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

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 $S := \{a - xb : x \in \mathbb{Z} \quad \text{and } a - xb \geq 0\}$. We know $S \neq 0$ since,

- if $a \geq 0$, then choose $m = 0$, them $a - mb = a \geq 0$
- 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 form $a = a + qb + r = q'b + r'$ 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 wasnt 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,

(i) $d \mid a$ and $d \mid b$

(ii) and if $e \in \mathbb{Z}$, $e \mid a$ and $e \mid b$, then $e \mid d$

(iii) $d = ax + by$

[1]You 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 $0 \leq q < d$. 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 $r < d$, contradiciting 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. ☐

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.

(i) $d \mid a$ and $d \mid b$

(ii) 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). ☐

Definition 1.6 (Greatest Common Divisor)**.** Let $a, b \in \mathbb{Z}$. Them 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,

(i) $\gcd(a, b) = \gcd(b, a)$

(ii) $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$

(iii) $\gcd(ac, bc) = |c| \gcd(a, b)$

(iv) $\gcd(1, a) = \gcd(a, 1) = a$

(v) $\gcd(0, a) = \gcd(a, 0) = |a|$

(vi) $c \mid \gcd(a, b)$ if and only if $c \mid a$ and $c \mid b$

(vii) $\gcd(a + cb, b) = \gcd(a, b)$

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 my (vi) we have $e = f$ as $f, e \geq 0$. ☐

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. ☐

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, $c = qd = aqx' + bqy'$ and so $x = qx'$ and $y = qy'$ gives a suitable solution. ☐

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,

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

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,

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

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 sequnces 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 it's 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.

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

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 $p \mid n$. □

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. □

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. □

2.1 Fundemental Theorem of Arithmetic

Lemma 2.6. Let $n \in Z$, 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, $d = 1$. □

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, $p \mid b$. □

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 $p^{k+1} \mid n$. 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 $v_p(mn) = v_p(m) + v_p(n)$. □

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

(i) (Existence) The number n can be written as a product of primes.

(ii) (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,
$$p_1 \leq p_2 \leq \dots \leq p_r \qquad \text{and} \qquad q_1 \leq q_2 \leq \dots \leq q_s$$
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. □

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 □

2.2 Congruences

Definition 2.12. Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}_1$. We write $a \equiv b \mod n$, and say 'a is congruent to b mod 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, $a \equiv 0 \mod n$ if and only if $m \mid a$

Example. Here are some examples:

- $4 \equiv 30 \mod 13$ since $13 \mid (4-30) = -26$
- $17 \not\equiv -17 \mod 4$ since $17 - (-17) = 34$ but $4 \nmid 34$.
- n is even if and only if $n \equiv 0 \mod 2$
- n is odd if and only if $n \equiv 1 \mod 2$
- $a \equiv b \mod 1$ 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,

(i) Reflexive: $\forall\, a \in \mathbb{Z}, a \equiv a \mod n$

(ii) Symmetric: $\forall\, a, b \in \mathbb{Z}$, $a \equiv b \mod n \implies b \equiv a \mod n$

(iii) Transitive: $\forall\, a, b \in \mathbb{Z}$, $a \equiv b \mod n$ and $b \equiv c \mod n \implies a \equiv c \mod n$.

Proof. The proof follows from,

(i) $n \mid 0$.

(ii) If $n \mid (a-b)$ then $n \mid (b-a)$

(iii) 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 $a \equiv \alpha \mod n$ and $b \equiv \beta \mod n$. Then,

(i) $a + b \equiv \alpha + \beta \mod n$

(ii) $a - b \equiv \alpha - \beta \mod n$

(iii) $ab \equiv \alpha\beta \mod n$

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

Proof. Check that $ab \equiv \alpha\beta \mod n$. Since, $a \equiv \alpha \mod n$ 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, $ab \equiv \alpha\beta \mod n$, as required. □

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

$$n = \sum_{i=0}^{k} a_i \times 10^i \qquad 0 \le a_i \le 9$$

Then, define $f(x)$ by,

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

Then, since $10 \equiv -1 \mod 11$, we see that $n = f(10) \equiv f(-1) \mod 11$, 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 $x^2 - 3y^2 \equiv x^2 \mod 3$. Now, $x \equiv 0, 1, 2 \mod 3$, so $x^2 \equiv 0, 1, 4 \mod 3 \equiv 0, 1 \mod 3$. Hence, $x^2 - 3y^2 \equiv x^2 \not\equiv 2 \mod 3$ and so $x^2 - 3y^2 \neq 2$.

