Number Theory

Aamod Varma

MATH - 4150, Fall 2025

Contents

Chapter 1

Divisibility and Factorization

1.1 Divisibility

Definition (Divisibility). Let $a, b \in \mathbb{Z}$, then a divides b and we write, $a \mid b$, if there exists $c \in \mathbb{Z}$ such that, $b = ac$. We also say a is a divisor of b or a factor. We write $a \not| b$ to say a does not divide b

Example.

1. $3|6$ as $c = 2 \in \mathbb{Z}$ such that $3 \cdot 2 = 6$
2. $3| - 6$ as $c = -2 \in \mathbb{Z}$ such that $3 \cdot 2 = 6$
3. If $a \in \mathbb{Z}$ then $a|0$ as for all a $c = 0$ will give us $a \cdot 0 = 0$
4. $0 \mid 0$ as for any $c \in \mathbb{Z}$ it holds true.

◇

Proposition 1.1. Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$

Proof. If $a|b$ then we have c_1 such that $ac_1 = b$ by definition. If $b|c$ then we have $bc_2 = c$ by definition. So we have,

$$\begin{aligned} bc_2 &= c \\ ac_1c_2 &= c \\ ac_3 &= c \quad \text{taking } c_3 = c_1c_2 \end{aligned}$$

which by definition implies that $a|c$ □

Proposition 1.2. Let $a, b, c, m, n \in \mathbb{Z}$. If $c|a$ and $c|b$ then $c|am + bn$.

Proof. If $c|a$ then exists c_1 such $cc_1 = a$ similarly exists c_2 such that $cc_2 = b$. Now we have,

$$\begin{aligned} cc_1 &= a \\ cc_1m &= am \end{aligned}$$

and

$$\begin{aligned} cc_2 &= b \\ cc_2n &= bn \end{aligned}$$

which gives us $am + bn = c(c_1m + c_2n) = cc_3$ which by definition implies that $c|am + bn$ $\square$

Definition (Greatest integer function)**.** Let $x \in \mathbb{R}$, the greatest integer function of x, denoted $[x]$ or $\lfloor x \rfloor$ is the greatest integer less than or equal to x.

Example.
1. If $a \in \mathbb{Z}$ then $[a] = a$ (The converse that if $[a] = a$ then $a \in \mathbb{Z}$ is also true.)
2. $[\pi] = 3, [e] = 2, [-1.5] = -2, [-\pi] = -4$

$\diamond$

Lemma 1.3. Let $x \in R$ then $x - 1 < [x] \leq x$

Proof. Suppose to the contrary that $[x] \leq x - 1$ then $[x] < [x] + 1 \leq x$. However $[x] + 1 \in \mathbb{Z}$ which mmakes $[x] + 1$ the greatest integer lesser than x. But this contradicts the definition hence we have $x - 1 < [x]$. $\square$

Theorem 1.4 (The Division Algorithm)**.** Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique q, r such that,

$$a = bq + r \qquad 0 \leq r < b$$

Proof. 1. Existence
Let $q = [\frac{a}{b}]$ and $r = a - b[\frac{a}{b}]$. Now by construction we have, $a = bq + r$. Now we show that $0 \leq r < b$. By Lemma we have,

$$\begin{aligned}
\frac{a}{b} - 1 < [\frac{a}{b}] &\leq \frac{a}{b} \\
b - 1 > -b[\frac{a}{b}] &\geq -a \\
b - a > -b[\frac{a}{b}] &\geq -a \\
b > a - b[\frac{a}{b}] &= r \geq 0
\end{aligned}$$

2. Uniqueness
Assume there are q_1, q_2, r_1, r_2 such that,

$$a = bq_1 + r_1 \quad a = bq_2 + r_2$$

We have,

$$\begin{aligned}
0 &= a - a \\
&= (bq_1 + r_1) - (bq_2 + r_2) \\
&= b(q_1 - q_2) + (r_1 - r_2)
\end{aligned}$$

Now,

$$r_2 - r_1 = b(q_1 - q_2)$$

so now we have $b|r_2 - r_1$, but we know that $-(b-1) \leq r_2 - r_1 \leq b - 1$ which means that $r_2 - r_1 = 0$ which implies that $r_1 = r_2$. Similarly we have $b(q_1 - q_2) = r_2 - r_1 = 0$ which means that $q_1 - q_2 = 0$ or $q_1 = q_2$ $\square$

Note. $r = 0$ if and only if $b|a$

Example. Suppose $a = -5, b = 3$ then we have,

$$q = [\frac{a}{b}] = [-\frac{5}{3}] = -2$$

And

$$r = a - b[\frac{a}{b}] = -5 = 3(-2) = 1$$

So $-5 = 3 \cdot -2 + 1$ $\diamond$

Note. We can also write $-5 = -3 \cdot 1 - 2$. However this doesn't contradicts the uniqueness as $r = -2$ is not in the bounds defined in our definition.

Definition. Let $n \in \mathbb{Z}$, then n is even if $2|n$ and odd otherwise.

1.2 Prime Numbers

Definition (Prime Numbers)**.** Let $p \in \mathbb{Z}$ with $p > 1$. Then p is prime if and only if the only positive divisors of p are 1 and itself. If $n \in \mathbb{Z}$ and $n > 1$, if n is not prime then n is composite.

Note. 1 is neither prime nor composite.

Example. 2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41, 43, 47 $\diamond$

Lemma 1.5. Every integer greater than 1 has a prime divisor

Proof. Assume this is not true and by the well ordering principle there exists a least number n that does not have a prime divisor. Note $n|n$ so n can't be prime so assume n is composite then that means $n = ab$ for some $1 < a, b < n$. However, n is the least integer that doesn't have a prime divisor. Which means that both a, b have prime divisors which also means that n has a prime divisor. This contradicts our assumption and therefore every integer $n > 1$ has a prime divisor. $\square$

Note. Well ordering principle sates that every non-empty subset of the positive integers has a least element.

Theorem 1.6. There are infinitely many primes.

Proof. Assume not true and let $p_1, \ldots, p_n$ be the finite primes. Now consider $N = p_1 p_1 \ldots p_n + 1$, this must be composite by assumption. Now using Lemma 1.5 this means that N has some prime divisor p_i. This means that $p_i|N$. We also know $p_i|p_1 p_2 \ldots, p_n$. This means $p_i|N - p_1, \ldots, p_n$ or $p_i|1$ which is false. Hence, by contradiction our assumption is wrong and there are infinitely many primes. $\square$

Note. Try to modify the proof and construct infinitely many problematic N.

Proposition 1.7. If n is composite, the n has prime divisor that is less than or equal to $\sqrt{n}$

Proof. Consider $n = ab$ where $1 < a, b < n$. now, without loss of generality choose b such that $b \geq a$. now we show that $a \leq \sqrt{n}$. Suppose to the contrary $a > \sqrt{n}$. Then we have $n = ab \geq a^2 > n$. Which is not true. Hence we have $a \leq \sqrt{n}$. By lemma 1.5, a has a prime divisor p. But $p|a$ and $a|n>$ Since $p|a$ we have $p \leq a \leq \sqrt{n}$. $\square$

Note. This means if all prime divisors n are greater than $\sqrt{n}$ then n is prime.

Example. To find primes less than n then we can delete multiples of primes less than $\sqrt{n}$. ◇

Proposition 1.8. For any positive integer n, there are at least n consecutive composite numbers.

Proof. Consider the following set of numbers,

$$\{(n+1)!+2, \ldots, (n+1)!+(n+1)\}$$

Note that for any $2 \leq m \leq n+1$, clearly $m|m$ and $m|(n+1)!$ so we have by Proposition 1.2,

$$m|(n+1)!+m$$

Hence every integer in the set is composite. □

Note. Primes can also be very close,

$$(2,3),(3,5),(5,7)$$

Conjecture. There are infinitely many pairs of primes that differ by exactly 2.

Note. Zhang (2013) showed that infintely many pairs whose diff is $\leq 70,000,000$. This has been lowered to 246

Note. Assuming UBER strong conjectures, we can get down to 6.

Average Gaps

Gauss conjectured that as $x \to \infty$ the number of primes $\leq x$ denoted by $\pi(x)$ goes to $\frac{x}{\log(x)}$.
Or, the "probability" that $n \leq x$ is prime is $\frac{\pi(x)}{x} \sim \frac{1}{\log(x)}$

Note. This was proven independently in 1896

Definition. Let $x \in \mathbb{R}$, $\pi(x) = |\{p : p \text{ is prime}, p \leq x\}|$

Theorem 1.9.

$$\lim_{x\to\infty} \frac{\pi(x)\log(x)}{x} = 1$$

Conjecture (Goldbach's Conjecture)**.** Every even integer ≥ 4 is the sum of two primes.

Note. Ternary Goldbach shows that odd number ≥ 7 is a sum of 3 primes and is proved.

Mersenne and Fermats Primes

If $p = 2^n - 1$ is prime then its called a Mersenne prime.
If $p = 2^{2^n} + 1$ is prime then its called a Fermat prime.
Conjectures are there are infinitely many Mersenne primes and but finitely many Fermat primes.

1.3 Greatest Common Divisors

Given $a, b \in \mathbb{Z}$, not both zero, consider the following set,

$$S = \{c \in \mathbb{Z} : c|a \text{ and } c|b\}$$

So S contains ± 1 so is nonempty and also finite since at least one of a and b is non-zero
Thus the maximal element of S exists

Definition (GCD)**.** Let $a, b \in \mathbb{Z}$ with a, b not both 0. Then the **greatest common divisor** of a and b denoted by (a, b) is the largest integer d such that $d|a$ and $d|b$. If $(a, b) = 1$ then a and b are **relatively prime** (or co-prime).

Remark. are,

1. $(0, 0)$ is undefined
2. $(a, b) = (-a, b) = (a, -b) = (-a, -b) = d$
3. $(a, 0) = |a|$

Example. Compute $(24, 60)$. We have,
Divisors of 24 are $\pm(1, 2, 3, 4, 6, 8, 12, 24)$
Divisors of 60 are $\pm(1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60)$
So $(24, 60) = 12$ ◇

Proposition 1.10. Let $(a, b) = d$ then $(\frac{a}{d}, \frac{b}{d}) = 1$

Proof. Let $d' = (\frac{a}{d}, \frac{b}{d})$. Then $d'|\frac{a}{d}$ and $d'|\frac{b}{d}$, so, there is e, f such that,

$$d'e = \frac{a}{d} \text{ and } d'f = \frac{b}{d}$$
$$dd'e = a \text{ and } dd'f = b$$

Thus $dd'|a$ and $dd'|b$ so dd' is a common divisor of a, b. Thus $d' = 1$ otherwise $dd' > d$ contradicting that $(a, b) = d$. □

Proposition 1.11. Let $a, b \in \mathbb{Z}$ both not zero. Let

$$T = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$$

Then $\min T$ exists and is equal to (a, b)

Proof. Without loss of generality let $a \neq 0$. Note that $a = a \times 1 + b \times 0$ and $-a = a \times (-1) + b \times 0$ so we have $a \in T$ and hence T is non-empty. Now by the well ordering principle as T is a non-empty set of non-negative numbers it contains a minimal element call it d.
Then $d = m'a + n'b$ for some $m', n' \in \mathbb{Z}$. Now we show that $d|a$ and $d|b$. By the division algorithm we have,

$$a = dq + r, \quad \mathit{0} \leq r < d$$

So we have

$$\begin{aligned} r = a - dq &= a - (m'a + n'b)q \\ &= a(1 - m'q) - n'qb \end{aligned}$$

So r is an integral linear combination of a and b. But d is the least positive integral linear

combination of a, b and $0 \leq r < d$ so r must be 0. Thus $d|a$. The argument for $d|b$ is similar. Thus d is a common divisor of a, b.
Suppose $c|a$ and $c|b$ then,

$$c|ma + nb \text{ and in particular } c|d$$

Which means c is a divisor of d and hence $c \leq d$. Thus $d = (a, b)$ □

Note. If $(a, b) = d$ then $d = ma + nb$ for some $m, n \in \mathbb{Z}$. If $d = 1$ the converse is true. If,

$$1 = ma + nb \text{ and } d|a, d|b,$$

then, $d|1$ so $d = 1$

Remark. Along the way, we showed that any common divisor of a, b divides (a, b).

