we say that a and b are incongruent mod n .

Remark. In particular, $a \equiv 0 \pmod{n}$ if and only if $n \mid a$

Example. Here are some examples:

- $4 \equiv 30 \pmod{13}$ since $13 \mid (4 - 30) = -26$
- $17 \not\equiv -17 \pmod{4}$ since $17 - (-17) = 34$ but $4 \nmid 34$.
- n is even if and only if $n \equiv 0 \pmod{2}$
- n is odd if and only if $n \equiv 1 \pmod{2}$
- $a \equiv b \pmod{1}$ for all $a, b \in \mathbb{Z}$

Proposition 2.13. Let $n \in \mathbb{N}_1$ being congruent mod n is an equivalence relation, so,

1. Reflexive: $\forall a \in \mathbb{Z}, a \equiv a \pmod{n}$
2. Symmetric: $\forall a, b \in \mathbb{Z}, a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$
3. Transitive: $\forall a, b \in \mathbb{Z}, a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.

Proof. The proof follows from,

1. $n \mid 0$.
2. If $n \mid (a - b)$ then $n \mid (b - a)$
3. If $n \mid (a - b) + (b - c) = (a - c)$

□

Proposition 2.14. Congruences respect addition, subtraction and multiplication. Then let $a, b, \alpha, \beta \in \mathbb{Z}$. Suppose that $a \equiv \alpha \pmod{n}$ and $b \equiv \beta \pmod{n}$. Then,

1. $a + b \equiv \alpha + \beta \pmod{n}$
2. $a - b \equiv \alpha - \beta \pmod{n}$
3. $ab \equiv \alpha\beta \pmod{n}$

Moreover, if $f(x) \in \mathbb{Z}[x]$ then $f(a) \equiv f(\alpha) \pmod{n}$

Proof. Check that $ab \equiv \alpha\beta \pmod{n}$. Since, $a \equiv \alpha \pmod{n}$ and so, $n \mid (a - \alpha)$ and so $a = \alpha + ns$ for some $s \in \mathbb{Z}$. Similarly $b = \beta + nt$. Hence,

$$ab = (\alpha + ns)(\beta + nt) = \alpha\beta + n(s\beta + t\alpha + nst)$$

and so $n \mid (ab - \alpha\beta)$. Therefore, $ab \equiv \alpha\beta \pmod{n}$, as required. □

Example. Let $n \in \mathbb{N}_1$ and write n in decimal notation,

$$n = \sum_{i=0}^k a_i \times 10^i \quad 0 \leq a_i \leq 9$$

Then, define $f(x)$ by,

$$f(x) = \sum_{i=0}^k a_i x^i$$

Then, since $10 \equiv -1 \pmod{11}$, we see that $n = f(10) \equiv f(-1) \pmod{11}$, whence,

$$11 \mid n \iff 11 \mid f(-1) \iff 11 \mid (a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k)$$

This is an easy way to test for divisibility by 11.

Example. Does $x^2 - 3y^2 = 2$ have a solution with $x, y \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}$. Note that $x^2 - 3y^2 \equiv x^2 \pmod{3}$. Now, $x \equiv 0, 1, 2 \pmod{3}$, so $x^2 \equiv 0, 1, 4 \pmod{3} \equiv 0, 1 \pmod{3}$. Hence, $x^2 - 3y^2 \equiv x^2 \not\equiv 2 \pmod{3}$ and so $x^2 - 3y^2 \neq 2$.

Remark. Suppose we have $f \in \mathbb{Z}[x_1, \dots, x_m]$ if we have $a_1, \dots, a_m \in \mathbb{Z}$ such that $f(a_1, \dots, a_m) = 0$ then $f(a_1, \dots, a_m) \equiv 0 \pmod{n}$ for every $n \in \mathbb{N}$. Therefore if there exist an $n \in \mathbb{N}_1$ such that $f(x_1, \dots, x_m) \equiv 0 \pmod{n}$ has no solution, there cannot exist $a_1, \dots, a_m \in \mathbb{Z}$ such that $f(a_1, \dots, a_m) = 0$.

We are going to prove the following theorem,

Theorem 2.15. There are infinitely many primes p with $p \equiv 3 \pmod{4}$

Proof. Suppose that p is a prime. Then $p \equiv 0, 1, 2, 3 \pmod{4}$, but $p \not\equiv 0 \pmod{4}$ because $4 \nmid p$. If $p \equiv 2 \pmod{4}$ then $p = 4k + 2$ for some $k \in \mathbb{Z}$, so $2 \mid p$ so in fact $p = 2$. Therefore there are three types of primes,

1. $p = 2$
2. $p \equiv 1 \pmod{4}$
3. $p \equiv 3 \pmod{4}$

Let $N \in \mathbb{N}$ it suffices to show that there exist a type (iii) prime with $p > N$. Let $4(N!) - 1$ and so $M \geq 3$ and so by the existence of FTA we can write $M = p_1 \dots p_k$. If $p \leq N$, then $M \equiv -1 \pmod{p}$ so $p \nmid M$. Hence, $p_j > N$ for all j . Moreover $p_j \neq 2$ for all j because M is odd. Therefore for each j we have $p_j \equiv 1, 3 \pmod{4}$. If $p_j \equiv 3 \pmod{4}$ for any j then we are done. If this is not the case, then $p_j \equiv 1 \pmod{4}$ for all j , and so, $M \equiv 1 \times 1 \times \cdots \times 1 \pmod{4} \equiv 1 \pmod{4}$; but by definition of M we have $M \equiv -1 \equiv 3 \pmod{4}$ - contradiction! \square

Remark. Congruences do not respect division, $4 \equiv 14 \pmod{10}$ but $2 \not\equiv 7 \pmod{10}$

Proposition 2.16. Let $a, b, s \in \mathbb{Z}$ and $d, n \in \mathbb{N}_1$.

1. If $a \mid b \pmod{n}$ and $d \mid n$ then $a \mid b \pmod{d}$
2. Suppose $s \neq 0$. Then $a \equiv b \pmod{n}$ if and only if $as \equiv bs \pmod{ns}$

Proof. (i) follows from transitivity of divisibility;

(ii) follows from multiplication and cancellation properties. \square

Theorem 2.17 (Cancellation law for Congruences). Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}_1$. Let $d = \gcd(c, n)$. Then $ac \mid bc \pmod{n} \iff a \equiv b \pmod{\frac{n}{d}}$. In particular, if n and c are coprime, then $ac \equiv bc \pmod{n} \iff a \equiv b \pmod{n}$.

Proof. Since, $d = \gcd(c, n)$, we may write $n = dn'$ and $c = dc'$ where $n', c' \in \mathbb{Z}$. Suppose $ac \equiv bc \pmod{n}$. Then $n \mid c(a - b)$ and so $n' \mid c'(a - b)$. However, $\gcd(n', c') = 1$ and so $n' \mid (a - b)$ by Euclid's Lemma. Thus, $a \equiv b \pmod{n'}$.

Suppose conversely $a \equiv b \pmod{n'}$ and so, $n' \mid (a - b)$ and so $n \mid d(a - b)$. But $d \mid c$ and so $d(a - b) \mid c(a - b)$ and thus $n \mid c(a - b)$ by the transitivity of divisibility. Thus $ac \equiv bc \pmod{n}$. \square

Proposition 2.18. Let $a, m, n \in \mathbb{Z}$. If m and n are coprime and if $m \mid a$ and $n \mid a$ then $nm \mid a$.

Proof. Since $m \mid a$ we can write $a = mc$ for some $c \in \mathbb{Z}$. Now $n \mid a = mc$ and $\gcd(m, n) = 1$ and so by Euclid's Lemma, $n \mid c$. Hence, $mn \mid mc = a$. \square

Corollary 2.19. Let $m, n \in \mathbb{N}$ be coprime and let $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ then $a \equiv b \pmod{mn}$.

Proof. We have $n \mid (a - b)$ and $m \mid (a - b)$. Since m and n are coprime we therefore have $mn \mid (a - b)$. \square

3 Residue Classes

Proposition 3.1. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}_1$. If $a \equiv b \pmod{n}$ and $|b - a| < n$ then $a = b$.

Proof. Since $n \mid (a - b)$, by the comparison property of divisibility we have $n \leq |a - b|$ unless $a - b = 0$. \square

As \pmod{n} is an equivalence relation,

Definition 3.2 (Residue Class). Consider $n \in \mathbb{N}$, then $a \in \mathbb{Z}$ we write $[a]_n$ for an equivalence class $a \pmod{n}$. Thus,

$$[a]_n = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\} = \{a + qn : q \in \mathbb{Z}\}$$

This is called the residue class of a modulo n

$[a]_n$ is the coset, $\mathbb{Z}/n\mathbb{Z}$.

Example. Consider $n = 2$, then,

$$[0]_2 = \{x \in \mathbb{Z} : x \equiv 0 \pmod{2}\}$$

$$[1]_2 = \{x \in \mathbb{Z} : x \equiv 1 \pmod{2}\}$$

Proposition 3.3. Let $n \in \mathbb{Z}$. The n residue classes are disjoint and thier union is the set of all integers. Or $\forall x \in \mathbb{Z}, x \equiv y \pmod{n}$ such that y is precisely one of $\{0, 1, \dots, n - 1\}$.

Proof. The integers $0, 1, \dots, n - 1$ are incongruent \pmod{n} by the Proposition 3.1. Hence, the residue classes are distinct and thus disjoint. Every integer must be in one of these classes by the division algorithm, as we can write $x = nq + r$. The result then follows from taking $x \equiv r \pmod{n}$ and hence, $x \in [r]_n$. \square

Distinct left cosets of $\mathbb{Z}/n\mathbb{Z}$ are always disjoint and partition \mathbb{Z} .

3.1 Complete Residue Systems

Definition 3.4 (Complete Residue System). Let $n \in \mathbb{N}_1$. If S is a subset of \mathbb{Z} containing exctly one element of each residue class modulo n we say that S is a complete residue system modulo n .

Proposition 3.5. The last proposition says $S = \{0, 1, \dots, n - 1\}$ is a complete residue system. Note, that if S is any complete residue system, then $|S| = n$. Any set of integers that are incongruent \pmod{n} are a complete residue system \pmod{n} .

Example. The following are complete residue systems,

$$\begin{aligned} &\{1, 2, \dots, n\} \\ &\{1, n + 2, 2n + 3, 3n + 4, \dots, n^2\} \\ &\{x \in \mathbb{Z} : -\frac{n}{2} < x \leq \frac{n}{2}\} \end{aligned}$$

Proposition 3.6. Let $n \in \mathbb{N}_1$ an $k \in \mathbb{Z}$. Assume n and k are coprime. If $\{a_1, \dots, a_n\}$ is a complete residue system modulo n then so is $\{ka_1, \dots, ka_n\}$.

Proof. If $ka_i \equiv ka_j \pmod{n}$ then by the cancellation law for congruences we have $a_i \equiv a_j \pmod{n}$ since $\gcd(k, n) = 1$. Therefore no two distinct elements in this set, $\{ka_1, \dots, ka_n\}$, are congruent modulo n . \square

Example. The set $\{0, 1, 2, 3, 4\}$ is a complete residue system $\pmod{5}$ and so $\{0, 2, 4, 6, 8\}$ is also a complete residue system $\pmod{5}$.

3.2 Linear Congruences

The most basic congruences are linear congruence, for example,

$$ax \equiv b \pmod{n}$$

When n is small, we can brute force it, however, it becomes impractical quickly.

Theorem 3.7 (Linear Congruences with exactly one solution). Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose that a and n are coprime. Then the linear congruence,

$$ax \equiv b \pmod{n}$$

has exactly one solution.

Proof. We need only to test $1, 2, \dots, n$ since they constitute a complete residue system. Therefore, we consider the products, $a, 2a, \dots, na$. Since a and n are coprime, these numbers are also a complete residue system. Hence, exactly one of the elements of this sets is congruent to $b \pmod{n}$. \square

Theorem 3.8 (Solubility of a Linear Congruence). Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Then the linear congruence,

$$ax \equiv b \pmod{n} \tag{1}$$

has one or more solutions if and only if $\gcd(a, n) \mid b$.

Proof. By definition, the congruence (1) is soluble if and only if $n \mid (b - ax)$ for some $x \in \mathbb{Z}$, and this is true if and only if $b - ax = ny$ for some $x, y \in \mathbb{Z}$. Hence (1) is soluble if and only if,

$$ax + ny = b$$

for some $x, y \in \mathbb{Z}$. Therefore this result follows from the solubility of linear equations theorem \square

Theorem 3.9. Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Let $d = \gcd(a, n)$. Suppose $d \mid b$ and write $a = da'$, $b = db'$ and $n = dn'$. Then the linear congruence

$$ax \equiv b \pmod{n} \tag{2}$$

has exactly d solutions modulo n . These are,

$$t, t + n', t + 2n', \dots, t + (d - 1)n' \tag{3}$$

where t is the unique solution $\pmod{n'}$ to,

$$a'x \equiv b' \pmod{n'} \tag{4}$$

Proof. Every solution of (2) is a solution of (4) and vice versa. Since a' and n' are coprime, (4) has exactly one solution, $t \pmod{n'}$ by the Theorem 3.7. Thus the d numbers in (3) are solutions of (4) and hence (2).

No two items in the list are congruent \pmod{n} since the relationships

$$\begin{aligned} t + rn' &\equiv t + sn' \pmod{n} && \text{with } 0 \leq r < d, 0 \leq s < d \\ rn' &\equiv sn' \pmod{n} && \text{and hence } r \equiv s \pmod{d} \end{aligned}$$

But $0 \leq |r - s| < d$ so $r = s$. It remains to show that (2) has no solutions other than (3). If y is a solution of (2), then $ay \equiv b \pmod{n}$. But we also have $at \equiv b \pmod{n}$. Thus $y \equiv t \pmod{n'}$ by the cancellation law for congruences. Hence, $y = t + kn'$ for some $k \in \mathbb{Z}$. But $r \equiv k \pmod{d}$ for some $r \in \mathbb{Z}$ such that $0 \leq r < d$. Therefore we have,

$$kn' \equiv rn' \pmod{n} \quad \text{and so } y \equiv t + rn' \pmod{n}$$

Therefore y is congruent \pmod{n} to one of these numbers in (3). \square

Algorithm. Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose we want to solve,

$$ax \equiv b \pmod{n} \quad (5)$$

Firstly apply Extended Euclidian algorithm to compute $d := \gcd(a, n)$ to find $x', y' \in \mathbb{Z}$ such that,

$$ax' + ny' = d \quad (6)$$

if $d \nmid b$ then there are no solutions. Otherwise, these are exactly d solutions \pmod{n} , which we find as follows. Write $a = da'$, $b = db'$ and $n = dn'$. Dividing (6) through by d gives,

$$a'x' + n'y' = 1 \quad (7)$$

Thus reducing this $\pmod{n'}$ gives $a'x' \equiv 1 \pmod{n'}$ and multiplying through by b' gives $a'(b'x') \equiv b' \pmod{n'}$. Therefore $t := b'x'$ is the unique solution to $a'x' \equiv b' \pmod{n'}$. Now the solutions to (5) are,

$$t, t + n', t + 2n', \dots, t + (d - 1)n'$$

4 $\mathbb{Z}/n\mathbb{Z}$, Chinese Remainder Theorem and $\varphi(n)$

4.1 $\mathbb{Z}/n\mathbb{Z}$ and its units

Definition 4.1. Let $n \in \mathbb{N}$. We write $\mathbb{Z}/n\mathbb{Z} = \{[a]_n : 0 \leq a \leq n-1\}$ (such that $|\mathbb{Z}/n\mathbb{Z}| = n$). We set $[a]_n + [b]_n := [a+b]_n$ and $[a]_n[b]_n := [ab]_n$. (We have showed that both of these are well defined).