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

We are going to prove the following theorem,

Theorem 2.15. There are infinitely many primes p with $p \equiv 3 \mod 4$

Proof. Suppose that p is a prime. Then $p \equiv 0, 1, 2, 3 \mod 4$, but $p \not\equiv 0 \mod 4$ because $4 \nmid p$. If $p \equiv 2 \mod 4$ 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,

(i) $p = 2$

(ii) $p \equiv 1 \mod 4$

(iii) $p \equiv 3 \mod 4$

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 $M = p_1 \ldots p_k$. If $p \leq N$, then $M \equiv -1 \mod p$ 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 $p_j \equiv 1, 3 \mod 4$. If $p_j \equiv 3 \mod 4$ for any j then we are done. If this is not the case, then $p_j \equiv 1 \mod 4$ for all j, and so, $M \equiv 1 \times 1 \times \cdots \times 1 \mod 4 \equiv 1 \mod 4$; but by definition of M we have $M \equiv -1 \equiv 3 \mod 4$ - contradiction! □

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

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

(i) If $a \mid b \mod n$ and $d \mid n$ them $a \mid b \mod d$

(ii) Suppose $s \neq 0$. Then $a \equiv b \mod n$ if and only if $as \equiv bs \mod ns$

Proof. (i) follows from transitivity of divisibility;
(ii) follows from multiplication and cancellation properties. □

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 $ac \mid bc \mod n \iff a \equiv b \mod \frac{n}{d}$. In particular, if n and c are coprime, then $ac \equiv bc \mod n \iff a \equiv b \mod n$.

Proof. Since, $d = \gcd(c, n)$, we may write $n = dn'$ and $c = dc'$ where $n', c' \in \mathbb{Z}$. Suppose $ac \equiv bc \mod n$. 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, $a \equiv b \mod n'$.
Suppose conversely $a \equiv b \mod n'$ 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 $ac \equiv bc \mod n$. □

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 $a \equiv b \mod m$ and $a \mid b \mod n$ then $a \equiv b \mod mn$.

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 $a \equiv b \mod n$ 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 $a - b = 0$. □

As $\mod n$ 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 $a \mod n$. Thus,

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

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,

$$[0]_2 = \{x \in \mathbb{Z} : x \equiv 0 \mod 2\}$$
$$[1]_2 = \{x \in \mathbb{Z} : x \equiv 1 \mod 2\}$$

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

Proof. The integers $0, 1, \ldots, n-1$ are incongruent $\mod n$ 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 $x \equiv r \mod n$ and hence, $x \in [r]_n$. □

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 $S = \{0, 1, \ldots, n-1\}$ is a complete residue system. Note, that if S is any complete residue system, then $|S| = n$. Any set of integers that are incongruent $\mod n$ are a complete residue system $\mod n$.

Example. The following are complete residue systems,

$$\{1, 2, \ldots, n\}$$
$$\{1, n+2, 2n+3, 3n+4, \ldots, n^2\}$$
$$\{x \in \mathbb{Z} : -\frac{n}{2} < x \leq \frac{n}{2}\}$$

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

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

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

3.2 Linear Congruences

The most basic congruences are linear congruence, for example,

$$ax \equiv b \mod n$$

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,

$$ax \equiv b \mod n$$

has exactly one solution.