Definition. Let $a, \ldots, a_n \in \mathbb{Z}$ with at least one nonzero. The greatest common divisor of $a_1, \ldots, a_n$ denoted $(a_1, \ldots, a_n)$, is the largest integer d such that $d|a_1, \ldots, d|a_n$. If $(a_1, \ldots, a_n) = 1$ the integers $a_1, \ldots, a_n$ are relatively prime and if $(a_i, a_j) = 1$ for $i \neq j$ then they are pairwise relatively prime.

Note. Pairwise implies relatively prime but the converse is not true.

Euclidean Algorithm

Lemma 1.12. If $a, b \in \mathbb{Z}, a \geq b > 0$ and $a = bq + r$ with $q, r \in \mathbb{Z}$. Then $(a, b) = (b, r)$.

Proof. It suffices to show that the two sets of common divisors of a, b and b, r are the same. Denote by S_1 and S_2 the two sets, respectively. Let $c \in S_1$ which means that $c|a$ and $c|b$. But we have $r = a - bq$ which means that $c|r$ and hence $c \in S_2$ which means that $S_1 \subseteq S_2$.
Now let $c \in S_2$ so $c|r$ and $c|b$. As $a = bq + r$ we have $c|a$ so $c \in S_1$ and hence $S_1 \subseteq S_2$ and $S_1 = S_2$. Thus $\max S_1 = \max S_2 \Rightarrow (a, b) = (r, b)$. □

Example. Calculate $(803, 154)$.
We have, $803 = 154 * 5 + 33$ so,

$$\begin{aligned}
(803, 154) &= (33, 154) \\
(154, 33) &= (33, 22) \\
(33, 22) &= (22, 11) \\
(22, 11) &= (11, 0)
\end{aligned}$$

◇

Theorem 1.13. Let $a, b \in \mathbb{Z}, a \geq b > 0$. By the division algorithm, there exists $q_1, r_1 \in \mathbb{Z}$ such that,

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b$$

Then again by the division algorithm there is $q_2, r_2 \in \mathbb{Z}$ such that,

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 \leq r_1$$

And again,

$$r_1 = q_3 r_2 + r_3, 0 \leq r_3 < r_2$$

and so on.
Then $r_n = 0$ for some $n \geq 1$ and $(a, b) = b$ if $n = 1$and r_{n-1} if $n > 1$

Proof. Note $r_1, > r_2 > \dots$ if $r_n \neq 0$ for all $n \geq 1$, then this is a strictly decreasing infinite sequence of positive integers which is not possible. Thus $r_n = 0$ for some n. If $n > 1$, repeatedly apply Lemma 1.12 to get,

$$(a, b) = (r_1, b) = (r_1, r_2) = \cdots = (r_{n-1}, 0) = r_{n-1}$$

□

Example. By reversing this process we can write (a, b) as an integral linear combination of a, b. We had, $(803, 154) = 11$. By reversing we have,

$$\begin{aligned} 11 &= 33 - 1 \times 22 = 33 - \times(154 - 33 \times 4) \\ &= 33 \times 5 - 154 = 5 \times (803 - 154 \times 5) - 154 \\ &= 5 \times 803 - 154 \times 26 \end{aligned}$$

◇

Note. This is **not** unique

1.4 The fundamental Theorem of Arithmetic

Lemma 1.14 (Euclid)**.** Let $a, b \in \mathbb{Z}$ and let p be a prime number. If $p|ab$ then show that $p|a$ or $p|b$.

Proof. If $p|a$ then we're done, so assume that $p \not| a$. So that means that $(p, a) = 1$ which means there is some $m, n \in \mathbb{Z}$ such that,

$$am + pn = 1$$

Now $p|ab$ so exists $c \in \mathbb{Z}$ such that $pc = ab$, so we have,

$$\begin{aligned} am + pn &= 1 \\ amb + pnb &= b \\ pmc + pnb &= b \\ p(mc + nb) &= b \\ p(k) &= b \end{aligned}$$

Where $k = mc + nb$. So we showed that $pk = b$ which implies that $p|b$. So we got either $p|a$ or $p|b$. □

Remark. This fail if p is composite. Take $p = 6, a = 2, b = 3$. We have $p|ab$ but not $p|a$ or $p|b$.

Corollary 1.15. Let $a_1, \dots, a_n$ be integers and p a prime. If $p|a_1 \dots a_n$ then $p|a_i$ for some $1 \leq i \leq n$.

Proof. Induction on n. For $n = 1$ it's trivial. For $n = 2$, is just Lemma 1.14. Now assume that it is true for some $n \geq 2$. To show that it holds for $n + 1$.

Assume $p|a_1 \dots a_n \Rightarrow p|a_i$ for some $i \leq i \leq n$. Suppose $p|a_1 \dots a_{n+1}$. Then $p|(a_1 \dots a_n)a_{n+1}$. So we have either $p|(a_1 \dots a_{n+1})$ or $p|a_{n+1}$ by Lemma 1.14. If $p|(a_1 \dots a_n$ then we know $p|i$ for some $1 \leq i \leq n$ else we have $p|a_{n+1}$. So we have $p|a_i$ for some $1 \leq 1 \leq n + 1$. □

Theorem 1.16 (Fundamental theorem of arithmetic). Every integer greater than 1 may be expressed in the form $m = p_1^{a_1} \dots p_n^{a_n}$ where $p_1, \dots, p_n$ are distinct primes and $a_1, \dots, a_n \in \mathbb{Z}^+$. This form is called the ***prime factorization of m***. This factorization is unique up to permutations of the factors $p_i^{a_i}$.

Proof. (i) Existence
Assume $m > 1$ does not have a prime factorization. Without loss of generality assume m is the smallest such integer by the well ordering integer. In particular, m is not prime, which means that $m = ab$ for some $1 < a, b < m$. As $a, b \leq m$ this means that a, b have prime factorization. The product of which will give us the prime factorization for m. Contradiction, hence every integer > 1 has a prime factorization.

(ii) Uniqueness
Assume $m = p_1^{a_1} \dots p_n^{a_n} = q_1^{b_1} \dots q_r^{b_r}$. Without loss of generality assume that $p_1 < p_2 \dots < p_n$ and $q_1 < q_2 \dots < q_r$. To show these are the same we need to show that,

$$\begin{cases} \text{n} = \text{r} \\ \text{p}_i = q_i \text{ for each } i \\ \text{a}_i = b_i \text{ for each } i \end{cases}$$

Let $p_i|m$ then $p_i|q_i^{a_i} \dots q_r^{a_r}$, then $p_i|q_j$ for some $1 \leq j \leq r$ then $p_i = q_i$. Similarly, given q_i we have $q_i = p_j$ for some. Thus the primes in both the factorization are the same. Thus $n = r$ and by our ordering $p_i = q_i$ for each $1 \leq i \leq n$ so we have,

$$m = p_1^{a_1} \dots p_n^{a_n} = p_1^{b_1} \dots p_n^{b_n}$$

Suppose to the contrary that $a_i \neq b_i$ for some i. Without loss of generality let $a_i < b_i$. Then $p_i^{b_i}|m$. So,

$$p_i^{b_i}|p_i^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{a_i} p_{i+1}^{a_{i+1}} \dots p_n^{a_n}$$

Thus,

$$p_i^{b_i - a_i}|p_i^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_n^{a_n}$$

Since $a_i < b_i$, $b_i - a_i$. So $p_i|p_i^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_n^{a_n}$. Thus $p_i|p_j$ for some $i \neq j$ and then $p_i = p_j$ as they are all distinct prime numbers. This is a contradiction and hence $a_i = b_i$ for each i.

□

Remark. This is one of many reasons why 1 is not prime. If 1 was a prime then we can write $m = (\text{product})1^b$ where b is not unique.

Definition (LCM). Let $a, b \in \mathbb{Z}^+$. The *least common multiple of a and b* denoted $[a, b]$ is the least positive integer m such that $a|m$ and $b|m$.

Remark. By the well ordering principle $[a, b]$ always exists as it forms a non-empty set (ab is in the set).

Example. We have,

$$6 \to 6, 12, 18, 24, 30, 36, 42, 48, \dots$$
$$7 \to 7, 14, 21, 28, 35, 42, 49, \dots$$

So $[6, 7] = 42$ ◇

Remark. The FTA can be used to compute both the GCD and LCMs.

Proposition 1.17. Let $a, b \in \mathbb{Z}^+$. Write $a = p_1^{a_1} \dots p_n^{a_n}$ and $b = p_1^{b_1} \dots p_n^{b_n}$ where p_i are distinct and $a_i, b_i \geq 0$. Then

$$(a, b) = p_1^{\min a_1, b_1} \dots p_n^{\min a_n, b_n}$$

.

$$[a, b] = p_1^{\max a_1, b_1} \dots p_n^{\max a_n, b_n}$$

Proof. Use $(a, b) = p_1^{c_1} \dots p_n^{c_n}$ and $[a, b] = p_1^{a_1} \dots p_n^{d_n}$ and use properties of GCD and LCM. $\square$

Example. Compute $(75, 2205)$ and $[75, 2205]$. So we have,

$$756 = 2^2 3^3 5^0 7^1$$
$$2205 = 2^0 3^2 5^1 7^2$$

So GCD is $2^0 3^2 5^0 7^1 = 63$ and LCM is $2^2 3^3 5^1 7^2 = 26460$ $\diamond$

Lemma 1.18. Given $x, y \in \mathbb{R}$, we have $\min(x, y) + \max(x, y) = x + y$

Proof. If $x = y$ it is obvious.
If $x < y$ then we have $\min(x, y) = x$ and $\max(x, y) = y$ so they sum up to $x + y$, similar for $x > y$. $\square$

Theorem 1.19. Let $a, b \in Z$ with $a, b > 1$. Then $(a, b)[a, b] = ab$.

Proof. Write $a = p_1^{a_1} \dots p_n^{a_n}, b = p_1^{b_1} \dots p_n^{b_n}$ with $a_i, b_i \geq 0$ with p_i distinct. Then,

$$\begin{aligned}(a, b)[a, b] &= p_1^{\min(a_1, b_1)} \dots p_n^{\min(a_n, b_n)} p_1^{\max(a_1, b_1)} \dots p_n^{\max(a_n, b_n)} \\ &= p_1^{\min(a_1, b_1) + \max(a_1, b_1)} \dots p_n^{\min(a_n, b_n) + \max(a_n, b_n)} \\ &= p_1^{a_1 + b_1} \dots p_n^{a_n + b_n} \\ &= ab\end{aligned}$$

$\square$

Theorem 1.21. Let $a, b \in \mathbb{Z}$ with $a, b > 0$ and $(a, b) = 1$, then the ***arithmetic progression***,

$$a, a + b, a + 2b, a + 3b, \dots$$

contains infinitely many prime numbers

Remark. Setting $a = b = 1$ recovers the fact the there are infinitely many primes.

Remark. We can use the fundamental theorem of arithmetic to prove special cases. i.e. when $a = 3, b = 4$ so $p = 4n + 3$

Proposition 1.22. There are infinitely many primes of the form $4n + 3, n > 0$.

Lemma 1.23. Let $a, b \in \mathbb{Z}$, if a, b are expressive in the form $4n + 1$, so is ab.