Lemma 4.2. The set $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with $0 = [0]_n$ and $1 = [1]_n$

Proof. MTH2010 □

Definition 4.3. Let $n \in \mathbb{N}$. Let $(\mathbb{Z}/n\mathbb{Z})^\times$ denote the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$. Explicitly, we have

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} : \exists [b]_n \in \mathbb{Z}/n\mathbb{Z} \text{ such that } [a]_n[b]_n = 1\}$$

This is a finite group under multiplication, and is abelian since $\mathbb{Z}/n\mathbb{Z}$ is commutative.

Definition 4.4 (Multiplicative inverse). Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then the unique solution to $ax \equiv 1 \pmod{n}$ is called the multiplicative inverse of $a \pmod{n}$ and is denoted $[a]_n^{-1}$ or $a^{-1} \pmod{n}$

4.2 Chinese Remainder Theorem

Theorem 4.5 (Special Chinese Remainder Theorem). Let $n, m \in \mathbb{N}$ be coprime and $a, b \in \mathbb{Z}$ be given. Then the pair of linear congruences,

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a solution $x \in \mathbb{Z}$. Moreover, if x' is another solution $x \equiv x' \pmod{mn}$

Proof. Since n and m are coprime, there must exist some $a', b' \in \mathbb{Z}$ such that $a'n \equiv 1 \pmod{m}$ and $b'n \equiv 1 \pmod{n}$. Define $x := aa'n + bb'm$. Then $x \equiv a'an \equiv a \pmod{m}$ and $x \equiv bb'm \equiv b \pmod{n}$.

Hence x is a solution, so suppose we have an x' that satisfies these equations. Then $m \mid (x - x')$ and $n \mid (x - x')$. Hence, as m and n are coprime, then it follows that $mn \mid (x - x')$, which is the same as $x \equiv x' \pmod{mn}$ □

Remark. We used the fact that m and n are coprime twice in the above proof. This is necessary because, for example $x \equiv 2 \pmod{12}$ and $x \equiv 4 \pmod{20}$ has no solution.

Theorem 4.6 (Chinese Remainder Theorem). Let $n_1, n_2, \dots, n_t \in \mathbb{N}$ with $\gcd(n_i, n_j) = 1$ whenever $i \neq j$ and let $a_1, \dots, a_t \in \mathbb{Z}$ be given. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_t \pmod{n_t} \end{aligned}$$

has a solution $x \in \mathbb{Z}$. Moreover if x' is any other solution, then $x' \equiv x \pmod{N}$ where $N := n_1 n_2 \dots n_t$.

Proof. Define $N_i := \frac{N}{n_i}$. Then $\gcd(N_i, n_i) = 1$, since n_i is coprime to all factors of N_i . Hence by the theorem on linear congruences with exactly one solution, there exists $x_i \in \mathbb{Z}$ such that $N_i x_i \equiv 1 \pmod{n_i}$. Next, define $x := \sum_{i=1}^t a_i N_i x_i$. Thus $x \equiv a_k N_k x_k \pmod{n_k}$ since $n_k \mid N_i$ for all k . Therefore, $x \equiv a_k (N_k x_k) \equiv a_k \pmod{n_k}$ for all k .

Suppose $x' \equiv a_k \pmod{n_k}$ for all k . Then $x' \equiv x \pmod{n_k}$ thus, $n_k \mid (x' - x)$, then since all n_i are coprime, $N \mid (x' - x)$. This yields that $x' \equiv x \pmod{N}$. □

4.3 Euler φ function

Definition 4.7 (Euler Phi Function). For $n \in \mathbb{N}$ we define the φ function as,

$$\varphi(n) = \#\{a \in \mathbb{N} : 1 \leq a \leq n, \gcd(a, n) = 1\}$$

Remark. $\varphi(1) = 1$ and for p prime, $\varphi(p) = \#\{1, 2, \dots, p-1\} = p-1$.

Remark. On the proposition on uniots of $\mathbb{Z}/n\mathbb{Z}$ and complete residue systems. We have that $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})$. Note, since $\gcd(0, n) = \gcd(n, n) = n$ for all $n \in \mathbb{N}$, we also have,

$$\varphi(n) = \#\{a \in \mathbb{Z} : 0 \leq a < n, \gcd(a, n) = 1\}$$

Theorem 4.8. Let $m, n \in \mathbb{N}$ be coprime. Then $\varphi(mn) = \varphi(m)\varphi(n)$

Proof. Let $a \in \mathbb{Z}$ with $0 \leq a < mn$ and define $b, c \in \mathbb{Z}$ by,

$$a \equiv b \pmod{m} \quad \text{and} \quad a \equiv c \pmod{n}$$

where $0 \leq b < m$ and $0 \leq c < n$. The Chinese Remainder Theorem tells us that there is a bijective correspondence between choices of a and pairs (b, c) . We now show that $\gcd(a, mn) = 1 \iff \gcd(b, m) = \gcd(c, n) = 1$. We shall use the proposition on units of $\mathbb{Z}/n\mathbb{Z}$ several times.

Suppose $\gcd(a, mn) = 1$. Then $ax \equiv 1 \pmod{mn}$ has a solution $r \in \mathbb{Z}$. By an earlier proposition we have $ar \equiv 1 \pmod{m}$ since $m \mid mn$. Hence, $br \equiv ar \equiv 1 \pmod{m}$ and so the congruence $bx \equiv 1 \pmod{m}$ is soluble. Thus, $\gcd(b, m) = 1$. Similarly, $\gcd(c, n) = 1$.

Suppose conversely $\gcd(b, m) = \gcd(c, n) = 1$. Then the congruences $bx \equiv 1 \pmod{m}$ and $cy \equiv 1 \pmod{n}$ are soluble so there exist $s, t \in \mathbb{Z}$ such that $bs \equiv 1 \pmod{m}$ and $ct \equiv 1 \pmod{n}$. Since m and n are coprime, by Chinese Remainder Theorem there exists $r \in \mathbb{Z}$ such that $r \equiv s \pmod{m}$ and $r \equiv t \pmod{n}$.

Hence $ar \equiv bs \equiv 1 \pmod{m}$ and $ar \equiv ct \equiv 1 \pmod{n}$ and so $x = ar$ is the solution to,

$$x \equiv 1 \pmod{m} \quad \text{and} \quad x \equiv 1 \pmod{n}$$

By the Chinese Remainder Theorem $ar \equiv 1 \pmod{mn}$. Hence, $\gcd(a, mn) = 1$.

Therefore the number of integers a with $0 \leq a < mn$ is equal to the number of pairs of integers (b, c) with $0 \leq b < m$, $\gcd(b, m) = 1$ and $0 \leq c < n$, $\gcd(c, n) = 1$, ie. $\varphi(m)\varphi(n)$. \square

Theorem 4.9. Let p be a prime and $r \in \mathbb{N}$. Then

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

Proof. For all $m \in \mathbb{N}$, either $\gcd(p^r, m) = 1$ or $p \mid m$. Thus,

$$\begin{aligned} \varphi(p^r) &= \#\{m \in \mathbb{N} : m \leq p^r, p \nmid m\} \\ &= \#\{m \in \mathbb{N} : m \leq p^r\} - \#\{m \in \mathbb{N} : m \leq p^r, p \mid m\} \\ &= p^r - p^{r-1} \\ &= p^{r-1}(p-1) \end{aligned}$$

\square

Proposition 4.10. Let $n \in \mathbb{N}$ such that $n \geq 2$. By FTA, we may write $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_r^{e_r}$ where all p_i 's are distinct and $e_i \in \mathbb{N}$. Then,

$$\varphi(n) = \prod_{i=1}^r (p_i - 1)p_i^{e_i-1}$$

Proof. By the last two theorems we have,

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{e_1} \cdots p_r^{e_r}) = \prod_{i=1}^r \varphi(p_i^{e_i}) \\ &= \prod_{i=1}^r (p_i^{e_i} - p_i^{e_i-1}) \\ &= \prod_{i=1}^r (p_i - 1) p_i^{e_i-1}\end{aligned}$$

□

Corollary 4.11. Let $n \in \mathbb{N}$. Then,

$$\varphi = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product runs over all distinct prime divisors of n .

Proof. From above,

$$\varphi(n) = \prod_{i=1}^r (p_i - 1) p_i^{e_i-1} = \prod_{i=1}^r p_i^{e_i} (1 - p_i^{-1}) \quad (8)$$

$$= n \prod_{i=1}^r (1 - p_i^{-1}) = \prod_{p|n} \left(1 - \frac{1}{p}\right) \quad (9)$$

□

Proposition 4.12. Let $n \in \mathbb{N}$, we have $\sum_{d|n} \varphi(d) = n$

Proof. We classify $\{1, 2, \dots, n\}$ according to their greatest common divisor with n . Thus,

$$\{a \in \mathbb{N} : a \leq n\} = \bigcup_{d|n} \{a \in \mathbb{N} : a \leq n, \gcd(n, a) = d\}$$

where the union is disjoint. Hence, $n = \sum_{d|n} R_d$ where $R_d := \#\{a \in \mathbb{N} : 1 \leq a \leq n, \gcd(n, a) = d\}$. If $d \mid n$, we can write $n = dn'$ and then by the distributive law of gcd's we have $\gcd(n, a) = d$ if and only if $a = da'$ with $\gcd(a', n') = 1$. Moreover, $a \leq n$ if and only if $a' \leq n'$. It follows that,

$$R_d = \#\{a' \in \mathbb{N} : 1 \leq a' \leq n', \gcd(n', a') = 1\}$$

and hence $R_d = \varphi(n')$. Then the size of that set is just $\varphi(n')$. Therefore $n = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$. However, when $d \mid n$ we have $n = d \cdot \frac{n}{d}$, thus d runs over the positive divisors of n , so does $e = \frac{n}{d}$ and therefore we have $\sum_{e|n} \varphi(e)$ □

5 Modular Exponentiation

Proposition 5.1. Fix $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. There exists some $r \in \mathbb{N}$ such that $a^r \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$.

Proof. Suppose there exists $r \in \mathbb{N}$ such that $a^r \equiv 1 \pmod{n}$. Then a^{r-1} is a solution to $ax \equiv 1 \pmod{n}$ and so $\gcd(a, n) = 1$ by the proposition on units of $\mathbb{Z}/n\mathbb{Z}$. Suppose conversely that $\gcd(a, n) = 1$ and so there are only finitely many possible values of $a^k \pmod{n}$ so there exists $i, j \in \mathbb{N}$ with $i < j$ such that $a^i \equiv a^j \pmod{n}$. Since $\gcd(a, n) = 1$ we may apply the cancellation law for congruences i times obtain $a^{j-i} \equiv 1 \pmod{n}$. Thus take $r = j - i$. \square

Definition 5.2 (Order). Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ and suppose $\gcd(a, n) = 1$. Then the least $d \in \mathbb{N}$ such that $a^d \equiv 1 \pmod{n}$ is called the order of $a \pmod{n}$ and is written $\text{ord}_n(a)$.

Proposition 5.3. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Suppose that $\gcd(a, n) = 1$. For $r, s \in \mathbb{Z}$ we have $a^r \equiv a^s \pmod{n}$ if and only if $r \equiv s \pmod{\text{ord}_n(a)}$.

Proof. Let $k = \text{ord}_n(a)$. Then $a^k \equiv 1 \pmod{n}$. Now assume wlog $r > s$. Suppose $r \equiv s \pmod{k}$, then there exists some $t \in \mathbb{N}$ such that $r = s + tk$. Hence,

$$a^r \equiv a^{s+tk} \equiv a^s (a^k)^t \equiv a^s \pmod{n}$$

Suppose conversely that $a^r \equiv a^s \pmod{n}$. Since $\gcd(a, n) = 1$ we may apply the cancellation law s times to obtain $a^{r-s} \equiv 1 \pmod{n}$. By the division algorithm, there exist $u, t \in \mathbb{N}_0$ such that $r-s = tk+u$ where $0 \leq u < k$.

$$a^{r-s} \equiv a^{u+tk} \equiv a^u (a^k)^t \equiv a^u \pmod{n}$$

and so $a^u \equiv 1 \pmod{n}$. However, $0 \leq u < k$ and k is the least positive integer such this is true. Hence $u = 0$. Therefore, $k \mid (r-s)$, ie. $r \equiv s \pmod{k}$. \square

Corollary 5.4. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ and suppose that $\gcd(a, n) = 1$. Then $a^k \equiv 1 \pmod{n}$ if and only if $\text{ord}_n(a) \mid k$.

Proof. Just take $r = k$ and $s = 0$ in the above proposition. \square

Corollary 5.5. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ and suppose $\gcd(a, n) = 1$. Then the numbers $\{1, a, a^2, \dots, a^{\text{ord}_n(a)-1}\}$ are all incongruent \pmod{n} .

Proof. Combine the above proposition with the proposition that says if $c, d \in \mathbb{Z}$ with $c \equiv d \pmod{n}$ and $|c-d| < n$ then $c = d$. \square

5.1 Reduced Residue Systems

Definition 5.6 (Reduced Residue System). Let $n \in \mathbb{N}$. A subset $R \subseteq \mathbb{Z}$ is said to be a reduced residue system \pmod{n} if

- R contains $\varphi(n)$ elements
- no two elements of R are congruent \pmod{n} and,
- $\forall r \in R, \gcd(r, n) = 1$

Remark. If R is a reduced residue system \pmod{n} then,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n : a \in R\}$$

Proposition 5.7. Let $n \in \mathbb{N}$ and $k \in \mathbb{Z}$. If $\{a_1, a_2, \dots, a_{\varphi(n)}\}$ is a reduced residue system \pmod{n} and $\gcd(k, n) = 1$ then $\{ka_1, ka_2, \dots, ka_{\varphi(n)}\}$ is also a reduced residue system \pmod{n} .