Proof. We need only to test $1, 2, \ldots, n$ since they constitute a complete residue system. Therefore, we consider the products, $a, 2a, \ldots, na$. 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 $b \mod n$. □

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

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

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

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 □

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

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

has exactly d solutions modulo n. These are,

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

where t is the unique solution $\mod n'$ to,

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

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, $\mod n'$ 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 $\mod n$ since the relationships

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

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

$$kn' \equiv rn' \mod n \qquad \text{and so } y \equiv t + rn' \mod n$$

Therefore y is congruent $\mod n$ to one of these numbers in (3). □

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

$$ax \equiv b \mod n \tag{5}$$

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

$$ax' + ny' = d \tag{6}$$

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

$$a'x' + n'y' = 1 \tag{7}$$

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

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

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

4.1 $\mathbb{Z}/n\mathbb{Z}$ and it's 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 whth $0 = [0]_n$ 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 $ax \equiv 1\ modn$ is called the multiplicative inverse of $a \mod n$ and is denoted $[a]_n^{-1}$ or $a^{-1} \mod n$

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,

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

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

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

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

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

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

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

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

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

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, $\varphi(p) = \#\{1, 2, \ldots, p-1\} = p - 1$.

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 $m, n \in N$ 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,

$$a \equiv b \mod m \qquad \text{and} \qquad a \equiv c \mod n$$

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

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

Hence $ar \equiv bs \equiv 1 \mod n$ and $ar \equiv ct \equiv 1 \mod n$ and so $x = ar$ is the solution to,

$$x \equiv 1 \mod n \qquad \text{and} \qquad x \equiv 1 \mod n$$

By the Chinese Remainder Theorem $ar \equiv 1 \mod mn$. 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. $\varphi(m)\varphi(n)$. □

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,

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

□

Proposition 4.10. Let $n \in \mathbb{N}$ such that $n \geq 2$. By FTA, we may write $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_r^{e_r}$ 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,

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

□

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,

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

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

□

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 $\sum_{e|n} \varphi\left(e\right)$ □

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 $a^r \equiv 1 \mod n$ if and only if $\gcd(a, n) = 1$.

Proof. Suppose there exists $r \in \mathbb{N}$ such that $a^r \equiv 1 \mod n$. Then a^{r-1} is a solution to $ax \equiv 1 \mod n$ 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 $a^k \mod n$ so there exists $i, j \in \mathbb{N}$ with $i < j$ such that $a^i \equiv a^j \mod n$. Since $\gcd(a, n) = 1$ we may apply the cancellation law for congruences i times obtain $a^{j-i} \equiv 1 \mod n$/ Thus take $r = j - i$. □

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 $a^d \equiv 1 \mod n$ is called the order of $a \mod n$ and is written $\mathrm{ord}_n(a)$

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 $a^r \equiv a^s \mod n$ if and only if $r \equiv s \mod \mathrm{ord}_n(a)$

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

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

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

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

and so $a^u \equiv 1 \mod n$. However, $0 \le u < k$ and k is the least positive integer such this is true. Hence $u = 0$. Therfore, $k \mid (r - s)$, ie. $r \equiv s \mod k$. □

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

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

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

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

5.1 Reduced Residue Systems

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

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

Remark. If R is a reduced residue system $\mod n$ 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 $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ is a reduced residue system $\mod n$ and $\gcd(k, n) = 1$ then $\{ka_1, ka_2, \ldots, ka_{\varphi(n)}\}$ is also a reduced redidue system $\mod n$.

Proof. If $ka_i \equiv ka_j \mod n$ then by the cancellation law for congruences $a_i \equiv a_j \mod n$ since $\gcd(k, n) = 1$. Therefore, no two elements in $\{ka_1, ka_2, \ldots, ka_{\varphi(n)}\}$ are congruent $\mod n$. 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 □

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 $a^{\phi(n)} \equiv 1 \mod n$.