Proof. We have $a = 4n+1$ and $b = 4m+1$ so we have $ab = (4n+1)(4m+1) = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1 = 4k + 1$ where $k = 4nm + n + m$. So we have $ab = 4k + 1$ which concludes our proof. $\square$

Proof. (Proposition 1.22)
Assume to the contrary that there are only finite primes of the form $4n + 3$ labeled as,

$$p_0 = 3, p_1 = 7, p_2, p_3, \dots, p_r$$

Consider the integer $N = 4p_1 \dots p_r + 3$. The prime factorization of N must contain a prime of the desired form, otherwise N would be a product of prime of $p = 4n + 1$ and would then itself have the same form. Thus $3|N$ or $p_i|N$ for some $i \leq i \leq r$
Case 1. $3|N$. Then $3|N - 3$ so $3|p_1 \dots p_r$, contradiction.
Case 2. $p_i|N$ for some $1 \leq i \leq r$ then $p_i|N - 4p_1 \dots p_r$ so $p_i|3$, contradiction.
Therefore there are ∞ many primes such that $p = 4n + 3$ $\square$

Chapter 2

Congruences

2.1 Congruences

Definition. Let $a, bm \in \mathbb{Z}$ with $m > 0$. Then a *is said to be congruent to* b *mod* m written $a \equiv b \pmod{m}$, if $m \mid a - b$.

Note. The integer m is called the modulus.

Example. $25 \equiv 1 \pmod{4}$, $25 \equiv 4 \pmod{7}$ ◇

Proposition 2.1. Congruence modulo m is an equivalence relation on $\mathbb{Z}$.

Proof. Reflexive. Since $m|0$ so $m|a - a$ so $a \equiv a \pmod{m}$.

Symmetric. Consider $a \equiv b \pmod{m}$ so $m|a - b$ or for some $k \in \mathbb{Z}$ $km = a - b$ which means $(-k)m = b - a$ which means $m|b - a$ or $b \equiv a \pmod{m}$

Transitive. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. We have from both,

$$a - b = k_1 m \quad \text{for some } k_1$$

$$b - c = k_2 m \quad \text{for some } k_2$$

Adding both we have $a - c = (k_1 + k_2)m$ or $m|a - c$ which means $a \equiv c \pmod{m}$ □

Consequence 2.2. $\mathbb{Z}$ is partitioned into equivalence classes modulo m.

Remark. Given $a \in \mathbb{Z}$, let $[a]$ denote the equivlance class of a modulo m

Example. The equivalence classes under congruence mod 4 are,

$$\begin{aligned}
[0] &= \{n : n \equiv 0 \pmod{4}, n \in \mathbb{Z}\} = \{\dots, -4, 0, 4, \dots\} \\
[1] &= \{n : n \equiv 1 \pmod{4}, n \in \mathbb{Z}\} = \{\dots, -3, 1, 5, \dots\} \\
[2] &= \{n : n \equiv 2 \pmod{4}, n \in \mathbb{Z}\} = \{\dots, -2, 2, 6, \dots\} \\
[3] &= \{n : n \equiv 3 \pmod{4}, n \in \mathbb{Z}\} = \{\dots, -1, 3, 7, \dots\}
\end{aligned}$$

◇

Definition (Residue)**.** A set of m integers such that every integer is congruent modulo m to exactly one integer of the set is called a *complete residue system*.

Example. $\{0, 1, 2, 3\}$ is a complete residue system modulo 4. So is $\{4, 5, -6, -1\}$ ◇

Proposition 2.3. The set $\{0, 1, \dots, m-1\}$ is a complete residue system mod m.

Proof. Existence. Let $a \in \mathbb{Z}$, then by the division algorithm there is some $q, r \in \mathbb{Z}$ such that $0 \leq r < m$ such that $a = qm + r$ or $a - r = qm$ implies that $a \equiv r \pmod{m}$

Uniqueness. Assume $a \equiv r_1 \pmod{m}$ and $a \equiv r_2 \pmod{m}$ where $r_1, r_2 \in \{0, 1, \dots, m-1\}$. Then we have $r_1 \equiv r_2 \pmod{m}$ by transitivity or that $r_1 - r_2 = km$ but $-(m-1) \leq r_1 - r_2 \leq m - 1$ so $r_1 - r_2 = 0$ or $r_1 = r_2$. $\square$

Definition. The set $\{0, 1, \dots, m-1\}$ is called the set of *least non-negative residues modulo m.*

Proposition 2.4. Let $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$

Proof. (a) Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ so we have,

$$\begin{aligned} a - b &= k_1 m \quad k_1 \in \mathbb{Z} \\ c - d &= k_2 m \quad k_2 \in \mathbb{Z} \end{aligned}$$

Adding two together we have,

$$(a + c) - (b + d) \equiv (k_1 + k_2)m$$

or that,

$$a + c \equiv b + d \pmod{m}$$

(b) If $m \mid a-b$ then $m \mid c(a-b)$ similarly $m \mid d-c$ means $m \mid a(d-c)$. This $m \mid c(a-b)+a(c-d)$ or $m \mid ac - bd$ or that $ac \equiv bd \pmod{m}$

$\square$

Consider $\{0^2, 1^2, 2^2, 3^2\} = \{0, 1, 0, 1, \} = \{0, 1\}$

Note. Exceptional Characters, Seigel zeros

2.2 Calculations

Example. Compute a complete residue system mod 5,

- Using only even numbers
- Using only prime numbers
- Using only numbers congruent to $1 \pmod{4}$

Default is $\{0, 1, 2, 3, 4\}$ so even numbers are $\{0, 6, 2, 8, 4\}$. For prime numbers we have,

$$\begin{aligned} 0, 5 \\ 1, 6, 11 \\ 2, 7 \\ 3, 8, 13 \\ 4, 9, 14, 19 \end{aligned}$$

So we have $\{5, 11, 7, 13, 19\}$ ◇

Note. We know that addition and multiplication are closed under congruence . We can think of this in terms of equivalnece classes,

$$[a] + [b] = [a + c]$$
$$[b] \cdot [d] = [bd]$$

This turns the set of equivalence classes into a ring. We can construct addition and multiplication tables,

Proposition 2.5. Let $a, b, c, m \in \mathbb{Z}, m > 0$ then $ca \equiv cb \pmod{m}$ if and only if $a \equiv b \pmod{\frac{m}{(m,c)}}$

Proof. $\Rightarrow$. Assume $ca \equiv cb \pmod{m}$ so we have, $m \mid ca - cb$ or $m \mid c(a - b)$. Let $d = (m, c)$. By transitivity we have $\frac{m}{d} \mid \frac{c}{d}(a - b)$ but $(\frac{m}{d}, \frac{c}{d}) = 1$ which implies that $\frac{m}{d} \mid (a - b)$ or $a \equiv b \pmod{\frac{m}{d}}$ by definition.

$\Leftarrow$. Assume $a \equiv b \pmod{\frac{m}{(m,c)}}$ and $d = (m, c)$. We have $\frac{m}{d} \mid a - b$ so $m \mid d(a - b)$ and so $m \mid d(a - b)\frac{c}{d}$ or $m \mid c(a - b)$ or $ca \equiv cb \pmod{m}$ □

2.3 Linear Congruences in one variable

Definition. Let $a, b \in \mathbb{Z}$. A congruence of the form $ax \equiv b \pmod{m}$ is called a *linear congruence* in the variable x.

Example. If $2x \equiv 3 \pmod{4}$ has no solutions. But $2x \equiv 4 \pmod{6}$ has $x = 2$ as the only solution. And $3x \equiv 9 \pmod{6}$ has $1, 3, 5$. ◇

Theorem 2.6. Let $ax \equiv b \pmod{m}$ and $d = (a, m)$. If $d \nmid b$ then there are no solutions in $\mathbb{Z}$. Else, the congruence has exactly d *incongruent* solutions modulo m in $\mathbb{Z}$.

Note. This means that for any solution there are d equivalence classes.

Proof. Note that $ax \equiv b \pmod{m}$ iff $m \mid ax - b$ iff $ax - b = my$ for some $y \in \mathbb{Z}$ iff $ax - my = b$. Thus $ax \equiv b \pmod{m}$ is solvable in x if $ax - my = b$ is solvable in x, y. Let x, y be a solution of $ax - my = b$. Since, $d \mid a$ and $d \mid m$ so $d \mid b$. Taking contrapositives, if $d \nmid b$ then there is no solution.

Assume now that $d \mid b$. We prove the second part in four steps.

1. We'll show that $ax \equiv b \pmod{m}$ has a solution x_0.
2. We'll show that there are infinitely many solutions of a particular form.
3. We'll show that any solution has a particular form involving x_0 (combining with 2 will give us all possible solutions).
4. We'll show there are exactly d equivalence classes.

First, since $d = (a, m)$, there exists $r, s \in \mathbb{Z}$ such that $ar + ms = d$. Now as $d \mid b$ we have $b = \frac{b}{d}d = \frac{b}{d}(ra + sm) = (\frac{b}{d}r)a + (\frac{b}{d}s)m$ thus $b - a(\frac{b}{d})r = (\frac{b}{d}s)m$ and we have $m \mid b - a(\frac{b}{d}r)$.

Thus $a(\frac{b}{d}r) \equiv b \pmod{m}$ and we have $x_0 = \frac{b}{d}r$ is a solution.

Now, let x_0 be any solution. Consider the number $x_0 + (\frac{m}{d})n$ where $n \in \mathbb{Z}$. So,

$$\begin{aligned} a(x_0 + \frac{m}{d}n) &\equiv ax_0 + \frac{m}{d}n \pmod{m} \\ &\equiv b + \frac{a}{d}mn \pmod{m} \\ &\equiv b \pmod{m} \end{aligned}$$

Let x_0 be an arbitrary solution of $ax \equiv b \pmod{m}$. So we have $ax_0 - my_0 = b$ for some $y_0 \in \mathbb{Z}$. Let x be any other solution. Then $ax - my = b$ for some $y \in \mathbb{Z}$. Subtracting both we have,

$$\begin{aligned} (ax_0 - my_0) - (ax - my) = 0 \\ a(x_0 - x) - m(y_0 - y) = 0 \\ a(x_0 - x) &= m(y_0 - y) \\ \frac{a}{d}(x_0 - x) &= \frac{m}{d}(y_0 - y) \end{aligned}$$

If $y_0 - y = 0$ then $x_0 - x = 0$. Now as solution are different we can assume $y_0 \neq y$. Now, we see that $(\frac{m}{d}, \frac{a}{d}) = 1$, so $\frac{m}{d} \mid \frac{a}{d}(x_0 - x)$ we have $\frac{m}{d} \mid x_0 - x$ by Prop 1.10. And we have $x \equiv x_0 \pmod{\frac{m}{d}}$. Thus, all solutions to $ax \equiv b \pmod{m}$ are given by $x = x_0 + \frac{m}{d}n, n \in \mathbb{Z}$ and x_0 is any particular solution.

Let $x_0 + \frac{m}{d}n, x_0 + \frac{m}{d}n_2$ be solutions. Then,

$$\begin{aligned} x_0 + \frac{m}{d}n_1 &\equiv x_0 + \frac{m}{d}n_2 \pmod{m} \\ \frac{m}{d}n_1 &\equiv \frac{m}{d}n_2 \pmod{m} \end{aligned}$$

This means that $m \mid \frac{m}{d}(n_1 - n_2)$ or $\frac{m}{d}(n_1 - n_2) = km$ and we have $n_1 - n_2 = kd$ and $n_1 \equiv n_2 \pmod{d}$. Since there are d choices for the equivalence class of n. All solutions must fall into one of these cases.

□

Corollary 2.7. Consider the linear congruence $ax \equiv b \pmod{m}$, and let $d = gcd(a, m)$. If $d \mid b$, then there are exactly d incongruent solutions modulo m given by,

$$x = x_0 + \left(\frac{m}{d}n\right), \quad n = 0, 1, 2, \ldots, d-1$$

and x_0 is any particular solution.