Proof. If $ka_i \equiv ka_j \pmod{n}$ then by the cancellation law for congruences $a_i \equiv a_j \pmod{n}$ since $\gcd(k, n) = 1$. Therefore, no two elements in $\{ka_1, ka_2, \dots, ka_{\varphi(n)}\}$ are congruent \pmod{n} . Moreover, since $\gcd(a_i, n) = \gcd(k, n) = 1$ we have $\gcd(ka_i, n) = 1$ so each ka_i is coprime to n . \square

5.2 Euler- Fermat Theorem

Theorem 5.8 (Euler-Fermat). Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Let $\{b_1, \dots, b_{\phi(n)}\}$ be a reduced residue system \pmod{n} . Then since $\gcd(a, n) = 1$, then $\{ab_1, ab_2, \dots, ab_{\phi(n)}\}$ is also a reduced residue system by the proposition on reduced residue systems. Hence the product in the first is congruent to the product of the second. Therefore,

$$b_1 b_2 \dots b_{\phi(n)} \equiv a^{\phi(n)} b_1 b_2 \dots b_{\phi(n)} \pmod{n}$$

then by the cancellation property and $\gcd(b_i, n)$ apply it repeatedly to get the required result. \square

Corollary 5.9. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ and suppose $\gcd(a, n) = 1$. Then $\text{ord}_n(a) \mid \phi(n)$.

Proof. Combine the Euler-Fermat Theorem and the earlier corollary that since $\gcd(a, n) = 1$, we have $a^k \equiv 1 \pmod{n}$ if and only if $\text{ord}_n(a) \mid k$. \square

Example. If we consider $\phi(12) = 4$. So for every $a \in \mathbb{Z}$ with $\gcd(a, 12) = 1$ we must have $\text{ord}_n(a) = 1, 2$ or 4 . In fact, we can notice that with the reduced residue systems $\{1, 5, 7, 11\}$ there isn't an element with order 4, and hence no element of order $\phi(12)$.

Corollary 5.10. Let p be a prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$

Proof. This follows immediately as $\phi(p) = p - 1$. \square

Example. We know that $\text{ord}_{19}(3) = 18 = \phi(19)$ and we know $\text{ord}_{19}(8) = 6$ which is a factor of 18.

Theorem 5.11 (Fermat's Little Theorem). Let p be a prime and let $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$.

Proof. If $p \nmid a$, this follows from the earlier corollary. If $p \mid a$, then a^p and a are congruent to $0 \pmod{p}$. \square

Remark. Many of the results in this section can be thought of in terms of group theory once we realise that, $(\mathbb{Z}/n\mathbb{Z})^\times$ is just a finite abelian group. For example, $\text{ord}_n(a)$ is just the order of $[a]_n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Moreover, Lagranges Theorem tells us that the order of an element divides the order of the group; so $\text{ord}_n(a) \mid \phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ which hence gives Euler-Fermat Theorem.

5.3 Modular Exponentiation

Let $b \in \mathbb{Z}$ and $e, m \in \mathbb{N}$. We want a way to compute $b^e \pmod{m}$ efficiently. We can write e in binary, ie. $e = \sum_{i=0}^k a_i 2^i$ where $a_i \in \{0, 1\}$ for $0 \leq i \leq k$. Then we observe,

$$b^e = b^{(\sum_{i=0}^k a_i 2^i)} = \prod_{i=0}^k \left(b^{2^i}\right)^{a_i}$$

Based on this we have the following algorithm,

Algorithm. Let $b \in \mathbb{Z}$ and $e, m \in \mathbb{N}$. Set $x = 1$ (x is the product). While $e > 0$ repeat,

1. If e is odd, the replace x by bx and reduce this \pmod{m} . (If e is even x is not altered).
2. Replace b by b^2 and reduce \pmod{m}
3. If e is even replace e by $\frac{e}{2}$, if e is odd, then replace e by $\frac{e-1}{2}$. (Drop the units in the binary expansion and shift the digits one to the right)

When this is completed $x \equiv b^e \pmod{m}$.

Example. We want to compute $3^{499} \bmod 997$. We set $b = 3$, $e = 499$, $m = 997$ and $x = 1$. Hence we get

step	$x \bmod m$	$b \bmod m$	e
0	1	3	499
1	3	9	249
2	27	81	124
3	27	579	62
4	27	249	31
5	741	187	15
6	981	74	7
7	810	491	3
8	904	804	1
9	3	-	0

$3^{499} \bmod 997$. Note that we don't need to calculate b in the last step. Moreover we get the binary expansion of 499, which is 111110011 (by going from bottom to top in e , ignoring the 0, letting odd be 1 and even 0). This minimises the number of multiplications, at one step we are just multiplying two integers modulo m , so they are small numbers.

5.4 Polynomial Congruence

Theorem 5.12 (Legranges Polynomial Congruence Theorem). Let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$$

and let p be a prime such that $p \nmid a_d$. Then $f(x) \equiv 0 \pmod p$ has at most d solutions $\bmod p$.

Remark. More generally, any polynomial equation of degree d over a field has at most d solutions (note that $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field).

Proof. The proof is by induction on d . When $d = 1$ we get that,

$$a_1x + a_2 \equiv 0 \pmod p$$

since $a_1 \not\equiv 0 \pmod p$, then $\gcd(a_1, p) = 1$ and so there is exactly one solution.

Assume that the theorem is true for polynomials of degree $d - 1$ and suppose for a contradiction that $f(x) \equiv 0 \pmod p$ has $d + 1$ incongruent solutions $\bmod p$ say x_0, x_1, \dots, x_d where $f(x_k) \equiv 0 \pmod p$. Recall we have for $r \in \mathbb{N}$,

$$x^r - y^r = (x - y)(x^{r-1} + x^{r-2}y + \cdots + xy^{r-2} + y^{r-1})$$

Hence,

$$f(x) - f(x_0) = \sum_{r=1}^n a_r(x^r - x_0^r) = \sum_{r=1}^n a_r(x - x_0)g_r(x)$$

where each $g_r \in \mathbb{Z}[x]$ is of degree $r - 1$ and has leading coefficient 1. Hence, $f(x) - f(x_0) = (x - x_0)g(x)$. Thus,

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \pmod p$$

since $f(x_k) \equiv f(x_0) \equiv 0 \pmod p$. But $x_k - x_0 \not\equiv 0 \pmod p$ if $k \neq 0$ so we must have $g(x_k) \equiv 0 \pmod p$ for each $k \neq 0$ (by cancellation law for congruences). But this means $g(x) \equiv 0 \pmod p$ has d incongruent solutions $\bmod p$ - contradiction! Hence desired result is proved. \square

Corollary 5.13. Let $a \in \mathbb{Z}$ and p be an odd prime. If $a^2 \equiv 1 \pmod p$, then $a \equiv \pm 1 \pmod p$.

Proof. Lagranges Polynomial Theorem says that $a^2 \equiv 1 \pmod{p}$ has at most two solutions and these are $a \equiv \pm 1 \pmod{p}$ are solutions and these must be distinct because p is odd. Therefore we have found all the solutions. \square

Example. Let p and q be distinct odd primes. Consider the congruence,

$$x^2 \equiv 1 \pmod{pq}$$

It is clear that $x \equiv \pm 1 \pmod{pq}$ are solutions, but are there any other solutions? By the CRT we have,

$$\begin{aligned} x^2 &\equiv 1 \pmod{pq} \\ \iff x^2 &\equiv 1 \pmod{p} \text{ and } x^2 \equiv 1 \pmod{q} \\ \iff x &\equiv \pm 1 \pmod{p} \text{ and } x \equiv \pm 1 \pmod{q} \end{aligned}$$

Thus there are four solutions \pmod{pq} . Hence,

$$x \equiv 1 \pmod{pq} \iff \begin{cases} x \equiv 1 \pmod{p} \\ x \equiv 1 \pmod{q} \end{cases}$$

and

$$x \equiv -1 \pmod{pq} \iff \begin{cases} x \equiv -1 \pmod{p} \\ x \equiv -1 \pmod{q} \end{cases}$$

and so there remains two pairs of congruences,

$$\begin{cases} x \equiv 1 \pmod{p} \\ x \equiv -1 \pmod{q} \end{cases} \quad \text{and} \quad \begin{cases} x \equiv -1 \pmod{p} \\ x \equiv 1 \pmod{q} \end{cases}$$

Note that if x is a solution to one of these, then x is a solution of the other.

6 Hensel Lifting, Primitive Roots and Wilson's Theorem

6.1 Hensel Lifting

Suppose we want to solve a polynomial congruence,

$$f(x) \equiv 0 \pmod{n}$$

this can be reduced to solving a system of congruences,

$$f(x) \equiv 0 \pmod{p_i^{e_i}}$$

where $n = p_1^{e_1} \dots p_i^{e_i}$ and we shall now show that this can be reduced further to linear congruences of $\pmod{p_i}$.

Theorem 6.1 (Hensel's Lemma). Let p be a prime. Let $f(x) \in \mathbb{Z}[x]$ and let $f'(x) \in \mathbb{Z}[x]$ be its formal derivative. If $a \in \mathbb{Z}$ satisfies,

$$f(a) \equiv 0 \pmod{p}, \quad f'(a) \not\equiv 0 \pmod{p}$$

then for each $n \in \mathbb{N}$ there exists $a_n \in \mathbb{Z}$ such that

$$f(a_n) \equiv 0 \pmod{p^n} \quad \text{and} \quad a_n \equiv a \pmod{p}$$

Moreover, a_n is unique modulo p^n .

If we take $f(x) = x^2 + 1$ ($x^2 \equiv -1 \pmod{5^4}$) and $a = 2$, we can apply the above lemma. Let $a_2 = 2 + 5t_1$, we now plug this into $f(a_2) \equiv 0 \pmod{5^2}$ and get that $t_1 \equiv 1 \pmod{5}$, hence $a_2 = 7$. Now we could let $a_3 = 7 + 5^2t_2$ and then similarly to before solve for t_2 using $f(a_3) \equiv 0 \pmod{5^3}$. However, we can shortcut by writing $a_4 = 7 + 5^2t_3$, this is because we know $a_4 \equiv a_2 \pmod{5^2}$. Then we get that, $t_3 \equiv 7 \pmod{5^2}$. Therefore, $a_4 = 7 + 5^2 \times 7 = 182$. If we started with $a = -2$, then we would have ended up with $a_4 = -182$.

Remark. Even if the hypotheses of Hensel's Lemma are not satisfied, we can still try to use the same technique. However, it may not exist or be unique.

Proof of Hensel's Lemma.

Lemma 6.2. Let $f \in \mathbb{Z}[X]$ and let $f'(X)$ be its formal derivative. Then there exists $g \in \mathbb{Z}[X, Y]$ satisfying the following polynomial identity,

$$f(X + Y) = f(X) + f'(X)Y + g(X, Y)Y^2$$

Remark. The identity of the Lemma is similar to Taylor's Formula, but we don't have factorials as they can cause issues reducing modulo p .

Proof of Lemma 6.2. The formula comes from isolating the first two terms in the binomial theorem. Writing $f(X) = \sum_{i=0}^d c_i X^i$ we have,

$$f(X + Y) = \sum_{i=0}^d c_i (X + Y)^i = c_0 + \sum_{i=1}^d c_i (X^i + iX^{i-1}Y + g_i(X, Y)Y^2)$$

where $g_i \in \mathbb{Z}[X, Y]$.

$$\begin{aligned} f(X + Y) &= \sum_{i=0}^d c_i X^i + \sum_{i=1}^d i c_i X^{i-1} Y + \sum_{i=1}^d c_i g_i(X, Y) Y^2 \\ &= f(X) + f'(X)Y + g(X, Y)Y^2 \end{aligned}$$

where $g(X, Y) = \sum_{i=1}^d c_i g_i(X, Y)$. Gives the desired identity. \square

We will prove Hensel's Lemma by induction on $n \in \mathbb{N}$, the assumptive step being there exists a $a_n \in \mathbb{Z}$ satisfying (1) that is unique $\pmod{p^n}$. The $n = 1$ case is trivial using $a_1 = a$. We now suppose the inductive hypothesis holds for $n = k$ and prove for $n = k + 1$. The idea is to consider $a_k + p^k t_k$ and see if $t_k \in \mathbb{Z}$ can be chosen in such a way that $a_k + p^k t_k$ satisfies the required properties of a_{k+1} . By the earlier lemma with $X = a_k$ and $Y = p^k t_k$ there exists $z_k \in \mathbb{Z}$ such that,

$$\begin{aligned} f(a_k + p^k t_k) &= f(a_k) + f'(a_k)p^k t_k + z_k p^{2k} t_k^2 \\ &\equiv f(a_k) + f'(a_k)p^k t_k \pmod{p^{k+1}} \end{aligned}$$

We have $z_k \in \mathbb{Z}$ not $z_k \in \mathbb{Z}[X, Y]$ are consider $g(a, b)$ where we have already considered $a, n \in \mathbb{Z}$. Hence the second follows as $k + 1 \leq 2k$. In $f'(a_k)p^k t_k$ the factors $f'(a_k)$ and t_k only matter \pmod{p} since it already contains a factor of p^k and the modulus is p^{k+1} . Thus recalling that $a_k \equiv a \pmod{p}$ we have $f'(a)p^k t_k \equiv f'(a_k)p^k t_k \pmod{p^{k+1}}$.

Therefore we have,

$$\begin{aligned} f(a_k + p^k t_k) \equiv 0 \pmod{p^{k+1}} &\iff f(a_k) + f'(a_k)p^k t_k \equiv 0 \pmod{p^{k+1}} \\ &\iff f'(a_k)t_k \equiv -\frac{f(a_k)}{p^k} \pmod{p} \end{aligned}$$

Where we already know $-\frac{f(a_k)}{p^k} \in \mathbb{Z}$ by the induction hypothesis. But $f'(a) \not\equiv 0 \pmod{p}$ and so $\gcd(f'(a), p) = 1$ and thus by the theorem on linear congruences with exactly one solution, the last congruence (\pmod{p}) has a solution t_k , which is unique \pmod{p} . We set $a_{k+1} = a_k + p^k t_k$. Then we have $f(a_{k+1}) \equiv 0 \pmod{p^{k+1}}$ and $a_{k+1} \equiv a_k \pmod{p^k}$, so in particular $a_{k+1} \equiv a \pmod{p}$.