Proof. Let $\{b_1, \ldots, n_{\varphi(n)}\}$ be a reduced residue system $\mod n$. Then since $\gcd(a, n) = 1$, then $\{ab_1, ab_2, \ldots, ab_{\varphi(n)}\}$ 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,

$$b_1 b_2 \ldots b_{\varphi(n)} \equiv a^{\varphi(n)} b_1 b_2 \ldots b_{\varphi(n)} \mod n$$

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

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

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

Example. If we consider $\varphi(12) = 4$. 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 $\varphi(12)$.

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

Proof. This follows immediately as $\varphi(p) = p - 1$. □

Example. We know that $\text{ord}_{19}(3) = 18 = \varphi(19)$ 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 $a^p \equiv a \mod p$.

Proof. If $p \nmid a$, this follows from the earlier corollary. If $p \mid a$, then a^p and a are congruent to $0 \mod p$. □

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 $\text{ord}_n(a) \mid \varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ 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 $b^e \mod m$ efficiently. We can write e in binary, ie. $e = \sum_{i=0}^k a_i 2^i$ where $a_i \in \{0, 1\}$ for $0 \le i \le k$. Then we observe,

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

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,

(i) If e is odd, the replace x by bx and reduce this $\mod m$. (If e is even x is not altered).

(ii) Replace b by b^2 and reduce $\mod m$

(iii) 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 $x \equiv b^e \mod m$.

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

step	$x \mod m$	$b \mod m$	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

$3^{499} \mod 997$. 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 (Leggranges 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 $p \not| a_d$. Then $f(x) \equiv 0 \mod p$ has at most d solutions $\mod p$.

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,

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

since $a_1 \not\equiv 0 \mod p$, 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 $f(x) \equiv 0 \mod p$ has $d + 1$ incongruent solutions $\mod p$ say $x_0, x_1, \ldots x_d$ where $f(x_k) \equiv 0 \mod p$. Recall we have for $r \in \mathbb{N}$,

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

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,

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

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

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

Proof. Lagranges Polynomial Theorem says that $a^2 \equiv 1 \mod p$ has at most two solutions and these are $a \equiv \pm 1 \mod p$ 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,

$$x^2 \equiv 1 \mod pq$$

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

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

Thus there are four solutions $\mod pq$. Hence,

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

and

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

and so there remains two pairs of congruences,

$$\begin{cases} x \equiv 1 \mod p \\ x \equiv -1 \mod q \end{cases} \qquad \text{and} \qquad \begin{cases} x \equiv -1 \mod p \\ x \equiv 1 \mod q \end{cases}$$

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,

$$f(x) \equiv 0 \mod n$$

this can be reduced to solvbing a system of congruences,

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

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 $\mod p_i$.

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 it's formal derivative. If $a \in \mathbb{Z}$ satisfies,

$$f(x) \equiv 0 \mod p, \qquad f'(a) \not\equiv 0 \mod p$$

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

$$f(a_n) \equiv 0 \mod p \qquad \text{and } a_n \equiv a \mod p$$

Moreover, a_n is unique modulo p^n.

If we take $f(x) = x^2 + 1$ ($x^2 \equiv -1 \mod 5^4$) and $a = 2$, we can apply the above lemma. Let $a_2 = 2 + 5t_1$, we now plug this into $f(a_2) \equiv 0 \mod 5^2$ and get that $t_1 \equiv 1 \mod 5$, hence $a_2 = 7$. Now we could let $a_3 = 7 + 5^2 t_2$ and then similarly to before solve for t_2 using $f(a_3) \equiv 0 \mod 5^3$. However, we can shortcut by writing $a_4 = 7 + 5^2 t_3$, this is because we know $a_4 \equiv a_2 \mod 5^2$. Then we get that, $t_3 \equiv 7 \mod 5^2$. 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 satisfies, 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 it's 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 ientity of the Lemma is similar to Taylors 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 thoerem. 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. □

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 $\mod p^n$. The $n = 1$ case is trivial using $a_1 = a$. We now suppose the inductive hypothesys 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,

$$\begin{aligned} f(a_k + p^k t_k) &= f(a_k) + f'(a_k)p^k t_k + z_k p^{2k} t^2 \\ &\equiv f(a_k) + f'(a_k)p^k t_k \mod p^{k+1} \end{aligned}$$

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 $f'(a_n)p^k t_k$ the factors $f'(a_k)$ and t_k only matter $\mod p$ since it already contains a factor of p^k and the modulus is p^{k+1}. Thus recalling that $a_k \equiv a \mod p$ we have $f'(a)p^k t_k \equiv f'(a_k)p^k t_k \mod p^{k+1}$.