Example. Find all incongruent solutions to $16x \equiv 8 \pmod 2)8$. Here we have $d = gcd(a, m) = gcd(16, 28) = 4$. We see that $4 \mid 8$. Now we find a particular solution. Working backwards we have $4 = 2 \cdot 16 + (-1) \cdot 28$ so $8 \cdot 16 + (-2) \cdot 28$. Then $x_0 = 4$ is a solution, and we have all solutions given by,

$$x = 4 + \left(\frac{28}{4}\right)n, \quad n = 0, 1, 2, 3$$

Which gives us $x = 4, 11, 18, 25$ ◇

Definition. Any solution of $ax \equiv 1 \pmod{m}$ is call the *multiplicative inverse* of a modulo m.

Corollary 2.8. The congruence $ax \equiv 1 \pmod{m}$ has a solution if and only if $(a, m) = 1$

2.4 Chinese Remainder Theorem

Example. Find a positive integer having a remainder of 2 when divided by 3, a remainder of 1 when divided by 4, and a remainder of 3 when divided by 5. So this means,

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

◇

Theorem 2.9. Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime and let $b_1, \ldots, b_n \in \mathbb{Z}$. Then this system,

$$\begin{aligned} x &\equiv b1 \pmod{m_1} \\ &\vdots \\ x &\equiv bn \pmod{m_n} \end{aligned}$$

has a unique solution.

Proof. Let $M = m_1, \ldots, m_n$ and $M_i = M/m_i$. Then $M_i, m_i = 1$. There are solutions to each system $M_i x_i \equiv 1 \pmod{m}$ denoted $x_i = \overline{M}_i$. Now consider $x = b_1 M_1 \overline{M}_1 + b_2 M_2 \overline{M}_2 + \cdots + b_n M_n \overline{M}_n$.

Note that,

$$\begin{aligned} x &\equiv 0 + \cdots + b_i M_i \overline{M}_i + \cdots + 0 \pmod{m}_i \\ &\equiv b_i \pmod{m}_i \end{aligned}$$

This gives existence. For uniqueness, let x' be another solution. Then $x' \equiv b_i \pmod{m}_i$ for each $1 \leq i \leq n$. Then $x \equiv x' \pmod{m}_i$. Then $m_i \mid x - x'$. So $M \mid x - x'$ since m_i are pairwise relative prime and $x \equiv x' \pmod{M}$ □

Example (Continued)**.** We have,

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

We have $M = 3 \cdot 4 \cdot 5 = 60$ and $M_1 = 20, M_2 = 15, M_3 = 12$. So we need to solve,

$$\begin{aligned} 20y_1 &\equiv 1 \pmod{3} \\ 15y_2 &\equiv 1 \pmod{4} \\ 12y_3 &\equiv 1 \pmod{5} \end{aligned}$$

For each we have $7 \cdot 3 - 20 = 1$, $4 \cdot 4 - 15 = 1$ and $5 \cdot 5 - 2 \cdot 12 = 1$. So $y_1 = -1 = 32, y_2 = -1 = 3, y_3 = -2 = 3$.
So,

$$x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233.$$

And we have $233 \equiv 53 \pmod{60}$ which means 53 is the least positive solution. $\diamond$

Lemma 2.10. Let p be a prime and let $a \in \mathbb{Z}$. Then a is it's own inverse modulo $p \Leftrightarrow a \equiv \pm 1 \pmod{p}$

Proof. Suppose a is it's own inverse so $a = \overline{a}$. Then $a^2 \equiv 1 \pmod{p}$ then $p \mid a^2 - 1$ so $p \mid (a+1)(a-1)$ so we have either $p \mid (a+1)$ or $p \mid (a-1)$. In both cases we have either $a \equiv \pm 1 \pmod{p}$

Now suppose $a \equiv \pm 1 \pmod{p}$. Squaring both sides we get $a^2 \equiv 1 \pmod{p}$ so $a = \overline{a}$. $\square$

2.5 Wilson's Theorem

Theorem 2.11 (Wilson's Theorem). Let p be a prime. Then $(p-1)! \equiv -1 \pmod{p}$

Proof. Easily check for $p = 2, 3$. Suppose $p > 3$ is a prime. Then each $1 \leq a \leq p-1$ has a unique inverse modulo p and this inverse is distinct from a if $2 \leq a \leq p-2$. Pair each such integer with its inverse modulo p say a, a'. The product of all these primes is $(p-2)!$ and $(p-2)! \equiv 1 \pmod{p}$ and we get $(p-1)! \equiv (p-1)(p-2)! \equiv (p-1) \equiv -1 \pmod{p}$.

The converse is also true. $\square$

Proposition 2.12. Let $n \in \mathbb{Z}$ with $n > 1$. If $(n-1)! \equiv -1 \pmod{n}$ then n is prime.

Proof. Suppose $n = ab$ with $1 \leq a < n$. It suffices to show that $a = 1$. Since $a < n$ so $a \mid (n-1)!$. Also $n \mid (n-1)! + 1$. Now since $a \mid n$ we have $n \mid (n-1)! + 1$. But we know $a \mid (n-1)!$ so we need $a \mid 1$ which means $a = 1$. $\square$

Example. Take $p = 11$ then, $11 - 1 \equiv 10! \pmod{11}$. By previous Lemma, 10 and 1 are their own inverses. For the other numbers between 2 and 9, we can pair them with their inverses like $2 \Leftrightarrow 6, 3 \Leftrightarrow 4, 5 \Leftrightarrow 9, 7 \Leftrightarrow 8$ which means,

$$(11-1)! \equiv 10 \cdot 1 \equiv -1 \pmod{11}.$$

$\diamond$

Definition. A prime p is a *Wilson Prime* if $(p-1)! \equiv -1 \pmod{p^2}$. The first few are,

$$5, 13, 563.$$

2.6 Fermat's Little Theorem

Theorem 2.13 (Fermat's Little Theorem). Let p be a prime and let $a \in \mathbb{Z}$ then if $p \nmid a$ then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof. Consider the $p-1$ integers as follows,

$$a, 2a, 3a, \ldots, a(p-1)$$

We know that $p \nmid a$ and $p \nmid 1, \ldots, p-1$ so we have $p \nmid ai$ for $1 \leq i \leq p-1$. Note also that for no two of the above numbers are congruent mod p. (Suppose they are congruent i.e. $ai \equiv aj \pmod{p}$, then as p is a prime then we can use the inverse to get $i \equiv j \pmod{p}$. But that means that $i = j$ which is not true by construction).

Thus we have $a, 2a, \ldots, (p-1)a$ is a complete non-zero residue system of p. Thus,

$$\begin{aligned}
a(2a)(3a)\ldots(p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p} \\
a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\
a^{p-1} &\equiv 1 \pmod{p}
\end{aligned}$$

as $(p-1)!$ has an inverse mod p.

□

Remark. The underlying motivation is that for a prime number, given a set of residues if we scale it by any other residue it gives us a permutation of the residues.

2.6.1 Consequences of FLT

Corollary 2.14. Let p be a prime and $a \in \mathbb{Z}, p \nmid a$. Then a^{p-2} is the inverse of a modulo p.

Proof. We have,

$$a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$$

So $a^{p-2} = \overline{a}$ □

Corollary 2.15. Let p be prime and $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$.

Proof. If $p \mid a$ then both sides are congruent to 0 mod p and hence it's true. If $p \nmid a$ then we have,

$$\begin{aligned}
a^{p-1} &\equiv 1 \pmod{p} \\
a \cdot a^{p-1} &\equiv a \pmod{p} \\
a^p &\equiv a \pmod{p}
\end{aligned}$$

□

Corollary 2.16. Let p be a prime. Then $2^p \equiv 2 \pmod{p}$.

Definition (Pseudoprimes)**.** If $n \in \mathbb{Z}$ and n is composite with $n > 1$ and $2^n \equiv 2 \pmod{n}$ then n is called a *pseudoprime*.

Example. For $n = 341$ observe that $n = 11 \cdot 31$. To prove that $2^{341} \equiv 2 \pmod{341}$, it suffices to show that $2^{341} \equiv 2 \pmod{11}$ and $2^{341} \equiv 2 \pmod{3}1$. Note that,

$$\begin{aligned} 2^{341} &\equiv (2^{10})^{34} \cdot 2 \pmod{11} \\ &\equiv 1^{34} \cdot 2 \pmod{11} \\ &\equiv 2 \pmod{11} \end{aligned}$$

Similarly,

$$\begin{aligned} 2^{341} &\equiv (2^{30})^{11} \cdot 2^{11} \pmod{31} \\ &\equiv 1^{11} \cdot (2^5)^2 \cdot 2 \pmod{31} \\ &\equiv 2 \pmod{31} \end{aligned}$$

◇

2.7 Euler's Theorem

Definition. Let $n \in \mathbb{Z}, n > 0$. Eulers phi-function denoted by $\phi(n)$ is the number of positive integers that are less than or equal to n that are relatively prime.

$$\phi(n) = |\{m \in \mathbb{Z} : 1 \leq m \leq n, (m, n) = 1\}|$$

Example. $\phi(4) = 2, \phi(14) = 6, \phi(p) = p - 1$ ◇

Theorem 2.17 (Euler's Theorem)**.** Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$. Then we have,

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Proof. Let $r_1, r_2, \ldots, r_{\phi(m)}$ be distinct positive integers not exceeding m such that $(r_i, m) = 1$. Consider the integers,

$$ar_1, ar_2, \ldots, a_{\phi(m)}$$

Note that $(ar_i, m) = 1$ and for $i \neq j$ we have $ar_i \not\equiv ar_j \pmod{m}$ cause if it weren't true, we can multiply a inverse on both sides to get $r_i \equiv r_j \pmod{m}$. But $r_i \neq r_j$ so we cannot have this to be true.

So we have,

$$\begin{aligned} ar_1 ar_2 \ldots a_{r_{\phi(m)}} &\equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m} \\ a^{\phi(m)}(r_1 \ldots r_{\phi(m)}) &\equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m} \end{aligned}$$

And $r_1 \ldots r_{\phi(m)}$ is coprime to m as each individual elements are coprime to it so we have an inverse to get,

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

□

Definition. Let m be a positive integer. A set of $\phi(m)$ integers such that each integer is relatively prime to m and no two elements are congruent mod m is called a *reduced residue system modulo m*.

Example. $\{1, 5, 7, 11\}$ is a reduced residue system modulo 12. So is $5 \cdot \{1, 5, 7, 11 = \{5, 25, 35, 55\}$

$\{1, \ldots, p - 1\}$ is a reduced residue set modulo p for any prime p. ◇

Corollary 2.19. Let $a, m \in \mathbb{Z}, m > 0, (a, m) = 1$. Then,

$$\overline{a} = a^{\phi(m)-1}$$

Chapter 3

Arithmetic functions and multiplicativity

Definition. An arithmetic function is a function whose domains is the set of positive integers.

Example. of arithmetic functions are,

1. Euler's ϕ function (multiplicative)
2. $v(n)$, the number of positive divisors (multiplicative)
3. $\sigma(n)$, the sum of divisor (multiplicative)
4. $\omega(n)$, the number of distinct prime factors
5. $p(n)$, the number of partitions of n
6. $\Omega(n)$, number of total prime factors.

◇

Definition. An arithmetic function f is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. f is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all integers m, n.

Note. Note that if $n > 1, n = p_1^{a_1} \dots p_r^{a_r}$. Then if f is multiplicative we have,

$$f(n) = f(p_1^{a_1} \dots p_r^{a_r}) = f(p_1^{a_1}) \dots f(p_r^{a_r})$$

so multiplicative functions are determined by their behavior on primes powers. If f is completely multiplicative we have,

$$f(n) = f(p_1)^{a_1} \dots f(p_r)^{a_r}$$

so completely multiplicative functions are determined by their behavior on primes.