It remains to show uniqueness. Suppose $\exists b_{k+1} \in \mathbb{Z}$ with $f(b_{k+1}) \equiv 0 \pmod{p^{k+1}}$ and $b_{k+1} \equiv a \pmod{p}$ and so $f(b_{k+1}) \equiv 0 \pmod{p^k}$. Then by the induction hypothesis we have $b_{k+1} \equiv a_k \pmod{p^k}$. Thus $b_{k+1} = a_k + p^k s_k$ for some $s_k \in \mathbb{Z}$. But the displayed equation above and proceeding discussion shows that $s_k \equiv t_k \pmod{p}$ and thus, $a_{k+1} \equiv b_{k+1} \pmod{p^{k+1}}$ as desired. \square

Remark. An adaptation of the above proof can show in principle one can always lift from a solution from p^k to a solution $\pmod{p^{2k}}$.

Moreover, for $m > n > 1$ we always have $a_m \equiv a_n \pmod{p^n}$.

6.2 Primitive Roots

We recall that if $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ and $\gcd(a, n) = 1$, then $\text{ord}_n(a) \mid \phi(n)$. In this section we are interested where $\text{ord}_n(a) = \phi(n)$.

Definition 6.3 (Primitive Root). Let $n \in \mathbb{N}$, we say $a \in \mathbb{Z}$ is a primitive root \pmod{n} if and only if $\gcd(a, n) = 1$ and $\text{ord}_n(a) = \phi(n)$.

Remark. This is equivalent for $[a]_n$ to be a generator for the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$, which then must be cyclic.

another remark,

Remark. For some values of n there are no primitive roots, for example every non trivial element of $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ and so $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic.

Lemma 6.4. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that they are coprime. Then for $k \in \mathbb{Z}$ we have,

$$\text{ord}_n(a^k) = \frac{\text{ord}_n(a)}{\gcd(\text{ord}_n(a), k)}$$

In particular, $\text{ord}_n(a) = \text{ord}_n(a^k)$ if and only if $\gcd(\text{ord}_n(a), k) = 1$.

Proof. Let $f = \text{ord}_n(a)$. The integer $\text{ord}_n(a^k)$ is the least $d \in \mathbb{N}$ such that $a^{dk} \equiv 1 \pmod{n}$. By an earlier corollary, this is also the least d such that $dk \equiv 0 \pmod{f}$. But, by the cancelation law for congruence we can say $d \equiv 0 \pmod{\frac{f}{h}}$ where $h = \gcd(f, k)$. But it is clear the least positive integer that is a solution is just $d = \frac{f}{h}$ and so $\text{ord}_n(a^k) = \frac{f}{h}$ as required. \square

Theorem 6.5. Let p be a prime and let $d \in \mathbb{N}$ be a divisor of $p-1$. Then there are exactly $\phi(d)$ elements $a \pmod{p}$ such that $\text{ord}_p(a) = d$. In particular there are $\phi(p-1)$ primitive roots \pmod{p} .

Proof. Fix a prime p and for any $d \in \mathbb{N}$ such that $d \mid (p-1)$ define,

$$A(d) = \{a \in \mathbb{N} : 1 \leq a \leq p-1, \text{ord}_p(a) = d\}$$

Let $\psi(d) = \#A(d) \geq 0$. We aim to show that $\psi(d) = \phi(d)$. Since the sets $A(d)$ partition $\{1, 2, \dots, p-1\}$ we have,

$$\sum_{d \mid (p-1)} \psi(d) = p-1$$

and we also know that,

$$\sum_{d \mid (p-1)} \phi(d) = p-1$$

Therefore, we can show that if $\psi(d) < \phi(d)$ for all $d \mid (p-1)$ then $\psi(d) = \phi(d)$ for all such d . (Otherwise if $\psi(d_0) < \phi(d_0)$ then the sums can't be equal - contradiction.).

If $\psi(d) = 0$, then $\psi(d) < \phi(d)$ and we are done. Hence, $\psi(d) \geq 1$. Then $A(d) \neq \emptyset$ and so $a \in A(d)$ for some a . Hence $\text{ord}_p(a) = d$ and so $a^d \equiv 1 \pmod{p}$. Then $(a^i)^d \equiv 1 \pmod{p}$ for all $i \in \mathbb{Z}$.

In particular,

$$a, a^2, \dots, a^d$$

are all solutions to $x^d - 1 \equiv 0 \pmod{p}$. By an earlier corollary we have that all the above numbers are incongruent \pmod{p} and by Lagrange's polynomial congruence theorem, then the congruence above has at most d solutions. So the above numbers are solutions to that congruence and are the only solutions. Hence each number in $A(d)$ must be congruent to $a^k \pmod{p}$ for some $k = 1, \dots, d$. By Lemma 6.4, $\text{ord}_p(a^k) = d$ if and only if $\gcd(k, d) = 1$. In other words, from the list of numbers, there are $\phi(d)$ of them that have order $d \pmod{p}$. Thus $\psi(d) = \phi(d)$ if $\psi(d) \neq 0$, as required. \square

Corollary 6.6. Let p be prime, then there exists a primitive root g modulo p (not necessarily unique). In other words, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Moreover, for any $a \in \mathbb{Z}$ with $p \nmid a$, $\exists k \in \mathbb{Z}$, such that $a \equiv g^k \pmod{p}$.

Proof. The existence of primitive roots follow by the theorem as $\phi(p-1) \geq 1$. By definition, $\text{ord}_p(g) = p-1$ and $1, g, g^2, \dots, g^{p-2}$ are congruent modulo p , in some order which gives the last claim. \square

Theorem 6.7 (Primitive Root Test). Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ where a and n are coprime. Then a is a primitive root \pmod{n} if and only if

$$a^{\frac{\phi(n)}{q}} \not\equiv 1 \pmod{n}$$

for every prime $q \mid \phi(n)$.

Proof. If $a^{\frac{\phi(n)}{q}} \equiv 1 \pmod{n}$, then $\text{ord}_n(a) \leq \frac{\phi(n)}{q} < \phi(n)$ and so cannot be a primitive root modulo n .

Suppose conversely that $a^{\frac{\phi(n)}{q}} \not\equiv 1 \pmod{n}$ for every prime $q \mid \phi(n)$. Consider the prime factorisation of $n = \prod_i p_i^{r_i}$. Let $m = \text{ord}_n(a)$, then $m \mid \phi(n)$ and so $m = q_1^{t_1} \dots q_s^{t_s}$ where $0 \leq t_i \leq r_i$. Suppose that $m < \phi(n)$.

Then $\exists j, t_j < r_j$, hence $m \mid q_1^{r_1} \dots q_j^{t_j} \dots q_s^{r_s} = (\phi(n)/q_j)$. But $a^m \equiv 1 \pmod{n}$ and so $a^{\frac{\phi(n)}{q_j}} \equiv 1 \pmod{n}$ - Contradiction. \square

Theorem 6.8. Let p be a prime. If g is a primitive root mod p , then g is also a primitive root mod p^e for all $e > 1$ if and only if $g^{p-1} \not\equiv 1 \pmod{p^2}$.

Proof. Not examinable. See Apostol Introduction to ANT, Chp 10. \square

Theorem 6.9. Let $n \in \mathbb{N}$. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic \iff there exists a primitive root modulo $n \iff n = 1, 2, 4, p^e, 2p^e$ where $e \in \mathbb{N}$ and p is an odd prime.

Proof. Not examinable. See again Apostol Introduction to ANT, Chp 10. \square

6.3 Wilson's Theorem

Theorem 6.10 (Wilson's Theorem). An integer is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Proof. Suppose that n is composite. Then there exists d dividing n with $1 < d < n$. Therefore, $d \mid (n-1)!$ and $d \mid n$. So if $(n-1)! \equiv -1 \pmod{n}$, then $n \mid ((n-1)! + 1)$ and so $d \mid ((n-1)! + 1)$. Hence, $d \mid 1 = ((n-1)! + 1) - (n-1)!$ - Contradiction. Hence, $(n-1)! \not\equiv -1 \pmod{n}$.

Suppose p is a prime. The case $p = 2$ is easy so we can assume that p is odd. Each $a \in \{1, 2, \dots, p-1\}$ is coprime to p and therefore has a unique inverse $a^{-1} \in \{1, 2, \dots, p-1\}$ modulo p , that is $aa^{-1} \equiv 1 \pmod{p}$. Note that $(a^{-1})^{-1} \equiv a \pmod{p}$. If $a = a^{-1}$, the $1 \equiv aa^{-1} \equiv a^2 \pmod{p}$ and so $a \equiv \pm 1 \pmod{p}$ and so $a = 1$ or $a = p-1$. In the product,

$$(p-1)! = 1 \times 2 \times \dots \times (p-2) \times (p-1)$$

we pair off each term except 1 and $p-1$. Hence, $(p-1)! \equiv 1 \times (p-1) \equiv -1 \pmod{p}$. \square

We now consider an alternative proof using primitive roots.

Alternative proof using Primitive Roots for Wilson's Theorem. If n is composite, proceed as before. Again, we are reduced to considering p as an odd prime. Let g be a primitive root modulo p . Then the powers $1, g, g^2, \dots, g^{p-2}$ are congruent modulo p in some order,

$$(p-1)! = 1gg^2g^3 \dots g^{p-2} = g^{1+2+\dots+(p-2)}$$

and the sum is just an arithmetic progression we see that,

$$(p-1)! \equiv g^{(p-1)(p-2)/2} \pmod{p}$$

as p is odd, we can write $p = 2k+1$ and as $k < 2k = p-1$ then $g^k \not\equiv 1 \pmod{p}$ but $g^{2k} = g^{p-1} \equiv 1 \pmod{p}$ as $\text{ord}_p(g) = p-1$ by definition. Since $(g^k)^2 = g^{2k} \equiv 1 \pmod{p}$ and p is an odd prime we have $g^k \equiv \pm 1 \pmod{p}$. Hence, $g^k \equiv -1 \pmod{p}$. We now conclude,

$$\begin{aligned} (p-1)! &\equiv g^{(p-1)(p-2)/2} \pmod{p} \\ &= g^{(2k-1)k} \\ &= (g^k)^{2k-1} \\ &\equiv (-1)^{2k-1} \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

\square

7 Quadratic Residues, Legendre Symbols, Euler Criterion and Gauss' Lemma

We will study the theory of congruences modulo an odd prime p . By completing the square we can reduce any quadratic residue to,

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

Lemma 7.1. Let p be an odd prime and $a \in \mathbb{Z}$. Consider,

$$x^2 \equiv a \pmod{p} \tag{10}$$

if $p \mid a$, then (1) is equivalent to $x \equiv 0 \pmod{p}$. Otherwise if $p \nmid a$ and (1) has one solution, then $x \equiv b \pmod{p}$ then $p \nmid b$ and $x \equiv -b$ is another, different solution.

Proof. If $x \equiv 0 \pmod{p}$, then clearly $x^2 \equiv 0 \pmod{p}$. The converse follows from Euclid's Lemma for primes. Now suppose $p \nmid a$ and $b^2 \equiv a \pmod{p}$, then clearly $-b$ is also a solution to this equation. If $b \equiv -b \pmod{p}$ and so $b \equiv 0 \pmod{p}$. But then $a \equiv b^2 \equiv 0 \pmod{p}$ - Contradiction as $a \nmid p$. \square

Definition 7.2 (Quadratic Residue). Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then a is a Quadratic Residue mod p if $\exists x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$ and a is a Quadratic Non-Residue if not.

Proposition 7.3. Let p be an odd prime. Then every reduced residue system mod p contains exactly $\frac{(p-1)}{2}$ quadratic residues and $\frac{(p-1)}{2}$ quadratic non-residues mod p . The quadratic residue belong to the residue classes containing,

$$1^2, 2^2, \dots, \left(\frac{(p-1)}{2}\right)^2$$

Proof. First show that the list of numbers are distinct mod p . If $x^2 \equiv y^2 \pmod{p}$ where $1 \leq x, y \leq \frac{p-1}{2}$ then $(x+y)(x-y) \equiv 0 \pmod{p}$. But, $1 < x+y < p$ so $x+y$ is coprime to p . So by the Cancellation Law, we must have $x-y \equiv 0 \pmod{p}$ and so $x \equiv y \pmod{p}$ and as $|x-y| < p$, then $x = y$. The remaining squares are,

$$\left(\frac{p+1}{2}\right)^2, \left(\frac{p+3}{2}\right)^2, \dots, (p-2)^2, (p-1)^2$$

but $(p-k)^2 \equiv (-k)^2 \equiv k^2 \pmod{p}$ for every $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{(p-1)}{2}$, these are then congruent to,

$$\left(\frac{p-1}{2}\right)^2, \left(\frac{p-3}{2}\right)^2, \dots, 2^2, 1^2$$

this is our original list. Hence, there are precisely $\frac{p-1}{2}$ quadratic residues mod p and so there are $\frac{p-1}{2}$ quadratic non-residues mod p . \square

7.1 Legendre Symbol

Definition 7.4 (Legendre Symbol). Let p be an odd prime. For any $a \in \mathbb{Z}$, we define the Legendre Symbol to be,

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & p \nmid a \text{ and } a \text{ is a quadratic residue mod } p \\ -1 & p \nmid a \text{ and } a \text{ is not a quadratic residue mod } p \\ 0 & p \mid a \end{cases}$$

Remark. By an earlier lemma, we see that $x^2 \equiv a \pmod{p}$ has precisely $\left(\frac{a}{p}\right) + 1$ distinct solutions mod p

Remark. We always have $\left(\frac{1}{p}\right) = 1$. Moreover, if $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{p}$. Then, $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right)$. This is sometimes known as periodicity.

Example. If $m \in \mathbb{Z}$ with $p \nmid m$, then $\left(\frac{m^2}{p}\right) = 1$.

7.2 Eulers Criterion

Lemma 7.5. Let p be an odd prime and let g be a primitive root mod p . Let $a \in \mathbb{Z}$ with $p \nmid a$. Then $a \equiv g^k \pmod{p}$ for some $k \in \mathbb{Z}$ and a is a quadratic residue mod p if and only if k is even.