Therefore we have,

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

Where we already know $-\frac{f(a_k)}{p^k} \in \mathbb{Z}$ by the induction hypothesis. But $f'(a) \not\equiv 0 \mod p$ and so $\gcd(f'(a), p) = 1$ and thus by the theorem on linear congruences with exactly one solution, the last congruence ($\mod p$) has a solution t_k, which is unique $\mod p$. We set $a_{k+1} = a_k + p^k t_k$. Then we have $f(a_{k+1}) \equiv 0 \mod p^{k+1}$ and $a_{k+1} \equiv a_k \mod p^k$, so in particular $a_{k+1} \equiv a \mod p$.
It remains to show uniqueness. Suppose $\exists\, b_{k+1} \in \mathbb{Z}$ with $f(b_{k+1}) \equiv 0 \mod p^{k+1}$ and $b_{k+1} \equiv a \mod p$ an so $f(b_{k+1}) \equiv 0 \mod p^k$. Then by the induction hympothesis we have $b_{k+1} \equiv a_k \mod p^k$. 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 $s_k \equiv t_k \mod p$ and thus, $a_{k+1} \equiv b_{k+1} \mod p^{k+1}$ as desired. ☐

Remark. An adaptation of the above proof can show in principle one can always lift from a solution from p^k to a solution $\mod p^{2k}$.
Moreover, for $m > n > 1$ we always have $a_m \equiv a_n \mod p^n$.

6.2 Primitive Roots

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

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

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,

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

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

Proof. Let $f = \mathrm{ord}_n(a)$. The integer $\mathrm{ord}_n(a^k)$ is the least $d \in \mathbb{N}$ such that $a^{dk} \equiv 1 \mod n$. By an earlier corollary, this is also the least d such that $dk \equiv 0 \mod f$. But, by the cancelation law for congruence we can say $d \equiv 0 \mod \frac{f}{h}$ where $h = \gcd(f, k)$. But it is clear the least positive integer that is a solution i just $d = \frac{f}{h}$ and so $\mathrm{ord}_n(a^k) = \frac{f}{h}$ 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 mod p such that $\mathrm{ord}_p(a) = d$. In particular there are $\phi(p-1)$ primitive roots $\mod p$.

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

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

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

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

and we also know that,

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

Therfore, we can show that if $\psi(d) \leq phi(d)$ 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 $\psi(d) \leq \phi(d)$ and we are done. Hence, $\psi(d) \geq 1$. Then $A(d) \neq \varnothing$ and so $a \in A(d)$ for some a. Hence $\mathrm{ord}_p(a) = d$ and so $a^d \equiv 1 \mod p$. Then $(a^i)^d \equiv 1 \mod p$ for all $i \in \mathbb{Z}$.
In particular,

$$a, \, a^2, \, \ldots, \, a^d$$

are all solutions to $x^d - 1 \equiv 0 \mod p$. By an earlier corollary we have that all the above numbers are incongruent $\mod p$ and by Lagranges polynomial congruence theorem, then the congrucence 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 $a^k \mod p$ for some $k = 1, \ldots, d$. By Lemma 6.4, $\mathrm{ord}_p(a^k) = d$ 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 mod 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 $a \equiv g^k \mod p$.