Example. For instance $f(n) = 1$ or $f(n) = 0$ are completely multiplicative functions. ◇

Remark. If f is multiplicative and not identically 0 then $f(1) = 1$. Choose n such that $f(n) \neq 0$ then $f(n) = f(n \cdot 1) = f(n) \cdot f(1)$ so $f(1) = 1$.

Definition. $\sum_{d|n} f(d)$ denotes a sum over the positive divisors of n.

Example. $\sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$ ◇

Theorem 3.1. Let f be an arithmetic function over the integer, and for $n \in \mathbb{Z}, n > 0$, let,

$$F(n) = \sum_{d|n} f(d)$$

If f is multiplicative so is F.

Proof. Let $(m, n) = 1$. We need to show that $F(mn) = F(m)F(n)$. We have,

$$F(mn) = \sum_{d|n} f(d)$$

We know that every divisor d of mn can be written uniquely as $d = d_1 d_2$ where $d_1 \mid m$ and $d_2 \mid n$. And any product $d_1 d_2$ is a divisor of mn.

To see this, write $m = p_1^{a_1} \dots p_r^{a_r}, n = q_1^{b_1} \dots q_s^{b_s}$ where all $p_1, \dots, p_r, q_1, \dots, q_r$ are distinct. Then if $d \mid mn$ then,

$$d = p_1^{e_1} \dots p_r^{e_r} q_1^{f_1} \dots q_s^{f_s} \quad 0 \leq e_i \leq a_i, 0 \leq f_i \leq b_i$$

So choose $d_1 = p_1^{e_1} \dots p_r^{e_r}$ and $d_2 = q_1^{f_1} \dots q_s^{f_s}$. (This is unique as we can't have p for d_2 as that would make it NOT a divisor of n).

Now we have,

$$\begin{aligned} F(mn) = \sum_{d|mn} f(d) &= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= F(m)F(n) \end{aligned}$$

□

Example. Let $m = 4, n = 3$. So,

$$\begin{aligned} F(3 \cdot 4) &= \sum_{d|12} f(d) \\ &= f(1) + f(2) + f(3) + f(4) + f(6) + f(12) \\ &= f(1 \cdot 1) + f(1 \cdot 2) + f(1 \cdot 3) + f(1 \cdot 4) + f(2 \cdot 3) + f(3 \cdot 4) \\ &= f(1)f(1) + f(1)f(2) + f(1)f(3) + f(1)f(4) + f(2)f(3) + f(3)f(4) \\ &= (f(1) + f(3))(f(1) + f(2) + f(4)) \\ &= F(3)F(4) \end{aligned}$$

◇

3.1 Euler ϕ function

$\phi(n)$ is the number of integers smaller than n that is coprime to n.

Theorem 3.2. ϕ is multiplicative

Proof. Let $m, n \in \mathbb{Z}, m, n > 0$ and $(m, n) = 1$. We need to show that,

$$\phi(mn) = \phi(m)\phi(n)$$

Consider the array of integers $\leq mn$ write,

$$\begin{pmatrix} 1 & m+1 & 2m+1 & \dots & (n-m)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ i & m+i & 2m+i & \dots & (n-1)m+i \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & 2m+i & 3m+i & \dots & nm \end{pmatrix}$$

Consider the ith row. If $(i, m) > 1$, then no element on the $i'th$ row is relatively prime to m. Then we may restrict our attention to those i that satisfy $(i, m) = 1$. There are by definition $\phi(m)$ such values.

The entries in the $i'th$ row are $i, m + i, 2m + i, \dots (n - 1)m + 1$

Now this is a complete residue system modulo n. We see this as follows. Suppose it is not true so $km + i \equiv jm + i \pmod{n}$ for some $0 \leq k, j \leq n - 1$. So we have $km \equiv jm \pmod{n}$ and we get $k \equiv j \pmod{n}$ as inverse of m mod n exists as they are coprime. So that must mean that $k = j$. So for any non equal k, j it doesn't hold. Hence we have a full residue system.

Thus there are $\phi(n)$ elements in the $i'th$ row that are coprime to n. And as we have $(i, m) = 1$. So we have $\phi(mn) = \phi(m)\phi(n)$ □

Theorem 3.3. Let p be prime and $a \in \mathbb{Z}, a > 0$. Then,

$$\phi(p^a) = p^a - p^{a-1}$$

Proof. The total number of integers not exceeding p^a is p^a. The only integers not relatively prime to p^a are multiples of p smaller than p^a. So,

$$p, 2p, 3p, \dots, p^{a-1}p \quad \text{as } kp \leq p^{a-1}$$

So there are p^{a-1} integers not exceeding p^a that are not relative prime to p^a. Thus

$$\phi(p^a) = p^a - p^{a-1}$$

□

Theorem 3.4. Let $n \in \mathbb{Z}, n > 0$. Then,

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

Proof. Write $n = p_1^{a_1} \dots p_r^{a_r}$. Then,

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1} \dots p_r^{a_r}) \\
&= \phi(p_1^{a_1}) \dots \phi(p_r^{a_r})) \\
&= (p_1^{a_1} - p_1^{a_1 - 1}) \dots (p_r^{a_r} - p_r^{a_r - 1}) \\
&= (p_1^{a_1} p_r^{a_r}) \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p^r}\right) \\
&= n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

□

Remark. This says that $\phi(n)$ is n times the probability (in a loose way) that an integer is not disable by any of the primes dividing n.

Example. Calculate $\phi(504)$. We have,

$$504 = 2^3 \cdot 3^2 \cdot 7$$

So,

$$\begin{aligned}
\phi(504) &= 504 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7}) \\
&= 144
\end{aligned}$$

◇

Theorem 3.5. Let $n \in \mathbb{Z}, n > 0$ then,

$$\sum_{d \mid n} \phi(d) = n$$

Proof. Let $d$be a divisor of n. Let,

$$s_d = \{1 \leq m \leq n : (m, n) = d\}$$

Note that $(m, n) = d$ if and only if $(m/d, n/d) = 1$. Thus $|s_d| = \phi(n/d)$ as if $(m, n) = d$ then $(m/d, n/d) = 1$ and m/d satisfying this is $\phi(n/d)$.

Note also that every integer less than equal to n belongs to exactly one set s_d. Thus,

$$n = \sum_{d \mid n} |s_d| = \sum_{d \mid n} \phi(n/d) = \sum_{d \mid n} \phi(d)$$

□

Note. Every number smaller than N has some GCD with n and this gcd is unique, hence that number falls into one of the s_d. We can rewrite $s_d = \{1 \leq \frac{m}{d} \leq \frac{n}{d} : (\frac{m}{d}, \frac{n}{d} = 1)\}$. The count of all elements in s_d must now equal to the count of all the numbers smaller than $\frac{n}{d}$ which are coprime to it.

Note. Here we have $\sum_{d \mid n} \phi(\frac{n}{d}) = \sum_{d \mid n} \phi(d)$ as for every d we also have n/d a divisor of n. So the set of all divisors of n, $\{d : d \mid n\}$ is the same as this set, $\{n/d : d \mid n\}$ which is also the set of all divisors.

Definition. Let $n \in \mathbb{Z}$, the nuimber of positive divisors, denoted $\tau(n)$, is defined by $\tau(n) = \#\{d \in \mathbb{Z} : d > \theta, d \mid n\}$

Theorem 3.6. $\tau(n)$ is multiplicative

Proof. Observe that,

$$\tau(n) = \sum_{d|n} 1$$

the function $f(n) = 1$ for all n is a multiplicative function so $\tau(n)$ is multiplicative by theorem 3.1 □

Note. Since $\tau(n)$ is multiplicative it's determined by it's behavior on prime powers.

Theorem 3.7. Let p be prime and let $a \in \mathbb{Z}$, then $\tau(p^a) = a + 1$

Proof. As p is a prime, the only divisors of p^a is $1, p, p^2, p^3, \ldots, p^a$ which add up to $a + 1$ divisors. □

Theorem 3.8. Let $n = p_1^{a_1} \ldots p_r^{a_r}$ with $p_1, \ldots, p_2$ are distinct primes and $a_1, \ldots, a_r$ positive integers. Then,

$$\tau(n) = \prod_{i=1}^{r} (a_i + 1)$$

Proof. We have $\tau(n) = \tau(p_1^{a_1} \ldots p_r^{a_r})$ and as τ is multiplicative we have,

$$\begin{aligned}\tau(n) &= \tau(p_1^{a_1} \ldots p_r^{a_r}) \\ &= \tau(p_1^{a_1}) \ldots \tau(p_r^{a_r}) \\ &= (a_1 + 1)(a_2 + 1) \ldots (a_r + 1)\end{aligned}$$

□

Note. Look at Dirchlet's divisor problem

Example. Consider $504 = 2^3 3^2 7$. So $\tau(504) = (3 + 1)(2 + 1)(1 + 1) = 4 \cdot 3 \cdot 2 = 24$ ⋄

3.2 Sum of divisors

Definition. Let $n \in \mathbb{Z}, n > 0$. The sum of divisors function, denoted $\sigma(n)$ is the function defined by,

$$\sigma(n) = \sum_{d|n} d$$

Theorem 3.9. $\sigma(n)$ is a multiplicative function.

Proof. Note that $f(d) = d$ is a multiplicative function (why?). So $\sum_{d|n} d$ is a multiplicative function. □

Theorem 3.10. Let p be a prime and $a > 0$ then,

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}$$

Proof. We have the positive divisors of p^a as $1, p, p^2, p^3, \ldots, p^a$. So we get,

$$\begin{aligned}
\sigma(p^a) &= 1 + p + p^2 + \cdots + p^a \\
p\sigma(p^a) &= p + p^2 + \cdots + p^{a+1} \\
\sigma(p^a)(p-1) &= p^{a+1} - 1 \\
\sigma(p^a) &= \frac{p^{a+1} - 1}{p - 1}
\end{aligned}$$

□

Theorem 3.11. Let $n = p_1^{a_1} \ldots p_r^{a_r}$ then,

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

Example. Consider $504 = 2^3 3^2 7$. So,

$$\sigma(504) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{7^2 - 1}{7 - 1}$$

◇

3.3 Perfect Numbers

Definition. Let $n \in \mathbb{Z}, n > 0$ then n is a perfect number if $\sigma(n) = 2n$

Note. This is equivalent to saying $\sigma(n) - n = n$. Or that the sum of proper divisors (divisors except itself) is n.

Example. 6 is a perfect number as $1 + 2 + 3 = 6$. 28 is a perfect number $1 + 2 + 4 + 7 + 14 = 28$ ◇

Theorem 3.12. Let $n \in \mathbb{Z}, n > 0$. Then n is an even perfect number if and only if,

$$n = 2^{p-1}(2^p - 1)$$

for some p and $2^p - 1$ should be prime.

Note. This theorem gives a characterization of even perfect numbers and a bisection between even perfect numbers and mersenne primes.

Proof. ($\Rightarrow$) Assume that n is an even perfect number. So we can write $n = 2^a b$ where $a, b \in \mathbb{Z}, a > 1, b$ is an odd number.