Proof. First note that a primitive root $g \pmod{p}$ exists by an earlier Corollary, so $a \equiv g^k \pmod{p}$ for some $k \in \mathbb{Z}$. Suppose $k \in \mathbb{Z}$ is even. Then $k = 2j$ and so $a \equiv (g^j)^2 \pmod{p}$. Thus a is a quadratic residue mod p . Suppose conversely a is a quadratic residue mod p . Then $a \equiv b^2 \pmod{p}$ for some $b \in \mathbb{Z}$ and $p \nmid b$. Then $b \equiv g^r$ for some $r \in \mathbb{Z}$ and so $g^k \equiv (g^r)^2 \equiv g^{2r} \pmod{p}$. By an earlier proposition, we can say $k \equiv 2r \pmod{p-1}$ by an earlier proposition since $\text{ord}_p(g) = \phi(p) = p-1$. So $k \equiv 2r \pmod{2}$ since $2 \equiv (p-1)$. Hence $k \equiv 0 \pmod{2}$ and is even. \square

Theorem 7.6 (Eulers Criterion). If p is an odd prime and $a \in \mathbb{Z}$ then

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

Proof. This is obvious if $p \mid a$. So suppose $p \nmid a$. Let g be a primitive root mod p . Then there exists some $k \in \mathbb{Z}$ such that $a \equiv g^k \pmod{p}$. Since $\text{ord}_p(g) = p-1$ we have $g^{p-1} \equiv 1 \pmod{p}$ and $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Since p is an odd prime we have, $g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Therefore, $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Then,

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

The result now follows from the previous lemma. \square

Now for an alternative proof,

alternative proof. Again, we may suppose $p \nmid a$. Suppose that $\left(\frac{a}{p}\right) = 1$. Then $\exists b \in \mathbb{Z}$ with $p \nmid b$ such that $a \equiv b^2 \pmod{p}$. Thus by FLT we have,

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

Now suppose that $\left(\frac{a}{p}\right) = -1$ and consider the polynomial

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

since f has degree $\frac{p-1}{2}$, hence by Lagranges Polynomial Congruence Theorem,

$$f(x) \equiv 0 \pmod{p}$$

has $\frac{p-1}{2}$ solutions. But we have shown by that the quadratic residues mod p are solutions and there are $\frac{p-1}{2}$ of them. Hence, none of the quadratic non-residues are solutions and so $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. But by FLT we have $a^{p-1} \equiv 1 \pmod{p}$ and we can say that $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Therefore,

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

This completes the proof. \square

Theorem 7.7 (Multiplicity of Legendre's Symbol). Let p be an odd prime and $a, b \in \mathbb{Z}$. Then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$

Proof. If $p \mid a$ or $p \mid b$, then $p \mid ab$ so $\left(\frac{ab}{p}\right) = 0$ and so either $\left(\frac{a}{p}\right) = 0$ and $\left(\frac{b}{p}\right) = 0$, the result is proved.

No suppose $p \nmid a$ and $p \nmid b$. Then by Euclid's lemma for primes we have $p \nmid ab$. Moreover, Euler's Criterion tells us,

$$\begin{aligned} \left(\frac{ab}{p}\right) &= (ab)^{\frac{p-1}{2}} \\ &= a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \\ &= \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p} \end{aligned}$$

and both sides are ± 1 . If they were different, we could have $1 \equiv -1 \pmod{p}$ which means $p \mid 2$ - Contradiction. p is odd. \square

Now for another theorem,

Theorem 7.8. If p is an odd prime then,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$$

In other words, $x^2 \equiv -1 \pmod{p}$ is soluble if and only if $p \equiv 1 \pmod{4}$.

Proof. By Euler's Criterion,

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

and both sides are ± 1 . Then as above if they were different, $p \equiv 2$ and so they are the same as p is an odd prime. \square

Theorem 7.9. There are infinitely many primes p with $p \equiv 1 \pmod{4}$.

Proof. It suffices to prove that for any $N \in \mathbb{N}$ there exists a prime p with $p > N$ and $p \equiv 1 \pmod{4}$. Let $M = (2(N!))^2 + 1$. If p is a prime with $p \leq N$ then $M \equiv 1 \pmod{p}$ so $p \nmid M$. Let p be a prime factor of M , then $p > N$. As M is odd, p is also odd. Then we have $(2(N!))^2 \equiv -1 \pmod{p}$ and so the congruence $x^2 \equiv -1 \pmod{p}$ is soluble and so $p \equiv 1 \pmod{4}$ by the previous theorem. \square

7.3 Gauss' Lemma

We make the definition,

Definition 7.10. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. We write $\lambda(a, n)$ for the unique integer such that $a \equiv \lambda(a, n) \pmod{n}$ and $0 \leq \lambda(a, n) < n$, ie. $\lambda(a, n)$ is the remainder of the division algorithm applied to a and n .

We note this isn't standard notation, but it is useful. Now we move onto Gauss' Lemma,

Theorem 7.11 (Gauss' Lemma). Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then,

$$\left(\frac{a}{p}\right) = (-1)^\Lambda \quad \Lambda = \#\{j \in \mathbb{N} : 1 \leq j \leq \frac{p-1}{2}, \lambda(aj, p) > \frac{p}{2}\}$$

Example. Let $p = 13$ and $a = 5$.

If $j = 1$, then $\lambda(5, 13) = 5 < \frac{13}{2}$

If $j = 2$, then $\lambda(10, 13) = 10 < \frac{13}{2}$... and so on. We find that $\Lambda = \#\{2, 4, 5\} = 3$ and so $\left(\frac{5}{13}\right) = -1$.

Proof. Let $S_a = \{aj : 1 \leq j \leq \frac{p-1}{2}\}$ and we define,

$$\{r_i\}_{i=1}^m = \{\lambda(aj, p) : aj \in S_a, 0 \leq \lambda(aj, p) < \frac{p}{2}\}$$

$$\{s_i\}_{i=1}^n = \{\lambda(aj, p) : aj \in S_a, \frac{p}{2} \leq \lambda(aj, p) < p\}$$

so that $n = \Lambda$. Note that $\lambda(aj, p) \neq \frac{p}{2}$ since $\frac{p}{2} \notin \mathbb{Z}$ and $\lambda(aj, n) \neq 0$ since $p \nmid a$ and $p \nmid j$. Also note that $j_1 \neq j_2$ then $\lambda(aj_1, p) \neq \lambda(aj_2, p)$ since,

$$\begin{aligned} \lambda(aj_1, p) = \lambda(aj_2, p) &\implies aj_1 \equiv aj_2 \pmod{p} \\ &\implies j_1 \equiv j_2 \pmod{p} \\ &\implies j_1 = j_2 \end{aligned} \quad \text{since } 0 < j_1, j_2 < p.$$

Hence, $m + n = \#S_a = \frac{p-1}{2}$ as we proved that there isn't anything at the end points and distinct j 's return distinct values. We claim that,

$$\{r_1, \dots, r_m, (p - s_1), \dots, (p - s_n)\} = \{1, 2, \dots, \frac{p-1}{2}\}$$

It is clear that $r_i, (p - s_i) \in \{1, 2, \dots, \frac{p-1}{2}\}$ and there are $\frac{p-1}{2}$ elements so it suffices to prove that they are all different. We have already show that $r_i \neq r_j$ and $s_i \neq s_j$ for $i \neq j$. To show that $r_i \neq p - s_j$ we argue by contradiction. If $r_i + s_i = p$, let $r_i = \lambda(aj_1, p)$ and $s_i = \lambda(aj_2, p)$. Then,

$$\begin{aligned} r_i + s_j &= p \\ &= \lambda(aj_1, p) + \lambda(aj_2, p) \\ &\equiv aj_1 + aj_2 \pmod{p} \\ &\equiv a(j_1 + j_2) \pmod{p} \end{aligned}$$

Hence, $a(j_1 + j_2) \equiv 0 \pmod{p}$. So by Euclids Lemma for primes, either $p \mid a$ or $p \mid j_1 + j_2$. However, $p \nmid a$ and $2 \leq j_1 + j_2 \leq p - 1$ so then $p \nmid j_1 + j_2$ - Contradiction. Therefore $r_i \neq p - s_j$.

Now on the one hand we have,

$$\begin{aligned} r_1 r_2 \dots r_m (p - s_1)(p - s_2) \dots (p - s_n) &= 1 \times 2 \times \dots \times \frac{p-1}{2} = \left(\frac{p-1}{2}\right)! \\ &= r_1 r_2 \dots r_m s_1 s_2 \dots s_n (-1)^n \pmod{p} \end{aligned}$$

On the other hand, by the definition of r_i and s_j ,

$$\begin{aligned} r_1 r_2 \dots r_m s_1 s_2 \dots s_n &= \prod_{j=1}^{\frac{p-1}{2}} \lambda(aj, p) \\ &= \prod_{j=1}^{\frac{p-1}{2}} (aj) \\ &\equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \end{aligned}$$

Therefore,

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

Now since $p \nmid \left(\frac{p-1}{2}\right)!$, the cancellation law for congruences shows that,

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

Now we rearrange and get $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$ and so $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$ by Euler's Criterion. Then both sides are ± 1 , if they were different, then we get that $2 \mid p$ - Contradiction. Therefore $\left(\frac{a}{p}\right) = (-1)^\Lambda$ as required. \square

Definition 7.12 (Floor Function). For any $x \in \mathbb{R}$ we set $\lfloor x \rfloor := \max\{n \in \mathbb{Z}\}$

Corollary 7.13. If p is an odd prime, then,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$$

Proof. Apply Gauss' Lemma for $a = 2$,

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

where $\Lambda = \#\{1 \leq j \leq \frac{p-1}{2} : \lambda(2j, p) > \frac{p}{2}\}$. Note that for $1 \leq j \leq \frac{p-1}{2}$ we have $2 \leq 2j \leq p-1$ and so $\lambda(2j, p) = 2j$. Moreover, $2j < \frac{p}{2}$ if and only if $j < \frac{p}{4}$ and $\frac{p}{2} < 2j < p$ if and only if $\frac{p}{4} < j < \frac{p}{2}$. It follows that, $\Lambda = \#\{j \in \mathbb{N} : \frac{p}{4} < j < \frac{p}{2}\}$. We can calculate this,

$$\begin{aligned} \#\{j \in \mathbb{N} : \frac{p}{4} < j < \frac{p}{2}\} &= \#\{j \leq \frac{p-1}{2}\} - \#\{j < \frac{p}{4}\} \\ &= \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \end{aligned}$$

Since p is odd, then one of the following must occur,

1. $p = 8k + 1 \implies \frac{p-1}{2} = 4k, \left\lfloor \frac{p}{4} \right\rfloor = 2k \implies \Lambda = 2k.$
2. $p = 8k + 3 \implies \frac{p-1}{2} = 4k + 1, \left\lfloor \frac{p}{4} \right\rfloor = 2k \implies \Lambda = 2k + 1.$
3. $p = 8k + 5 \implies \frac{p-1}{2} = 4k + 2, \left\lfloor \frac{p}{4} \right\rfloor = 2k + 1 \implies \Lambda = 2k + 1.$
4. $p = 8k + 7 \implies \frac{p-1}{2} = 4k + 3, \left\lfloor \frac{p}{4} \right\rfloor = 2k + 1 \implies \Lambda = 2k + 2$

Hence, $(-1)^\Lambda = +1 \iff p = 8k + 1$ or $p = 8k + 7$. We note that if $p = 8k + r$, then,

$$\frac{p^2 - 1}{8} = \frac{r^2 + 16rk + 64k^2 - 1}{8} = \frac{r^2 - 1}{8} + 2(kr + 4k^2) \equiv \frac{p^2 - 1}{8} \pmod{2}$$

By checking cases of $r = \pm 1, \pm 3$ and see,

$$\frac{p^2 - 1}{8} \equiv \begin{cases} 0 & \pmod{2} & p \equiv \pm 1 \pmod{8} \\ 1 & \pmod{2} & p \equiv \pm 3 \pmod{8} \end{cases}$$

and the result follows. \square

We now prove that there are more infinitely many primes!

Theorem 7.14. There are infinitely many primes p with $p \equiv -1 \pmod{8}$

Proof. It suffices to prove that for any $N \in \mathbb{N}$ there exists a prime p with $p > N$ and $p \equiv -1 \pmod{8}$. Let $M = 8(N!)^2 - 1$. If p is a prime with $p \leq N$ then $M \equiv -1 \pmod{p}$ and so $p \nmid M$. Let p be a prime factor of M , then p is odd and $p > N$. Moreover,

$$(4(N!))^2 \equiv 16(N!)^2 \equiv 2M + 2 \equiv 2 \pmod{p}$$

Thus, $\left(\frac{2}{p}\right) = 1$ and so $p \equiv \pm 1 \pmod{8}$ by the Corollary above. But if all the prime factors of M were congruent to $1 \pmod{8}$, then $M \equiv 1 \pmod{8}$, which is not the case. Therefore, M must have at least one prime factor p with $p \equiv -1 \pmod{8}$ and $p > N$. \square

Lemma 7.15. Let p be an odd prime and $a \in \mathbb{Z}$ and $p \nmid a$. Then,

$$\left(\frac{a}{p}\right) = (-1)^t \quad t = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor$$

Proof. Recall the notation from Gauss' Lemma. Here, $\lambda(aj, p) = aj - pk$ for some $k \in \mathbb{Z}$ such that $0 \leq aj - pk < p$. It follows that $k \leq \frac{aj}{p} < k+1$ and hence $k = \left\lfloor \frac{aj}{p} \right\rfloor$. We therefore deduce that $\lambda(aj, p) = aj - p \left\lfloor \frac{aj}{p} \right\rfloor$. Now we recall r_i and s_i . Then,

$$\begin{aligned} \sum_{i=1}^m r_i + \sum_{i=1} s_i &= \sum_{j=1}^{\frac{p-1}{2}} \lambda(aj, p) \\ &= \sum_{j=1}^{\frac{p-1}{2}} \left(aj - p \left\lfloor \frac{aj}{p} \right\rfloor \right) \end{aligned}$$

Since a and p are odd, then,

$$\sum_{j=1}^{\frac{p-1}{2}} j - \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor \equiv \sum_{i=1}^m r_i + \sum_{i=1} s_i \pmod{2} \quad (*)$$

Now we recall from Gauss' Lemma that,

$$\{r_1, \dots, r_m, (p-s_1), \dots, (p-s_n)\} = \{1, 2, \dots, \frac{p-1}{2}\}$$

Thus,

$$\sum_{i=1}^m r_i + np + \sum_{i=1}^n s_i \equiv \sum_{j=1}^{\frac{p-1}{2}} j \pmod{2}$$

and so we now can say,

$$\sum_{i=1}^m r_i + \sum_{i=1}^n s_i \equiv n + \sum_{j=1}^{\frac{p-1}{2}} j \pmod{2}$$

Then comparing with (*),

$$n \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor \pmod{2}$$

and so the result follows from Gauss' Lemma. \square

8 Law of Quadratic Reciprocity

Here is the statement,

Theorem 8.1 (LQR). If p and q are distinct odd primes, then,

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \\ &= \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases} \end{aligned}$$

Remark. Often forget that p and q are distinct odd primes.