Proof. The existence of primitive roots follow by the thoerem as $\phi(p-1) \geq 1$. By definition, $\mathrm{ord}_p(g) = p-1$ and $1, \, g, \, g^2, \, \ldots, \, g^{p-2}$ 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 $\mod n$ if and only if

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

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

Proof. If $a^{\frac{\phi(n)}{q}} \equiv 1 \mod n$, then $\mathrm{ord}_n(a) \leq \frac{\varphi(n)}{q} < \phi(n)$ and so cannot be a primitive root modulo n.
Suppose conversely that $a^{\frac{\phi(n)}{q}} \not\equiv 1 \mod n$ for every prime $q \mid \phi(n)$. Consider the prime factorisation of $q = \prod_i p_i^{r_i}$. Let $m = \mathrm{ord}_n(a)$, then $m \mid \phi(n)$ and so $m = q_1^{t_1} \ldots q_s^{t_s}$ where $0 \leq t_i \leq r_i$. Suppose that $m < \phi(n)$. Then $\exists\, j, t_j < r_j$, hence $m \mid q_1^{r_1} \ldots q_j^{t_j} \ldots q_s^{r_s} = (\phi(n)/q_j)$. But $a^m \equiv 1 \mod n$ and so $a^{\frac{\phi(n)}{q_j}} \equiv 1 \mod n$ - 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 $g^{p-1} \not\equiv 1 \mod p^2$.

Proof. Not examinable. See Apostal Introduction to ANT, Chp 10. ☐

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 Apostal Introduction to ANT, Chp 10. ☐

6.3 Wilson's Theorem

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

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 $(n-1)! \equiv -1 \mod n$, then $n \mid ((n-1)!+1)$ and so $d \mid ((n-1)!+1)$. Hence, $d \mid 1 = ((n-1)!+1) - (n-1)!$ - Contradiction. Hence, $(n-1)! \not\equiv -1 \mod n$.

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

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

we pair off each term except 1 and $p-1$. Hence, $(p-1)! \equiv 1 \times (p-1) \equiv -1 \mod p$. ☐

We now consider an alternative proof using primitive roots.

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

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

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

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

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

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

☐

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,

$$x^2 \equiv a \mod p$$

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

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

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

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

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 $x^2 \equiv a \mod p$ 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 contaning,

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

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

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 $x^2 \equiv a \mod p$ has precisely $\left(\frac{a}{p}\right) + 1$ distinct solutions mod p

Remark. We always have $\left(\frac{1}{p}\right) = 1$. Moveover, if $a, b \in \mathbb{Z}$ such that $a \equiv b \mod p$. 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 $a \equiv g^k \mod p$ 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 mod p exists by an earlier Corollary, so $a \equiv g^k \mod p$ for some $k \in \mathbb{Z}$. Suppose $k \in \mathbb{Z}$ is even. Then $k = 2j$ and so $a \equiv (g^j)^2 \mod p$. Thus $a$is a quadratic residue mod p. Suppose conversely a is a quadratic resdiue mod p. Then $a \equiv b^2 \mod p$ for some $b \in \mathbb{Z}$ and $p \nmid b$. Then $b \equiv g^r$ for some $r \in \mathbb{Z}$ and so $g^k \equiv (g^r)^2 \equiv g^{2r} \mod p$. By an earlier proposition, we can say $k \equiv 2r \mod p-1$ by an earlier proposition since $\text{ord}_p(g) = \phi(p) = p-1$. So $k \equiv 2r \mod 2$ since $2 \equiv (p-1)$. Hence $k \equiv 0 \mod 2$ and is even. □

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

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

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 $a \equiv g^k \mod p$. Since $\text{ord}_p(g) = p-1$ we have $g^{p-1} \equiv 1 \mod p$ and $g^{\frac{p-1}{2}} \not\equiv 1 \mod p$. Since p is an odd prime we have, $g^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. Therefore, $g^{\frac{p-1}{2}} \equiv -1 \mod p$. Then,

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

The result now follows from the previous lemma. □

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 $a \equiv b^2 \mod p$. Thus by FLT we have,

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

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,

$$f(x) \equiv 0 \mod p$$

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 $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$. But by FLT we have $a^{p-1} \equiv 1 \mod p$ and we can say that $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. Therefore,

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

This completes the proof. □