We have,

$$
\begin{aligned}
\sigma(2^a b) &= \sigma(2^a)\sigma(b) \\
&= \frac{2^{a+1}-1}{2-1}\sigma(b) \\
&= (2^{a+1}-1)\sigma(b)
\end{aligned}
$$

Also, since n is perfect, we have,

$$
\sigma(2^a b) = 2 \cdot 2^a b = 2^{a+1} b
$$

Thus,

$$
(2^{a+1}-1)\sigma(b) = 2^{a+1} b
$$

Note that $2^{a+1} \mid (2^{a+1}-1)\sigma(b)$. As $(2^{a+1}, 2^{a+1}-1) = 1$ we have $2^{a+1} \mid \sigma(b)$. So we can write $\sigma(b) = 2^{a+1}c$ for some $c \in \mathbb{Z}, c > 0$. Substituting this we get,

$$
\begin{aligned}
(2^{a+1}-1)(2^{a+1}c) &= 2^{a+1} b \\
(2^{a+1}-1)c &= b
\end{aligned}
$$

We now show that $c = 1$. Suppose $c > 1$ then b has at least 3 distinct divisors namely $1, b, c$. Then $\sigma(b) \geq 1 + c + b$ however we also have $\sigma(b) = 2^{a+1}c = (2^{a+1} - 1 + 1)c = (2^{a+1}-1)c + c = b + c$. A contradiction. Thus we have $c = 1$ and,

$$
b = 2^{a+1} - 1
$$

and $\sigma(b) = b + 1$ thus b is prime. So we have $2^{a+1} - 1$ is prime. This implies that the exponent (a + 1) is also prime. And hence b is a mersenne prime and $n = 2^a(2^{a+1}-1)$.

($\Leftarrow$) Assume that $n = 2^{p-1}(2^p - 1)$ with both p and $2^p - 1$ both prime. Now,

$$
\begin{aligned}
\sigma(2^{p-1}(2^p-1)) &= \sigma(2^{p-1})\sigma(2^p-1) \\
&= \frac{2^p-1}{2-1}(2^p-1+1) \\
&= (2^p-1)(2^p) = 2 \cdot 2^{p-1}(2^p-1)
\end{aligned}
$$

□

3.4 The Möbius function

Definition. Let $n \in \mathbb{Z}, n > 0$ the Mobius function denoted (n) is defined as,

$$
\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some } p \\ (-1)^r & \text{if } n = p_1 \dots p_r \text{ where } p_i \text{ is distinct.} \end{cases}
$$

Example. Since $504 = 2^3 3^2 7$ and we have $\mu(504) = 0$ ◇

Theorem 3.13. $\mu(n)$ is multiplicative.

Proof. Let m, n by relatively prime positive integers. We need to show that $\mu(mn) = \mu(m)\mu(n)$. If m or n is 1 then it's clear. So assume that neither one is equal to 1. Note that m or n is divisible by a prime square if and only if mn is divisible by a prime square (as $(m, n) = 1$). In this case both $\mu(m)\mu(n)$ and $\mu(mn)$ are 0. Suppose now that m, n are products of distinct primes. So,

$$m = p_1, \dots, p_r, \quad n = q_1, \dots, q_s$$

Since $(m, n) = 1$ the entire set is distinct. Thus,

$$\mu(mn) = \mu(p_1 \dots p_r q_1 \dots q_r) = (-1)^{r+s} = -1^r - 1^s = \mu(m)\mu(n).$$

□

Proposition 3.14. Let $n \in \mathbb{Z}, n > 0$. Then,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases},$$

Proof. Since μ is multiplicative so is $F(n) = \sum_{d|n} \mu(d)$ by theorem 3.1. Thus we can calculate $F(n)$ by calculating $f(p^a)$ for prime powers.

$$\begin{aligned} F(p^a) &= \sum_{d|p^a} \mu(d) \\ &= \mu(1) + \dots + \mu(p^a) \\ &= \mu(1) + \mu(p) \\ &= \mu(1) + (-1) = 0 \end{aligned}$$

Also $F(1) = 1$. □

Theorem 3.15. (Mobius Inversion) Let f and g be arithmetic functions. Then,

$$f(n) = \sum_{d|n} g(d)$$

if and only if $g(n) = \sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(n/d) f(d)$

Proof. $(\Rightarrow)$ Assume $f(n) = \sum_{d|n} g(d)$. Then,

$$\sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(d) \sum_{a|n/d} f(a)$$

Note that $a \mid n/d$ if and only if $d \mid n/a$. So we have,

$$\sum_{a|n} g(a) \sum_{d|n/a} \mu(d) = \sum_{a|n} g(a) \begin{cases} 1 & \text{if } n = a \\ 0 & \text{otherwise} \end{cases} = g(n)$$

($\Leftarrow$) Assume that $g(n) = \sum_{d|n} \mu(d) f(n/d)$.

$$\begin{aligned}
\sum_{d|n} g(d) &= \sum_{d|n} \sum_{a|d} \mu(a) f(d/a) \\
&= \sum_{a|n} f(a) \sum_{d|n} \mu(d/a) \\
&= \sum_{a|n} f(a) \sum_{b|n/a} \mu(b) \\
&= f(n)
\end{aligned}$$

□

Example. By this theorem we have,

$$\sum_{d|n} \phi(d) = n$$

So by Mobius inversion,

$$\begin{aligned}
\phi(n) &= \sum_{d|n} \mu(d) n/d \\
&= n \sum_{d|n} \frac{\mu(d)}{d} \\
&= n \prod_{p^a|n} \sum_{d|p^a} \frac{\mu(d)}{d} \\
&= n \prod_{p|n} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

◇

Example. We have, $\tau(n) = \sum_{d|n} 1$ which is,

$$1 = \sum_{d|n} \tau(d)\mu(n/d) = \sum_{d|n} \tau(n/d)\mu(d)$$

◇

Example. We have $\sigma(n) = \sum_{d|n}, n = \sum_{d|n} \mu(d)\sigma(n/d)d$ ◇

Chapter 4

Quadratic Residues

4.1 Quadratic Residues

So far we have,

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

Now we're interested in quadratic congruences. Which is,

$$ax^2 + bx \equiv c \pmod{m}$$

Restrict to the case where p is an odd prime and,

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

Definition. Let $a, m \in \mathbb{Z}, m > 0$ and $(a, m) = 1$. Then a is a *quadratic residue* modulo m if the congruence,

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

has a solution. If there is no solution, then a is a *quadratic non-residue.*

Example. Quadratic residues mod 11,

$$\begin{aligned}
1^2 &\equiv 1 \pmod{11} \\
2^2 &\equiv 4 \pmod{11} \\
3^2 &\equiv 9 \pmod{11} \\
4^2 &\equiv 5 \pmod{11} \\
5^2 &\equiv 3 \pmod{11} \\
6^2 &\equiv 3 \pmod{11} \\
7^2 &\equiv 5 \pmod{11} \\
8^2 &\equiv 5 \pmod{11} \\
9^2 &\equiv 4 \pmod{11} \\
10^2 &\equiv 1 \pmod{11}
\end{aligned}$$

The quadratic residues are $\{1, 3, 4, 5, 9\}$ and non-residues are $\{2, 6, 7, 8, 10\}$ $\diamond$

Proposition 4.1. Let p be an odd prime and $a \in \mathbb{Z}, p \nmid a$. Then,

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

has either 0 or 2 incongruent solutions.

Proof. Assume $x^2 \equiv a \pmod p$ has a solution $x = x_0$ then $-x_0$ is also clearly a solution. And we have $x_0 \equiv -x_0 \pmod p$. Suppose for contradiction $x_0 \equiv -x_0 \pmod p$, then $2x_0 \equiv 0 \pmod p$ so $p \mid 2$ or $p \mid x_0$ but as p is odd we have $p \mid x_0$ which makes it not coprime so $x_0 \equiv 0 \pmod p$ a contradiction.

Thus $x^2 \equiv a \pmod p$ has at least two incongruent solutions modulo p if it has a single solution.

Now to show it has at most two solutions. Suppose x_0, x_1 are two solutoins, then,

$$x_0^2 \equiv x_1^2 \equiv a \pmod p$$

Then $x_0^2 - x_1^2 \equiv 0 \pmod p$ which means that $p\ mid x_0^2 - x_1^2 = (x_0 + x_1)(x_0 - x_1)$ which means $p \mid x_0 + x_1$ or $p \mid x_0 - x_1$ which means either $x_0 \equiv x_1 \pmod p$ or $x_0 \equiv -x_1 \pmod p$. Which means we have at most two solutions. □

Corollary 4.2. Let p be an odd prime and $a \in \mathbb{Z}, p \mid a$. If $x^2 \equiv a \pmod p$ is solvable with $x = x_0$, then the two solutions are x_0 and $p - x_0$.

Proposition 4.3. Let p be an odd prime. There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p.

Proof. Consider,

$$\begin{aligned} x &: 1, 2, 3 \ldots, p-1 \\ a &: 1, 2, 3, \ldots, p-1 \end{aligned}$$

For each $1 \le x \le p-1$, if $x^2 \equiv a \pmod p$ then $-x^2 \equiv a \pmod p$ and these are the only two such residues. That is, for each pair $(1, p-1), (2, p-2), \ldots, (i, p-i)$, $1 \le i \le \frac{p-1}{2}$, we get a unique quadratic residue, namely i^2. Since there are $\frac{p-1}{2}$ pairs of residues mod p farmed in this way, there are exactly $\frac{p-1}{2}$ quadratic residues modulo p. These can be represented by

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

□

4.2 The Legendre Symbol

Let p be an odd prime $a \in \mathbb{Z}, p \nmid a$. The Legendre symbol, denoted $\frac{a}{p}$, is,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue modulo p} \\ -1 \text{ if } a \text{ is a quadratic non-residue modulo p} \end{cases}$$

Example. $1, 3, 4, 5, 9$ are quadratic residues modulo 11. So,

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \cdots = \left(\frac{9}{11}\right) = 1$$

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \cdots = \left(\frac{10}{11}\right) = -1$$

◇

Example. Evaluate $\left(\frac{3}{7}\right)$. We need to check if there is a solution $x^2 \equiv 3 \pmod 7$. We have,

$$1^2 \equiv 1 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$

So we see that 3 is not a quadratic residue modulo 7 and hence $\left(\frac{3}{7}\right) = -1$ ◇

Exercise. Find all the quadratic residues modulo 23. We need,

$$x^2 \equiv a \pmod 2 3$$

1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6

Theorem 4.4 (Euler's Criterion)**.** Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then,

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

Proof. Suppose that $\left(\frac{a}{p}\right) = 1$. Then we have,

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

has a solution for some $x = x_0$. So we have,

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$$

Now let $\left(\frac{a}{p}\right) = -1$ so a is not a quadratic residues mod p. Since $p \nmid a$ for each $1 \le i \le p-1$ the congruence $ij \equiv a \pmod p$ has a solution j with $1 \le j \le p-1$. We have $\neq j$ as otherwise a is a quadratic residues.

Thus we can pair the residues $1, 2, \ldots, p-1$ into $\frac{p-1}{2}$ pairs (i, j) such that ,

$$ij \equiv a \pmod p$$

So this gives us,

$$12 \ldots (p-1) \equiv (p-1)! \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

by Wilson's theorem. □

Example. Calculate $\left(\frac{3}{7}\right)$. We have,

$$\left(\frac{3}{7}\right) \equiv 3^3 \equiv 27 \equiv -1 \pmod 7$$

◇

Proposition 4.5. Let p be an odd prime with $a, b \in \mathbb{Z}$ such that $p \nmid a$ and $p \nmid b$. Then,

1. $\left(\frac{a^2}{p}\right) = 1$
2. If $b \equiv a \pmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof. 1. We have $a^2 \equiv x^2 \pmod{p}$ has a solution $x = a$.

2. The congruence $x^2 \equiv a \pmod{p}$ is solvable if and only if $x^2 \equiv b \equiv a \pmod{p}$ is solvable.

3. By Euler's criterion we have,

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

Since the only values are ± 1 the congruence implies equality. $\square$

4.2.1 Further Properties

If $a = \pm 2^{a_0} p_1^{a_1} \dots p_r^{a_r}$, then

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{a_0}\left(\frac{p_1}{p}\right)^{a_1} \cdots \left(\frac{p_r}{p}\right)^{a_r}$$

To evaluate $\left(\frac{a}{p}\right)$ we only need to understand $\pm 1, 2, p_1, \dots, p_r$ over p.