We will prove this later, but it is the most important theorem in the module.

Example. What is $\left(\frac{29}{53}\right)$? In other words, can we solve $x^2 \equiv 29 \pmod{53}$? Use LQR,

$$\begin{aligned} \left(\frac{29}{53}\right) &= \left(\frac{53}{29}\right) \\ &= \left(\frac{24}{29}\right) \\ &= \left(\frac{2}{29}\right)^3 \left(\frac{3}{29}\right) \end{aligned}$$

Now we use LQR and the formula for $\left(\frac{2}{p}\right)$ repeatedly,

$$\begin{aligned} \left(\frac{2}{29}\right) &= -1 && (\text{since } 29 \equiv -3 \pmod{8}) \\ \left(\frac{3}{29}\right) &= \left(\frac{29}{3}\right) \\ &= \left(\frac{2}{3}\right) \\ &= -1 && (\text{since } 3 \equiv 3 \pmod{8}) \end{aligned}$$

Thus, $\left(\frac{29}{53}\right) = (-1)^4 = 1$ and hence $x^2 \equiv 29 \pmod{53}$ is soluble.

We recall Lemma 7.15,

Lemma 8.2 (Lemma 7.15). Let p be an odd prime and $a \in \mathbb{Z}$ with a odd and $p \nmid a$. Then,

$$\left(\frac{a}{p}\right) = (-1)^t \text{ where } t = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor$$

Proof of LQR. Note that the result we want is equivalent to showing that,

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

Hence, by the Lemma, it suffices to show,

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor = \frac{p-1}{2} \frac{q-1}{2}$$

We shall count the points in,

$$R := \{(x, y) \in \mathbb{N} \times \mathbb{N} : 0 < x < \frac{p}{2}, 0 < y < \frac{q}{2}\}$$

in two different ways. Note since p, q are odd, we have

$$\#R = \#\{x : 1 \leq x \leq \frac{p-1}{2}\} \times \#\{y : 1 \leq y \leq \frac{q-1}{2}\} = \frac{p-1}{2} \times \frac{q-1}{2}.$$

Now we find another expression for $\#R$. If a point were on the line $(0, 0)$ to $(\frac{p}{2}, \frac{q}{2})$ we would have $y = \frac{qx}{p}$ and hence $py = qx$. However, then we would have $p \mid qx$ which is impossible by Euclid's Lemma for primes, since $p \nmid q$ and $p \nmid x$ ($0 < x < \frac{p}{2}$). Thus there are no points (x, y) of R on the line from $(0, 0)$ to $(\frac{p}{2}, \frac{q}{2})$.

How many points (x, y) of R are there below the diagonal? For each value of x with $1 \leq x \leq \frac{p-1}{2}$, the pairs (x, y) below the diagonal must satisfy $1 \leq y \leq \frac{qx}{p}$. However, there are $\left\lfloor \frac{qx}{p} \right\rfloor$ such values of y . It follows that the total number of points below the line $y = \frac{qx}{p}$ is,

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor.$$

Similarly, there are

$$\sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor$$

points above the line. It follows that,

$$\#R = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor$$

Comparing the two values for $\#R$ gives the required result. \square

Here is an example,

Example. Determine $\left(\frac{3}{p}\right)$ where $p \geq 5$ is a prime. By LQR we have,

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) (-1)^{\frac{(p-1)(3-1)}{4}} = (-1)^{(p-1)/2} \left(\frac{p}{3}\right).$$

To determine $\left(\frac{p}{3}\right)$ we need to know the value of $p \bmod 3$. To determine $(-1)^{(p-1)/2}$ we need to know the value of $(p-1)/2 \bmod 2$, or equivalently the value of $p \bmod 4$. Thus, since 3 and 4 are coprime, by CRT it suffices to find the value of $p \bmod 12$. We have four cases to consider, namely $p \equiv 1, 5, 7, 11 \bmod 12$. Note that the other cases are excluded because $\varphi(12) = 4$ and p must be coprime to 12 as $p \geq 5$.

1. $p \equiv 1 \bmod 12$. In this case $p \equiv 1 \bmod 3$ so $\left(\frac{p}{3}\right) = 1$. Also $p \equiv 1 \bmod 4$, so $(p-1)/2$ is even. Hence $\left(\frac{3}{p}\right) = 1$.
2. $p \equiv 5 \bmod 12$. In this case $p \equiv 2 \bmod 3$ so

$$\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Also $p \equiv 1 \bmod 4$ so $(p-1)/2$ is even. Hence $\left(\frac{3}{p}\right) = -1$.

3. $p \equiv 7 \pmod{12}$. In this case $p \equiv 1 \pmod{3}$ so $\left(\frac{p}{3}\right) = 1$. Also $p \equiv 3 \pmod{4}$ so $(p-1)/2$ is odd. Hence $\left(\frac{3}{p}\right) = -1$.

4. $p \equiv 11 \pmod{12}$. In this case $p \equiv 2 \pmod{3}$ so $\left(\frac{p}{3}\right) = -1$. Also $p \equiv 3 \pmod{4}$ so $(p-1)/2$ is odd.

We summarise and see,

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \pmod{12} \\ -1 & p \equiv \pm 5 \pmod{12} \end{cases}$$

This doesn't work in general. In general if p is an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$ then we can use LQR and Euler's Criterion to compute $a^{(p-1)/2} \pmod{p}$. (In particular this must be ± 1).

9 Jacobi Symbol

We go right to the definition,

Definition 9.1 (Jacobi Symbol). Let n be an odd positive integer with prime factorisation $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Then for any $a \in \mathbb{Z}$ we define the Jacobi symbol $\left(\frac{a}{n}\right)$ by,

$$\left(\frac{a}{n}\right) = \prod_{i=1}^r \left(\frac{a}{p_i}\right)^{e_i}$$

where the symbols on the right are Legendre symbols. We also define $\left(\frac{a}{1}\right) = 1$.

Now for a property,

Theorem 9.2. Let n, m be odd positive integers and $a, b \in \mathbb{Z}$.

1. $\left(\frac{a}{n}\right) = \pm 1$ if a and n are coprime and $\left(\frac{a}{n}\right) = 0$, otherwise,
2. $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ whenever $a \equiv b \pmod{n}$
3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$ and $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$,
4. $\left(\frac{a^2}{n}\right) = 1$ whenever a and n are coprime.

Proof. These are provably by the definition of the Legendre symbol. □

Remark. Let $n = p_1^{e_1} \dots p_r^{e_r}$ be an odd positive integer. If the congruence

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

has a solution then $\left(\frac{a}{p_i}\right) = 1$ for each i and hence $\left(\frac{a}{n}\right) = 1$. However the converse isn't true since because an even number of factors of -1 could appear in the defining product of $\left(\frac{a}{n}\right)$.

Consider the following example on the previous remark,

Example.

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = (-1)(-1) = 1$$

However, $x^2 \equiv 2 \pmod{15}$ is insoluble, because $x^2 \equiv 2 \pmod{3}$ has no solutions.

The point of Jacobi symbol is **not** to determine solubility of congruences. It is a very useful computational device to calculate the Legendre symbol. We now move forward to prove the following Theorem,

Theorem 9.3. If n is an odd positive integer then,

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & n \equiv 1 \pmod{4} \\ -1 & n \equiv 3 \pmod{4} \end{cases}$$

Proof. Write $n = p_1 p_2 \dots p_r$ where the odd prime factors are not necessarily distinct. Then we have,

$$n = \prod_{i=1}^r (1 + p_i - 1) = 1 + \sum_{i=1}^r (p_i - 1) + \sum_{i \neq j} (p_i - 1)(p_j - 1) + \dots$$

But each $p_i - 1$ is even so each sum after the first is divisible by 4. Hence,

$$n \equiv 1 + \sum_{i=1}^r (p_i - 1) \pmod{4}$$

which gives,

$$\frac{1}{2}(n-1) \equiv \sum_{i=1}^r \frac{1}{2}(p_i-1) \pmod{2}$$

Therefore, the corresponding theorem for Legendre symbols we have,

$$\begin{aligned} \left(\frac{-1}{n}\right) &= \prod_{i=1}^r \left(\frac{-1}{p_i}\right) = \prod_{i=1}^r (-1)^{\frac{p_i-1}{2}} \\ &= (-1)^{\sum_{i=1}^r (p_i-1)/2} = (-1)^{(n-1)/2} \end{aligned}$$

which is the desired result. \square

Now for another Theorem,

Theorem 9.4. If n is an odd positive integer then,

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} +1 & n \equiv \pm 1 \pmod{8} \\ -1 & n \equiv \pm 3 \pmod{8} \end{cases}$$

Proof. Write $n = p_1 p_2 \dots p_r$ where the odd prime factors p_i are not necessarily distinct. Then we have,

$$n^2 = \prod_{i=1}^r (1 + p_i^2 - 1) = 1 + \sum_{i=1}^r (p_i^2 - 1) + \sum_{i \neq j} (p_i^2 - 1)(p_j^2 - 1) + \dots$$

But each p_i is odd, we have $p_i^2 - 1 \equiv 0 \pmod{8}$ so,

$$n^2 \equiv 1 + \sum_{i=1}^r (p_i^2 - 1) \pmod{64}.$$

Hence,

$$\frac{1}{8}(n^2 - 1) \equiv \sum_{i=1}^r \frac{1}{8}(p_i^2 - 1) \pmod{8}$$

This also holds modulo 2, hence the corresponding result for Legendre symbol,

$$\begin{aligned} \left(\frac{2}{n}\right) &= \prod_{i=1}^r \left(\frac{2}{p_i}\right) = \prod_{i=1}^r (-1)^{(p_i^2-1)/8} \\ &= (-1)^{\sum_{i=1}^r \frac{1}{8}(p_i^2-1)} = (-1)^{(n^2-1)/8} \end{aligned}$$

Then the result follows from checking cases. \square

Theorem 9.5 (Reciprocity Law for Jacobi Symbols). Let m and n be coprime odd positive integers. Then,

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4} = \begin{cases} +1 & m \equiv 1 \pmod{4} \text{ or } n \equiv 1 \pmod{4} \\ -1 & m \equiv n \equiv 3 \pmod{4} \end{cases}$$

Proof. Write $n = p_1 p_2 \dots p_r$ where the odd prime factors p_i are not necessarily distinct. Similarly, write $m = q_1 q_2 \dots q_s$ where the odd prime factors q_i are not necessarily distinct. (Note that m and n are coprime so $p_i \neq q_j$ for all i, j). Then,

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = \prod_{i=1}^r \prod_{j=1}^s \left(\frac{p_i}{q_j}\right) \left(\frac{q_j}{p_i}\right) = (-1)^t$$

for some $t \in \mathbb{Z}$. Applying the Quadratic Reciprocity law to the first factor of each term $\left(\frac{p_i}{q_j}\right) \left(\frac{q_j}{p_i}\right)$, we can take

$$t = \sum_{i=1}^r \sum_{j=1}^s \frac{1}{2}(p_i - 1) \frac{1}{2}(q_j - 1) = \sum_{i=1}^r \frac{1}{2}(p_i - 1) \sum_{j=1}^s \frac{1}{2}(q_j - 1).$$

However, the same argument as in the proof of the theorem of $\left(\frac{-1}{n}\right)$ shows that,

$$\frac{1}{2}(n - 1) \equiv \sum_{i=1}^r \frac{1}{2}(p_i - 1) \pmod{2}$$

and the corresponding result holds for $\frac{1}{2}(m - 1)$. Therefore,

$$t \equiv \frac{n-1}{2} \frac{m-1}{2} \pmod{2}$$

which completes the proof. □

Now for an example to see how use Jacobi symbols are in calculating Legendre symbols,

Example. Determine whether 888 is a quadratic residue or nonresidue mod 1999. We have,

$$\left(\frac{888}{1999}\right) = \left(\frac{2}{1999}\right)^3 \left(\frac{111}{1999}\right) = \left(\frac{111}{1999}\right)$$

Since $1999 \equiv -1 \pmod{8}$. To calculate $\left(\frac{111}{1999}\right)$ using Legendre symbols, we should write,

$$\left(\frac{111}{1999}\right) = \left(\frac{3}{1999}\right) \left(\frac{37}{1999}\right)$$

and apply LQR to each factor. However, it is easier to do it with the Jacobi symbol,

$$\left(\frac{111}{1999}\right) = -\left(\frac{1999}{111}\right) = -\left(\frac{1}{111}\right) = -1$$

Therefore 888 is a quadratic residue of 1999.

10 Sums of squares

10.1 Pythagorean Triples

We start with a definition,

Definition 10.1 (Pythagorean Triple). A pythagorean triple (x, y, z) isa triple of positive integers satisfying

$$x^2 + y^2 = z^2$$

If $\gcd(x, y, z) = 1$ then (x, y, z) is called a primitive Pythagorean triple.

Remark. If $g = \gcd(x, y, z)$, then $(x/g, y/g, z/g)$ is also a Pythagorean triple. It follows that if $g > 1$, (x, y, z) can be obtained from the ‘smaller’ primitive Pythagorean triple $(x/g, y/g, z/g)$ by multiplying each entry by g . Thus it is natural to focus on primitive Pythagorean triples.

It will be useful to know the following basic fact,

Theorem 10.2. Let (x, y, z) be a primitive Pythagorean triple. Then $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.

Proof. Suppose $\gcd(x, y) > 1$. Then there must be some p such that $p \mid x$ and $p \mid y$. Then $z^2 = x^2 + y^2 \equiv 0 \pmod{p}$. As $p \mid z^2$ then by Euclid’s Lemma for primes we have $p \mid z$ and so $p \mid \gcd(x, y, z)$, contradicting (x, y, z) being primitive. Thus $\gcd(x, y) = 1$. The proofs for $\gcd(x, z) = 1$ and $\gcd(y, z) = 1$ are similar. \square

Considering things mod 4 we can determine the parity of the numbers in a primitive Pythagorean triple.

Theorem 10.3. If (x, y, z) is a primitive triple, then one of x and y is even and the other odd. (Equivalently $x + y$ is odd). Also z must be odd.