Theorem 4.6. Let p be an odd prime. Then $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p = 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$

Proof. The first equivalence follows from Euler's Criterion. For the second we compute. If $\equiv 1 \pmod{4}$ then $p = 1 + 4k$ for some $k \in \mathbb{Z}$ so,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{4k} \equiv (-1)^{2k} \equiv 1 \pmod{p}$$

Similarly if $p = 3 + 4k$ then,

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

$\square$

Lemma 4.7 (Gauss' Lemma)**.** Let p be an odd prime and let $a \in \mathbb{Z}, p \nmid a$. Let n be the number of least positive residues of the integers in,

$$a, 2a, 3a, \dots, \frac{(p-1)}{2}a$$

that are greater than $\frac{p}{2}$. Then we have,

$$\left(\frac{a}{p}\right) = (-1)^n$$

Proof. Let $r_1, \dots, r_n$ be the least positive residues among $a, 2a, \dots, \frac{p-1}{2}a$ greater than $\frac{p}{2}$ and let $s_1, \dots, s_m$ be the ones less than $\frac{p}{2}$. Note, none of the r_i, s_j are 0 mod p. Consider the $\frac{p-1}{2}$ integers given by the following list,

$$p - r_1, p - r_2, \dots, p - r_n, s_1, \dots, s_m$$

This is the set of residues $1, 2, \dots, \frac{p-1}{2}$ in some order. All elements satisfy ≥ 1 and are less than equal to $\frac{p-1}{2}$ since they are all less than $\frac{p}{2}$. Thus it suffices to show that there are no duplicates. If $p - r_i \equiv p - r_j \pmod{p}$ then $r_i \equiv r_j \pmod{p}$ so $r_i = r_j$ but that means that $ak_i \equiv ak_j \pmod{p}$ but as $(a, p) = 1$ we have $k_i = k_j$ but they are distinct.

By a similar argument there is not repetition among the s_j. The only other possibility is to have $p - r_i \equiv s_j \pmod{p}$. This is,

$$-k_i a \equiv k_j a \pmod{p}$$

for some $1 \leq k_i, k_j \leq \frac{p-1}{2}$. So we have $-k_i \equiv k_j \pmod{p}$. But we have $p - k_i \geq p/2 > \frac{p-1}{2} > k_j$ so the congruence is impossible. So the list is just,

$$1, 2, \dots, \frac{p-1}{2}$$

Thus multiplying them we have,

$$\begin{aligned}
1 \cdot 2 \dots \frac{p-1}{2} &\equiv \frac{(p-1)}{2}! \pmod{p} \\
(-1)^n r_1 \dots r_n s_1 \dots s_m &\equiv \frac{p-1}{2}! \pmod{p} \\
(-1)^n (a)(2a) \dots (\frac{p-1}{2} a) &\equiv \frac{p-1}{2}! \pmod{p} \\
(-1)^n a^{\frac{p-1}{2}} \frac{(p-1)!}{2} &\equiv \frac{(p-1)!}{2} \pmod{p} \\
(-1)^n a^{\frac{p-1}{2}} &\equiv 1 \pmod{p} \\
a^{\frac{p-1}{2}} &\equiv (-1)^n \pmod{p} \\
\left(\frac{a}{p}\right) &\equiv (-1)^n \pmod{p}
\end{aligned}$$

and $\left(\frac{a}{p}\right) = (-1)^n$ □

Exercise. Calculate, $\left(-\frac{1}{13}\right), \left(\frac{2}{17}\right), \left(-\frac{14}{1}\right), \left(\frac{18}{23}\right)$

Theorem 4.8. Let p be an odd prime. Then,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8} \\ -1 & \text{if } p \equiv 3, 5 \pmod{8} \end{cases}$$

Proof. By Gauss' Lemma, we have $\left(\frac{2}{p}\right) = (-1)^n$ where n is the nmber of least positive residues of,

$$2, 2 \cdot 2, 3 \cdot 2, \dots, \frac{p-1}{2} \cdot 2$$

Let $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{p-1}{2}$. Note, $2k < \frac{p}{2}$ if and only if $k < \frac{p}{4}$, so there are $\lfloor \frac{p}{4} \rfloor$ values of k for which $2k < \frac{p}{2}$. Thus, there are $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$ values of k for which $2k > \frac{p}{2}$. Thus we have $n = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$. To show that $\frac{p^2-1}{8}$ and $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$ always have the same parity. Consider the four cases, $p \equiv 1, 3, 5, 7 \pmod{8}$.

1. For $p \equiv 1 \pmod{8}$. We have $p = 8m + 1$ for some $m \in \mathbb{Z}$. So we have $\frac{p-1}{2} = \frac{8m}{2} = 4m$ and

$\frac{p}{4} = 2m + \frac{1}{4}$ whose floor is $2m$. So we have $4m - 2m = 2m$ which is even. Now $\frac{p^2-1}{8}$ is even as well.

2.
3.
4.
Finally, the last equality follows by a similar case analysis.

□

Example. For $\left(\frac{2}{23}\right)$ is $(-1)^{\frac{23^2-1}{8}} = 1$ ◇

4.3 Quadratic Reciprocity

Theorem 4.9 (Law of Quadratic Reciprocity)**.** Let p, q be odd distinct primes. Then,

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

Remark. Q.R siplifies the calculation of $\left(\frac{p}{q}\right)$

Remark. Which primes are quadratic residues mod 17, i.e eval p such that $\left(\frac{p}{17}\right) = 1$ (note that this has a finite solution for p). Now consider for which primes p is 17 a quadratic residue for. (Here we have infinite possibilities for p).

Example. Compute $\left(\frac{7}{53}\right)$. We have $53 \equiv 1 \pmod 4$ so we get $\left(\frac{7}{53}\right)\left(\frac{53}{7}\right) = 1$. So both have to be equal which we get as,

$$\left(\frac{7}{53}\right) = \left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = 1$$

◇

Example. Compute $\left(\frac{-158}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{158}{101}\right) = 1 \cdot \left(\frac{158}{101}\right) = \left(\frac{57}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{19}{101}\right)$.

We have $101 \equiv 1 \pmod 4$ so we have, the above is equal to,

$$\begin{aligned} \left(\frac{-158}{101}\right) &= \left(\frac{101}{3}\right)\left(\frac{101}{19}\right) \\ &= \left(\frac{2}{3}\right)\left(\frac{6}{19}\right) \\ &= (-1)(-1)(-\left(\frac{19}{3}\right)) \\ &= -1 \end{aligned}$$

◇

Lemma 4.10. Let p be an odd prime. Let $a \in \mathbb{Z}, p \nmid a$ and a is odd. Let,

$$N = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor$$

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

Example. Consider $\left(\frac{7}{11}\right)$. Here we have,

$$N = \sum_{j=1}^{5} \left\lfloor \frac{7j}{11} \right\rfloor = 0+1+1+2+3 = 7$$

And we have $(-1)^7 = -1$ ◇

Proof. Let $r_1, r_2, \ldots, r_n$ be the least non-negative residues of $a, 2a, \ldots, \frac{p-1}{2}a$ that are $> \frac{p}{2}$. Likewise, let $s_1, \ldots, s_m$ be the remaining residues that are $< \frac{p}{2}$. Note $r_1, \ldots, r_n, s_1, \ldots, s_m$ are all distinct mod p as they come from $a, 2a, \ldots, \frac{p-1}{2}$. This means the fractions $\frac{r_i}{p}, \frac{s_j}{p}$ are also all distinct. Then,

$$\begin{aligned} ja &= p - \frac{ja}{p} \\ &= p\left(\left\lfloor \frac{ja}{p} \right\rfloor + \frac{remainder}{p}\right) \\ &= p\left\lfloor \frac{ja}{p} \right\rfloor + remainder \end{aligned}$$

here the remainders are exaclty $r_1, \ldots, r_n, s_1, \ldots, s_m$. So we have,

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum r_i + \sum s_j$$

Note also that,

$$\begin{aligned} \sum_{j=1}^{\frac{p-1}{2}} j &= \sum_{j=1}^{\frac{p-1}{2}} (p - r_i) + \sum s_j \\ &= p_n - \sum r_i + \sum s_j \end{aligned}$$

Note, subtracting this from above we have,

$$\begin{aligned} \sum_j ja - \sum_j j &= \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum r_i + \sum s_j - (p_n - \sum r_i + \sum s_j) \\ &= \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - p_n + 2\sum r_i \end{aligned}$$

Now since a is odd we have,

$$\sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor - pn \equiv 0 \pmod 2$$

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

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

So $N \equiv npmodn$ and hence we have $(-1)^N = (-1)^n$ so by gausses we have,

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

$\square$

Proof. of Theorem 4.9
Without loss of generality, assume $p > q$. Consider the picture, the number of lattice points in the rectangle OABC. This is clearly $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

1. The line ON has slope $\frac{q}{p}$. In particular, ON contains no lattice points.

2. The y-coordinate of M is $\frac{p-1}{2} \cdot \frac{q}{p} = \frac{q}{2} - \frac{q}{2p}$. This lies between the consecutive integers are $\frac{q-1}{2}$ and $\frac{q+1}{2}$. We have,

$$\frac{q-1}{2} = \frac{q}{2} - \frac{1}{2} < \frac{q}{2} - \frac{q}{2p} < \frac{q}{2} < \frac{q+1}{2}$$

The number of lattice points in the rectangle OABC, not on the axis and below ON is,

$$N_1 = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$$

Likewise, the number of lattice points above ON is,

$$N_2 = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$$

Thus, the total number of lattice points in question is $N_1 + N_2 = \frac{p-1}{2} \cdot \frac{q-1}{2}$.

From Lemma 4.10 we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{N_2}(-1)^{N_1} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ $\square$

Characterizing Particular Primes

Note, we have characterized the primes for which -1 and 2 are quadratic residues.

Example. For primes is 3 a quadratic residues. So for what p is $\left(\frac{3}{p}\right) = 1$.

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

2. Tabulate quadratic residues and quadratic non-residues mod 3. We have $1^2 = 1, 2^2 = 1 \pmod 3$. So only quadratic resiude is 1.

3. Analyze cases,
Suppose $p \equiv 1 \pmod 4$. Then, $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \pmod 3$

Suppose $p \equiv 3 \pmod 4$. Then, $\left(\frac{p}{3}\right) = -1$ if $p \equiv 2 \pmod 3$.

4. Chinese remainder theorem,
In case 1 we have $p \equiv 1 \pmod 4, p \equiv 1 \pmod 3$ and case 2 we have $p \equiv 3 \pmod 4, p \equiv 2 \pmod 3$.

For case 1 we get $p \equiv 1 \pmod{12}$ and for case 2 we have $p = 3 \cdot 3 \cdot \overline{3} + 2 \cdot 4 \cdot \overline{4} = -1$.

5. We have $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$ $\diamond$

Example. Characterize the primes p for which both 2 and 3 are quadratic residues. So we want p such that,

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

We have $\left(\frac{2}{p}\right) \equiv 1$ if $p \equiv \pm 1 \pmod 8$ and $\left(\frac{3}{p}\right) \equiv 1$ iff $p \equiv \pm 1 \pmod{12}$. This is equivalent to $p \equiv \pm 1 \pmod{24}$ $\diamond$

Example. Characterize the primes p for which 13 is a quadratic residue. So we want p such that,

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

We have $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right)$. Now we need to find squares modulo 13 which is $1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 3, 5^2 = 12, 6^2 = 10$. 13 is a quadratic residue mod p if and only if $p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$ $\diamond$

Chapter 5

Primitive Roots

5.1 Order of an Integer, Primitive Roots

Let m be a positive integer and $(a, m) = 1$. By Eulers theorem we have,

$$a^{\phi(n)} \equiv 1 \pmod{m}$$

However, it may happen that $a^g \equiv 1 \pmod{m}$ for some smaller g.