Proof. Note that if x is even, then $x^2 \equiv 0 \pmod{4}$ and if x is odd then $x^2 \equiv 1 \pmod{4}$. If x and y are both odd, then $x^2 \equiv y^2 \equiv 1 \pmod{4}$. Hence $z^2 \equiv x^2 + y^2 \equiv 2 \pmod{4}$, which is impossible. If x and y are both even, then $\gcd(x, y) \geq 2$ contradicting the theorem above. We conclude one of x and y is odd and the other even. In any case, $z \equiv z^2 = x^2 + y^2 \equiv x + y \pmod{2}$, so z is odd. \square

As the roles of x and y in Pythagorean triples are symmetric, it makes little loss in generality in studying only one primitive Pythagorean triple with x odd and y even. Now we can characterise the triples,

Theorem 10.4. Let (x, y, z) be a primitive Pythagorean triple with x odd. Then there are $r, s \in \mathbb{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd, such that,

$$x = r^2 - s^2 \quad y = 2rs \quad z = r^2 + s^2$$

Conversely, if $r, s \in \mathbb{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd, then,

$$(r^2 - s^2, 2rs, r^2 + s^2)$$

is a primitive Pythagorean triple.

Proof. Let (x, y, z) be a primitive Pythagorean triple with x odd. Then y is even and z is odd. Let $a = \frac{1}{2}(z - x)$, $b = \frac{1}{2}(z + x)$ and $c = \frac{y}{2}$. Then $a, b, c \in \mathbb{N}$. Also,

$$ab = \frac{(z - x)(z + x)}{4} = \frac{z^2 - x^2}{4} = \frac{y^2}{4} = c^2$$

Let $g = \gcd(a, b)$, then $g \mid (a + b)$ and $g \mid (b - a)$, that is $g \mid z$ and $g \mid x$. As $\gcd(x, z) = 1$, we have $g = 1$. That is $\gcd(a, b) = 1$.

Let p be a prime factor of a . Then $p \nmid b$, so $v_p(b) = 0$. Hence,

$$v_p(a) = v_p(a) + v_p(b) = v_p(ab) = v_p(c^2) = 2v_p(c)$$

is even. Thus a is a square. Similarly, b is a square. We can now write $a = s^2$ and $b = r^2$ where $r, s \in \mathbb{N}$. Then $\gcd(r, s) \mid a$ and $\gcd(r, s) \mid b$, as a and b are coprime then $\gcd(r, s) = 1$. Now $x = b - a = r^2 - s^2$, therefore $r > s$. Also $z = a + b = r^2 + s^2$. As $c^2 = ab = r^2 s^2$ and so $c = rs$, therefore $y = rs$. Finally, as x is odd,

$$1 \equiv x = b - a = r^2 - s^2 \equiv r^2 + s^2 \equiv r + s \pmod{2}$$

that is, $r + s$ is odd. This proves the first half of the theorem.

We seek to prove the converse. Suppose $r, s \in \mathbb{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd. Set $x = r^2 - s^2$, $y = 2rs$ and $z = r^2 + s^2$. Certainly $y, z \in \mathbb{N}$ and also $x \in \mathbb{N}$ as $r > s > 0$. We plug in,

$$\begin{aligned} x^2 + y^2 &= (r^2 - s^2)^2 + (2rs)^2 \\ &= (r^4 - 2r^2 s^2 + s^4) + 4r^2 s^2 \\ &= r^4 + 2r^2 s^2 + s^4 = z^2 \end{aligned}$$

Hence (x, y, z) is a Pythagorean triple. Certainly y is even, and

$$x = r^2 - s^2 \equiv r - s \equiv r + s \pmod{2}$$

Hence, x is odd. To show (x, y, z) is a primitive Pythagorean triple, we examine $g = \gcd(x, z)$. Since x is odd, g is odd. Also $g \mid (x + z)$ and $g \mid (z - x)$, that is $g \mid 2r^2$ and $g \mid 2s^2$. As r and s are coprime, then $\gcd(2r^2, 2s^2) = 2$ and so $g \mid 2$. As g is odd, then $g = 1$. Therefore (x, y, z) is a primitive Pythagorean triple. \square

Theorem 10.5. There do not exist $x, y, z \in \mathbb{N}$ with,

$$x^4 + y^4 = z^4 \tag{11}$$

Proof. We are going to prove a stronger result. We claim there is no $x, y, u \in \mathbb{N}$ with,

$$x^4 + y^4 = u^2 \tag{12}$$

A natural number solution (x, y, z) to 11 gives one for 12, namely, $(x, y, u) = (x, y, z^2)$. Thus it suffices to show 12 has no solution over \mathbb{N} . We use Fermat's method of descent. Given (x, y, u) of 12 we produce another solution (x', y', u') with $u' < u$. This is a contradiction if we start with a solution of 12 minimising u .

Let (x, y, u) be a solution of 12 over \mathbb{N} with minimum possible u . We claim that $\gcd(x, y) = 1$. If not, $p \mid x$ and $p \mid y$ for some prime p . Then $p^4 \mid (x^4 + y^4)$, that is $p^4 \mid u^2$. Hence $p^2 \mid u$. Then $(x', y', u') = (x/p, y/p, u/p^2)$ is a solution of 12 in \mathbb{N} with $u' < u$. This is a contradiction and so $\gcd(x, y) = 1$. As $\gcd(x, y) = 1$ then $\gcd(x^2, y^2) = 1$, and so (x^2, y^2, u) is a primitive Pythagorean triple by 12. By the symmetry we assume that x^2 is odd and y^2 is even, that is x odd and y even. Hence by the theorem on Pythagorean triples, there are $r, s \in \mathbb{N}$ with $\gcd(r, s) = 1$,

$$x^2 = r^2 - s^2 \quad y^2 = 2rs \quad u = r^2 + s^2$$

Then $x^2 + s^2 = r$, and as $\gcd(r, s) = 1$ then (x, s, r) is a primitive Pythagorean triple. As x is odd, there is some $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$ and,

$$x = a^2 - b^2 \quad s = 2ab \quad r = a^2 + b^2$$

by the Theorem on primitive triples. Then,

$$y^2 = 2rs = 4(a^2 + b^2)ab$$

Equivalently, $(y/2)^2 = ab(a^2 + b^2) = abr$. If p is prime and $p \mid \gcd(a, r)$ then $b^2 = (a^2 + b^2) - a^2 \equiv 0 \pmod{p}$ (as $r = a^2 + b^2$ and so $p \mid b^2$) and so $p \mid b$ by Euclid's Lemma for primes. This is impossible as $\gcd(a, b) = 1$. Thus $\gcd(a, r) = 1$. Similarly, $\gcd(b, r) = 1$. Now abr is a square. If $p \mid a$ then $p \nmid b$ and $p \nmid r$. Thus $v_p(a) = v_p(abr)$ is even and so a is a square. Similarly, b and r are also squares. So we write $a = x'^2$, $b = y'^2$ and $r = u'^2$ where $x', y', u' \in \mathbb{N}$. Then,

$$u'^2 = a^2 + b^2 = x'^4 + y'^4$$

so (x', y', u') is a solution of 12. Also,

$$u' \leq u'^2 = a^2 + b^2 = r \leq r^2 < r^2 + s^2 = u$$

This contradicts the minimality of u in the solution of (x, y, u) of 12. Hence 12 is insoluble over \mathbb{N} and 11 is insoluble over \mathbb{N} . \square

10.2 Sums of Squares

We make the definition,

Definition 10.6 (S_k). For $k \in \mathbb{N}$ we let,

$$S_k = \{a_1^2 + a_2^2 + \cdots + a_k^2 : a_1, \dots, a_k \in \mathbb{Z}\}$$

be the set of k squares. Note we allow zero.

Theorem 10.7. The sets S_2 and S_4 are closed under multiplication. That is,

1. If $m, n \in S_2$, then $mn \in S_2$
2. If $m, n \in S_4$, then $mn \in S_4$.

Proof. Let $m, n \in S_2$. Then $m = a^2 + b^2$ and $n = c^2 + d^2$ for some $a, b, c, d \in \mathbb{Z}$. We have,

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d^2) = |a + bi|^2 |c + di|^2 \\ &= |(a + bi)(c + di)|^2 \\ &= |(ac - bd) + (ad + bc)i|^2 \\ &= (ac - bd)^2 + (ad + bc)^2 \in S_2 \end{aligned}$$

This formula is sometimes known as the two-square formula. Now let $m, n \in S_4$. Then $m = a^2 + b^2 + c^2 + d^2$ and $n = r^2 + s^2 + t^2 + u^2$ for some $a, b, c, d, r, s, t, u \in \mathbb{Z}$. By the four-square formula,

$$\begin{aligned} mn &= (a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + u^2) \\ &= (ar - bs - ct - du)^2 + (as + br + cu - dt)^2 \\ &\quad + (at - bu + cr + ds)^2 + (au + bt - cs + dr)^2 \in S_4. \end{aligned}$$

\square

Remark. We have seen the two-square formula comes from complex numbers. Similarly the four-square formula comes from the theory of quaternions.

10.3 Sums of two squares

We start with a theorem,

Theorem 10.8. Let p be a prime and $p \equiv 3 \pmod{4}$ and let $n \in \mathbb{N}$. If $n \in S_2$ then $v_p(n)$ is even.

Proof. Let p be a prime such that $p \equiv 3 \pmod{4}$. Let $n = a^2 + b^2$ with $a, b \in \mathbb{Z}$ and suppose $p \mid n$. We aim to show that $p \mid a$ and $p \mid b$. Suppose $p \nmid a$. Then there is some $c \in \mathbb{Z}$ with $ac \equiv 1 \pmod{p}$. Then,

$$0 \equiv c^2 n = (ac)^2 + (bc)^2 \equiv 1 + (bc)^2 \pmod{p}$$

This implies that $\left(\frac{-1}{p}\right) = 1$, but we know $\left(\frac{-1}{p}\right) = -1$ when $p \equiv 3 \pmod{4}$. This contradiction proves $p \mid a$. Similarly $p \mid b$. Thus $p \mid (a^2 + b^2) = n$ and so $n/p^2 = (a/p)^2 + (b/p)^2 \in S_2$.

Let $n \in S_2$ and $k = v_p(n)$. We have seen that if $k > 0$ then $k \geq 2$ and $n/p^2 \in S_2$. Note that $v_p(n/p^2) = k - 2$. Similarly if $k - 2 > 0$ then $k - 2 \geq 2$ and $n/p^4 \in S_2$. Iterating the argument, if $k = 2r + 1$ is odd, then $n/p^{2r} \in S_2$ and $v_p(n/p^{2r}) = 1$, which is impossible. So k is even. \square

Remark. If $n \in \mathbb{N}$ we can write $n = rm^2$ where m is the largest square dividing n and r is squarefree, that is either $r = 1$ or r is a product of distinct primes. If any prime factor p of r is congruent to $3 \pmod{4}$ then $v_p(n) = 1 + 2v_p(m)$ is odd and $n \notin S_4$. Hence, if $n \in S_2$, the only possible prime factors of r are $p = 2$ and $p \equiv 1 \pmod{4}$. Obviously $2 = 1^2 + 1^2 \in S_2$. It would be nice if all primes congruent to $1 \pmod{4}$ were also in S_2 . Fortunately, this is the case.

Theorem 10.9. Let p be a prime with $p \equiv 1 \pmod{4}$. Then $p \in S_2$.

Proof. As $p \equiv 1 \pmod{4}$, then we have $\left(\frac{-1}{p}\right) = 1$ and so there exists $u \in \mathbb{Z}$ such that $u^2 \equiv -1 \pmod{p}$. Let,

$$\begin{aligned} A &= \{(m_1, m_2) : m_1, m_2 \in \mathbb{Z}, 0 \leq m_1, m_2 < \sqrt{p}\} \\ &= \{(m_1, m_2) : m_1, m_2 \in \mathbb{Z}, 0 \leq m_1, m_2 \leq \lfloor \sqrt{p} \rfloor\} \end{aligned}$$

Then A has $(1 + \lfloor \sqrt{p} \rfloor)^2$ elements and so $|A| > p$. For $\mathbf{m} = (m_1, m_2) \in \mathbb{R}^2$ define $\phi(\mathbf{m}) = um_1 + m_2$. Then $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}$ is a linear map, and if $\mathbf{m} \in \mathbb{Z}^2$ then $\phi(\mathbf{m}) \in \mathbb{Z}$. As $|A| > p$, the $\phi(\mathbf{m})$ for $\mathbf{m} \in A$ can't all be distinct modulo p . Hence, there are distinct $\mathbf{m}, \mathbf{n} \in A$ with $\phi(\mathbf{m}) \equiv \phi(\mathbf{n}) \pmod{p}$. Let $\mathbf{a} = \mathbf{m} - \mathbf{n}$. Then by linearity, $\phi(\mathbf{a}) = \phi(\mathbf{m}) - \phi(\mathbf{n}) \equiv 0 \pmod{p}$. Write $\mathbf{a} = (a, b)$. Then $\mathbf{a} = m_1 - n_1$ where $0 \leq m_1, n_1 < \sqrt{p}$ so that $|a| < \sqrt{p}$ and $|b| < \sqrt{p}$. Then $a^2 + b^2 < 2p$. As $\mathbf{m} \neq \mathbf{n}$ then $\mathbf{a} \neq (0, 0)$ and so $a^2 + b^2 > 0$. By $0 \equiv \phi(\mathbf{a}) = ua + b \pmod{p}$. Hence $b \equiv -ua \pmod{p}$ and so,

$$a^2 + b^2 \equiv a^2 + (-ua)^2 \equiv a^2(1 + u^2) \equiv 0 \pmod{p}$$

As $a^2 + b^2$ is a multiple of p , and so $0 < a^2 + b^2 < 2p$, then $a^2 + b^2 = p$. We conclude that $p \in S_2$. \square

We now give an alternative constructive proof,

Constructive Proof. As $p \equiv 1 \pmod{4}$ we have $\left(\frac{-1}{p}\right) = 1$ and so there exists $u \in \mathbb{Z}$ such that $u^2 \equiv -1 \pmod{p}$. In other words, there is some $m \in \mathbb{N}$ such that $u^2 + 1 = mp$. Note that we can assume $|u| < \frac{p}{2}$, so $u^2 + 1 < \frac{p^2}{4} + 1 < \frac{p^2}{2}$. Thus $1 \leq m < \frac{p}{2}$.

The idea is as follows. Given a representation $a^2 + b^2 = mp$ with $1 \leq m < p$ use this to find another representation $c^2 + d^2 = m'p$ with $1 \leq m' < m$. Then repeat this until we get $m' = 1$, giving the desired solution. Note that the starting point is $u^2 + 1 = mp$ of the first paragraph.

Suppose $a^2 + b^2 = mp$ for some $m \in \mathbb{N}$ with $1 < m < p$. Then there exist $a', b' \in \mathbb{Z}$ with $a \equiv a' \pmod{m}$, $|a| \leq \frac{m}{2}$ and $b \equiv b' \pmod{m}$ with $|b'| \leq \frac{m}{2}$. Let $c = \frac{aa' + bb'}{m}$ and $d = \frac{ab' - ba'}{m}$. Now,

$$aa' + bb' \equiv a^2 + b^2 \equiv 0 \pmod{m} \text{ and } ab' - ba' \equiv ab - ba \equiv 0 \pmod{m}$$

and so $c, d \in \mathbb{Z}$. Moreover, $(a')^2 + (b')^2 \equiv a^2 + b^2 \equiv 0 \pmod{m}$ and so,

$$\begin{aligned} c^2 + d^2 &= \frac{(aa' + bb')^2 + (ab' - ba')^2}{m^2} \\ &= \frac{(a^2 + b^2)(a'^2 + b'^2)}{m^2} = \frac{p(a'^2 + b'^2)}{m} \end{aligned}$$

is in fact an integer and a multiple of p . In other words, $c^2 + d^2 = m'p$ for some $m' \in \mathbb{Z}$. Now $a'^2 \leq \frac{m^2}{4}$ and $b'^2 \leq \frac{m^2}{4}$. So $a'^2 + b'^2 \leq \frac{m^2}{2}$. Thus,

$$0 \leq m' = \frac{a'^2 + b'^2}{m} \leq \frac{m}{2} < m < p$$

Suppose $m' = 0$ for contradiction. Then $a' = b' = 0$ and so $m \mid a$ and $m \mid b$. Thus $m^2 \mid (a^2 + b^2)$ and so $m \mid p$. But p is prime and $1 < m < p$ so $m \nmid p$ - contradiction. Thus $m \neq 0$ and therefore $1 < m' < m$. \square

recall the following,

Proposition 10.10. Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ and suppose that $\gcd(a, n) = 1$. For $r, s \in \mathbb{Z}$ we have $a^r \equiv a^s \pmod{n}$ if and only if $r \equiv s \pmod{\text{ord}_n(a)}$.

Now for a remark,

Remark. In order to create an algorithm to find an expression $p = a^2 + b^2$ when $p \equiv 1 \pmod{4}$ is prime we need to solve the equation $u^2 \equiv -1 \pmod{p}$. (This is the hard part). We write $p = 4k + 1$ where $k \in \mathbb{N}$. Let g be a primitive root mod p . Then $\text{ord}_p(g) = \varphi(p) = p - 1 = 4k$ and $g^0, g^1, g^2, \dots, g^{4k-1}$ are congruent to $1, 2, \dots, p - 1$ in some order. Now $x = g^{2k}$ is a solution to $x^2 \equiv 1 \pmod{p}$ and $x \not\equiv 1 \pmod{p}$, so $g^{2k} \equiv -1 \pmod{p}$ since p is an odd prime. If $t \equiv g^r \pmod{p}$ where r is odd then t^k is a solution of $x^2 \equiv -1 \pmod{p}$ since $2kr \equiv 2k \pmod{4k}$ (this is true because of the above proposition and the fact that $\text{ord}_p(g) = 4k$). We now pick $t \in \{1, \dots, p - 1\}$ at random, there is a 50% chance that $\tau \equiv g^r \pmod{p}$ with r odd. (Actually, its obvious that $t = 1$ won't work so don't pick this). Given such a t we set $u = t^k$.

Example. Let $p = 1997$. Note $p \equiv 1 \pmod{4}$. Writing $p = 4k + 1$ we see that $k = 499$. Try $t = 2$. Then $t^k \equiv 2^{499} \equiv 1585 \equiv -412 \pmod{1997}$ (here we use modular exponentiation algorithm). Note that we choose -412 because $|-412| < 1997/2$. Check that $(-412)^2 \equiv -1 \pmod{1997}$ (it does). Set $a = 412$ and $b = 1$, then $a^2 + b^2 = 169745 = 85 \times 1995$, so $m = 85$.

Now $412 \equiv -13 \pmod{85}$. So $a' = -13$ and $b' = 1$. Set,

$$c = \frac{aa' + bb'}{m} = -63 \quad d = \frac{ab' - ba'}{m} = 5$$

Now we have, $63^2 + 5^2 = 3994 = 2 \times 1997$. Now let $a = 63$, $b = 5$ and $m = 2$. Then $63 \equiv 1 \pmod{2}$ and $5 \equiv 1 \pmod{2}$. So we take $a' = b' = 1$,

$$c = \frac{aa' + bb'}{m} = 34 \quad d = \frac{ab' - ba'}{m} = 29$$

Now we have $34^2 + 29^2 = 1997$, so we are done.

We recall the previous two theorems. We will now use those two theorems to characterise the elements of S_2 .

Theorem 10.11 (Two Square Theorem). Let $n \in \mathbb{N}$. Then $n \in S_2$ if and only if $v_p(n)$ is even whenever p is a prime congruent to $3 \pmod{4}$.

Proof. If $n \in S_2$, p is prime and $p \equiv 3 \pmod{4}$ then $v_p(n)$ is even by the first theorem above. If $v_p(n)$ is even whenever $p \equiv 3 \pmod{4}$ a prime then $n = rm^2$ where each prime factor p of r is either 2 or $1 \pmod{4}$. By the second theorem all primes p with $p \equiv 1 \pmod{4}$ are in S_2 . Moreover, $2 = 1^2 + 1^2 \in S_2$. Hence $r \in S_2$ since S_2 is closed under multiplication. Hence $r = a^2 + b^2$ where $a, b \in \mathbb{Z}$ and so,

$$n = rm^2 = (am)^2 + (bm)^2 \in S_2$$

□

We now prove,

Theorem 10.12. Let p be a prime. If $p = a^2 + b^2 = c^2 + d^2$ with $a, b, c, d \in \mathbb{N}$ then either $a = c$ and $b = d$ or $a = d$ and $b = c$.

Proof. Consider,

$$\begin{aligned} (ac + bd)(ad + bc) &= (a^2 + b^2)cd + ab(c^2 + d^2) \\ &= p(ab + cd) \end{aligned}$$

As $p \equiv (ac + bc)(ad + bc)$ then by Euclid's lemma for primes either $p \equiv (ac + bd)$ or $p \equiv (ad + bc)$. Assume for former, the later can be proved by relabelling. Now $ac + bd > 0$ so that $ac + bc \geq p$. Also,

$$\begin{aligned} (ac + bd)^2 + (ad - bc)^2 &= (a^2 + b^2)(c^2 + d^2) \\ &= p^2 \end{aligned}$$

As $ac + bd \geq p$ the only way that this is possible is if $ac + bd = p$ and $ad - bc = 0$. Then $ac^2 + bcd = cp$ and $ad^2 + bcd = 0$, so adding gives $a(c^2 + d^2) = cp$, that is $ap = cp$ and so $a = c$. Then $c^2 + bd = p = c^2 + d^2$, that is $bd = d^2$ and so $b = d$. □

Example. Find two ‘essentially’ different ways of writing $629 = 17 \times 37$ as the sum of two squares. First note that 17 and 37 are both primes congruent $1 \pmod{4}$, and thus can be written as the sum of two squares in a unique way. In fact, $17 = 4^2 + 1^2$ and $37 = 6^2 + 1^2$.

$$629 = |4 + i|^2 |6 + i|^2 = |(4 + i)(6 + i)|^2 = |23 + 10i|^2 = 23^2 + 10^2$$

$$629 = |4 + i|^2 |6 - i|^2 = |(4 + i)(6 - i)|^2 = |25 + 2i|^2 = 25^2 + 2^2$$

10.4 Sums of Four Squares

We wish to prove a theorem of Lagrange to the effect that all natural numbers are the sums of four squares. It is crucial to establish this for primes.

Theorem 10.13. Let p be a prime. Then $p \in S_4$.

Proof. If $p \equiv 1 \pmod{4}$, then there are $a, b \in \mathbb{Z}$ with $p = a^2 + b^2 + 0^2 + 0^2$ and so $p \in S_4$. Also,

$$2 = 1^2 + 1^2 + 0^2 + 0^2 \quad 3 = 1^2 + 1^2 + 1^2 + 0^2$$

We may assume that $p > 3$ and that $p \equiv 3 \pmod{4}$. As a consequence $\left(\frac{-1}{p}\right) = -1$. Let w be the smallest positive integer with $\left(\frac{w}{p}\right) = -1$. (Note this forces $w \geq 2$). Then,

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

Hence there are $u, v \in \mathbb{Z}$ with,

$$w^2 - 1 \equiv u^2 \pmod{p} \quad -w^2 \equiv v^2 \pmod{p}$$

Then $1 + u^2 + v^2 \equiv 1 + (w - 1) - w \equiv 0 \pmod{p}$. Let,

$$\begin{aligned} B &= \{(m_1, m_2, m_3, m_4) : m_1, \dots, m_4 \in \mathbb{Z}, 0 \leq m_1, \dots, m_4 < \sqrt{p}\} \\ &= \{(m_1, m_2, m_3, m_4) : m_1, \dots, m_4 \in \mathbb{Z}, 0 \leq m_1, \dots, m_4 \leq \lfloor \sqrt{p} \rfloor\} \end{aligned}$$

Then B has $(1 + \lfloor \sqrt{p} \rfloor)$ elements. Hence $|B| > p^2$. We now define for $\mathbf{m} = (m_1, m_2, m_3, m_4)$,

$$\psi(\mathbf{m}) = (um_1 + vm_2 + m_3, -vm_1 + um_2 + m_4)$$

Then $\psi : \mathbb{R}^4 \rightarrow \mathbb{R}^2$ is a linear map. If $\mathbf{m} \in \mathbb{Z}^4$ then $\psi(\mathbf{m}) \in \mathbb{Z}^2$. Write $(a, b) \equiv (a', b') \pmod{p}$ if $a \equiv a' \pmod{p}$ and $b \equiv b' \pmod{p}$. If we have a list of $(a_1, b_1), \dots, (a_N, b_N)$ of vectors in \mathbb{Z}^2 with $N > p^2$, then there must be some distinct i and j with $(a_i, b_i) \equiv (a_j, b_j) \pmod{p}$. This happens for the vectors $\psi(\mathbf{m})$ with $\mathbf{m} \in B$ as $|B| > p^2$. Thus there are distinct $\mathbf{m}, \mathbf{n} \in B$ with $\psi(\mathbf{m}) \equiv \psi(\mathbf{n}) \pmod{p}$. Let $\mathbf{a} = \mathbf{m} - \mathbf{n}$. Then $\psi(\mathbf{a}) = \psi(\mathbf{m}) - \psi(\mathbf{n}) \equiv (0, 0) \pmod{p}$. Write $\mathbf{a} = (a, b, c, d)$. Then $a = m_1 - n_1$ where $0 \leq m_1, n_1 < \sqrt{p}$ so that $|a| < \sqrt{p}$. Similarly $|b|, |c|, |d| < \sqrt{p}$. Then $a^2 + b^2 + c^2 + d^2 < 4p$. As $\mathbf{m} \neq \mathbf{n}$ then $\mathbf{a} \neq (0, 0, 0, 0)$ and so $a^2 + b^2 + c^2 + d^2 > 0$. Now $(0, 0) \equiv \psi(\mathbf{a}) = (ua + vb + c, -va + ub + d) \pmod{p}$. Hence $c \equiv -ua - vb \pmod{p}$ and $d \equiv va - ub \pmod{p}$. Then,

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ua + vb)^2 + (va - ub)^2 \\ &\equiv (1 + u^2 + v^2)(a^2 + b^2) \equiv 0 \pmod{p} \end{aligned}$$

This holds because we have already shown that $1 + u^2 + v^2 \equiv 0 \pmod{p}$. As $a^2 + b^2 + c^2 + d^2$ is a multiple of p and $0 < a^2 + b^2 + c^2 + d^2 < 4p$. When $a^2 + b^2 + c^2 + d^2 = p$ then $p \in S_4$. Alas, we need to consider the **other** cases where,

$$a^2 + b^2 + c^2 + d^2 = 2p \text{ or } 3p.$$

Suppose $a^2 + b^2 + c^2 + d^2 = 3p$. Then $a^2 + b^2 + c^2 + d^2 \equiv 3 \pmod{4}$ so that two of a, b, c, d are odd and the other two even. Without loss of generality, suppose a, b are odd and c, d are even. Then $\frac{1}{2}(a + b)$, $\frac{1}{2}(a - b)$, $\frac{1}{2}(c + d)$ and $\frac{1}{2}(c - d)$ are all integers and a simple computation gives,

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{a^2 + b^2 + c^2 + d^2}{2} = p$$

so that $p \in S_4$.

Suppose $a^2 + b^2 + c^2 + d^2 = 3p$, then $a^2 + b^2 + c^2 + d^2$ is a multiple of 3 but not 9. As $a^2 \equiv 0$ or $1 \pmod{3}$ then either exactly one or all four of a, b, c, d are multiples of three. The later case isn't possible as then it would be a multiple of 9. So without loss of generality $3 \nmid a$ and $b, c, d \equiv \pm 1 \pmod{3}$. By replacing b by $-b$, etc. as necessary we may assume that $b \equiv c \equiv d \equiv 1 \pmod{3}$. Then $\frac{1}{3}(b + c + d)$, $\frac{1}{3}(a + b - c)$, $\frac{1}{3}(a + c - d)$, $\frac{1}{3}(a + d - b)$ are all integers and a simple computation gives,

$$\left(\frac{b+c+d}{3}\right)^2 + \left(\frac{a+b-c}{3}\right)^2 + \left(\frac{a+c-d}{3}\right)^2 + \left(\frac{a+d-b}{3}\right)^2 = \frac{a^2 + b^2 + c^2 + d^2}{3} = p$$

so that $p \in S_4$. □

Now we can prove,

Theorem 10.14 (Lagrange's four-square theorem). If $n \in \mathbb{N}$ then $n \in S_4$

Proof. Either $n = 1 = 1^2 + 0^2 + 0^2 + 0^2 \in S_4$ or n is a product of primes. By the above theorem, each prime of n lies in S_4 . Then since S_4 is closed under multiplication, we have $n \in S_4$. □