Definition (order)**.** Let $a, m \in \mathbb{Z}$ with $m > 0, (a, m) = 1$. Then the *order of a modulo m*, denoted $ord_m a$, is the least positive integer n such that,

$$a^n \equiv 1 \pmod{m}$$

Example. We have $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1 \pmod{7}$ so $ord_7 2 = 3$. And Euler's tells us that

$$ord_7 2 \leq \phi(7) = 6$$

◇

Example. Consider $ord_7 3$, we have $ord_7 3 = 6$ ◇

Proposition 5.1. Let $a, m \in \mathbb{Z}, m > 0, (a, m) = 1$. Then $a^n \equiv 1 \pmod{m}$ for some positive integer n if and only if $ord_m a \mid n$. In particular,

$$ord_m a \mid \phi(m)$$

Proof. ($\Rightarrow$) Suppose $a^n \equiv 1 \pmod{m}$. By the division algorithm we have $q, r \in \mathbb{Z}$ such that,

$$n = q(ord_m a) + r, \quad 0 \leq r < ord_m a$$

Then,

$$\begin{aligned} a^n \equiv a^{q(ord_m a)+r} &\equiv (a^{ord_m a})^q a^r \pmod{m} \\ &\equiv 1 \cdot a^r \equiv 1 \pmod{m} \end{aligned}$$

So we have $a^r \equiv 1 \pmod{m}$. Thus $r = 0$ by definition of $ord_m a$ and $0 \leq r < ord_m a$. Therefore $ord_m a \mid n$.

($\Leftarrow$) Suppose $ord_m a \mid n$. Then $n = qord_m a$, and $a^n \equiv a^{qord_m a} = (a^{ord_m a})^q \equiv 1 \pmod m$ □

Example. By the above proposition we only need to check the divisor of $\phi(n)$ to find the order. We have that $ord_7 2 \mid \phi(7) = 6$, so $ord_7 2$ can only be $1, 2, 3, 6$.

◇

Example. Consider $ord_{13} 2 \mid \phi(13) = 12$, so,

$$ord_{13} 2 = 1, 2, 3, 4, 6, 12$$

Out of these we check and find $2^{12} \equiv 1 \pmod{13}$. ◇

Proposition 5.2. Let $a, m \in \mathbb{Z}, m > 0, (a, m) = 1$. If i, j are non-negative integers then,

$$a^i \equiv a^j \pmod m$$

if and only if,

$$i \equiv j \pmod{ord_m a}$$

Proof. Without loss of generality suppose $i > j$.
($\Rightarrow$) Assume $a^i \equiv a^j \pmod m$. Then,

$$a^i \equiv a^j a^{i-j} \equiv a^j \pmod m$$

We can multiple the inverse of a^j from both sides as $(a, m) = 1$. So we have,

$$\begin{aligned} a^{i-j} a^j &\equiv a^j \pmod m \\ a^{i-j} &\equiv 1 \pmod m \end{aligned}$$

By Prop 5.1 we have $ord_m a \mid i - j$ or that $i \equiv j \pmod{ord_m a}$

($\Leftarrow$) Assume that $i \equiv j \pmod{ord_m a}$. Then $ord_m a \mid i - j$ so we have some k such that $i - j = kord_m a$. Thus we have $i = j + kord_m a$. And we get,

$$\begin{aligned} a^i &\equiv a^{j + kord_m a} \pmod m \\ &\equiv a^j a^{ord_m a k} \pmod m \\ &\equiv a^j 1 \pmod m \end{aligned}$$

So we have $a^i \equiv a^j \pmod m$ □

Example. We've seen that $ord_7 2 = 3$. So if i, j are non-negative integers such that $2^i \equiv 2^j \pmod 7$, then $i \equiv j \pmod 3$. Note that,

$$2000 \equiv 2 \pmod 3$$

Thus $2^{2000} \equiv 2^2 = 4 \pmod 7$ ◇

Definition. Let $r, m \in \mathbb{Z}$ with $m > 0, (r, m) = 1$. Then r is called a *primitive root* modulo m if $ord_m r = \phi(m)$

Example. 3 is a primitive root modulo 7, as $ord_7 3 = \phi(7)$. And 2 is a primitive root modulo 13. ◇

Example. Prove that there are no primitive roots modulo 8. The reduced residues are,

$$1, 3, 5, 7$$

Also $\phi(8) = 4$. So we have $1^1 \equiv 1, 3^2 = 5^2 = 7^2 \equiv 1 \pmod 8$. So none of them are primitive roots modulo 8.

$\diamond$

Note. Not all integers m posses a primitive root. The Primitive Root Theorem tells us which m have a primitive root.

Proposition 5.3. Let r be a primitive root. Then the set,

$$\{r, r^2, r^3, \ldots, r^{\phi(m)}\}$$

is a set of reduced residues.

Note. This says that a primitive root when it exists generates the reduced residues modulo m.

Proof. Since r is a primitive root we have $(r, m) = 1$ and so $(r^n, m) = 1$ for any $n \geq 1$ and there are $\phi(m)$ elements. So it remains to show that they are distinct modulo m.

Suppose $r^i \equiv r^j \pmod m$ for some $1 \leq i, j \leq j$. Then Prop 5.2 implies that $i \equiv j \pmod \phi)(m)$ so as $i, j < \phi(m)$ we have $i = j$. $\square$

Example. 3 is a primitive root modulo 7. We have,

$$\{3^1, 3^2, 3^3, \ldots, 3^6\} = \{3, 2, 6, 4, 5, 1\}$$

$\diamond$

Note. If a primitive root exists it is in general not unique. If it exists we have $\phi(\phi(m))$. Note that every reduced residue class's generators that are cyclic are a primitive root (i think)

Example. Show there are no primitive roots modulo 12. 5,7,11
5 25 - 1 = 24
7, 49 - 1 = 48
11, 121 -1 = 120 $\diamond$

Proposition 5.4. Let $a, m \in \mathbb{Z}, m > 0, (a, m) = 1$. If i is a positive integer, then,

$$ord_m(a^i) = \frac{ord_m a}{(ord_m a, i)}$$

Proof. Let $d = (ord_m a, i)$ so we have some $b, c \in \mathbb{Z}$ such that $ord_m a = db, i = dc$ and $(b, c) = 1$. Note,

$$\begin{aligned}(a^i)^b \equiv (a^{dc})^{\frac{ord_m a}{d}} &\equiv a^{c\ ord_m a} \\ &\equiv 1^c \pmod m\end{aligned}$$

By Proposition 5.1, $ord_m(a^i) \mid b$. Now,

$$a^{i(ord_m a^i)} \equiv a^{iord_m(a^i)} \equiv 1 \pmod m$$

By Proposition 5.1 we know that $ord_m a \mid i_m(a^i)$. Thus,

$$db \mid dcord_m(a^i), \text{ so } b \mid cord_m(a^i)$$

But $(b, c) = 1$ we have $b \mid ord_m a^i$ but we also have $ord_m a^i \mid b$ so we have $ord_m a^i = b$ which means that,

$$ord_m(a^i) = b = \frac{ord_m a}{d} = \frac{ord_m a}{(ord_m a, i)}$$

□

Corollary 5.5. Let $a, m \in \mathbb{Z}, m > 0, (a, m) = 1$. If i is a positive integer then,

$$ord_m(a^i) = ord_m(a)$$

if and only if $(ord_m a, i) = 1$

Corollary 5.6. If a primitive root modulo m exists, then there are exactly $\phi(\phi(m))$ incongruent primitive roots modulo m.

Proof. Let r be a primitive root. Then $ord_m r = \phi(m)$. By prop 5.3, then set,

$$r^1, r^2, \ldots, r^{\phi(m)}$$

is a reduced residue system modulo m. If $1 \leq i \leq \phi(m)$, then, $ord_m(r^i) = ord_m r = \phi(m)$ if and only if $(i, \phi(m)) = 1$. That is, there are $\phi(\phi(m))$ such i, and each gives a distinct primitive root. □

Example. We showed that 3 is a primitive root modulo 7. There are exactly $\phi(\phi(7)) = \phi(6) = 2$ primitive roots. In particular the other one must have,

$$ord(3^i) = 6 \Leftrightarrow (i, 6) = 1$$

Thus $i = 1, 5$ so we have $3^1 \equiv 3 \pmod 7, 3^5 \equiv 5 \pmod 7$. So our primitive roots are $3, 5$. ◇

Example. 2 is a primitive root modulo 13. Thus there are $\phi(\phi(13)) = \phi(12) = 4$. ◇

Note. We have $\phi(\phi(8)) = 2$ but this does not mean that 8 has 2 primitive roots as 8 doesn't have 1 to begin with.

5.2 Primitive roots for Primes numbers

The following theorem of Lagrange is analogous to the fundamental theorem of algebra.

Theorem 5.7 (Lagrange)**.** Let p be a prime and let,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

be a polynomial with degree n and integer coefficients given by $a_0, a_1, \ldots, a_n$ such that $p \mid a_n$. Then the congruence

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

has at most n solutions.

Proof. Proceed by induction on n. For $n = 1$. Then $f(x) = a_1 x + a_0$ where $p \nmid a_1$. So then,

$$a_1 x + a_0 \equiv 0 \pmod p \Leftrightarrow a_1 x \equiv -a_0 \pmod p$$

Since $p \nmid a_1$ it's inverse exists and there is exactly one solution,

$$x \equiv -a_0 \overline{a_1} \pmod p$$

Suppose $n = k \geq 1$ and the theorem holds for this case. Now Suppose $n = k + 1$, then,

$$f(x) = a_{k+1}x^{k+1} + \cdots + a_0$$

where $p \nmid a_{k+1}$. Now if $f(x) \equiv 0 \pmod{p}$ has no solutions, then we're done. Suppose that y is a solution. By polynomial long division, there exists a polynomial $q(x)$ with integer coefficients such that,

$$f(x) = (x - x_0)q(x) + r$$

For some integer r where $q(x)$ has degree k. Note,

$$0 = f(x_0) \equiv (x_0 - x_0)q(x_0) \equiv r \pmod{p}$$

So $r \equiv 0 \pmod{p}$ and,

$$f(x) \equiv (x - x_0)q(x) \pmod{p}$$

Now if $0 \equiv f(x_1) \equiv (x_1 - x_0)q(x_1) \pmod{p}$. So we have either $p \mid (x_1 - x_0)$ or $p \mid q(x_1)$. So if $x_1 \not\equiv x_0 \pmod{p}$ then $q(x_1) \equiv 0 \pmod{p}$ and $q(x_1)$ has at most k roots. Thus $f(x)$ has at most $k + 1$ roots. □

Proposition 5.8. Let p be a prime and let $d \in \mathbb{Z}$ that is positive and $d \mid p - 1$. Then the congruence,

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d in congruent solutions modulo p.

Remark. This is a generalization of the case where $d = 2$ where $x^2 \equiv 1 \pmod{p}$ has exactly two solutions 1 and -1, for odd primes p.

Proof. Since $d \mid p - 1$, there exists $e \in \mathbb{Z}$ such that $p - 1 = de$. Note that if $p \nmid x$, then $0 \equiv x^p - 1 = x^{de} - 1 = (x^d - 1)(x^{e-1} + x^{d(e-2)} + \cdots + x^d + 1) \pmod{p}$.

Thus either $x^d - 1 \equiv 0 \pmod{p}$ or $(x^{d(e-1)} + \ldots 1) \equiv 0 \pmod{p}$. By theorem 5.7, (2) has at most $d(e - 1) = (p - 1) - d$ solutions and (1) has at most d solutions. But $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ solutions. So $x^d - 1 \equiv 0 \pmod{p}$ has at least d solutions. Therefore it has exactly d solutions. □

Example. To show that 3 is a primitive root modulo 43 and use this to calculate all elements of order 14.

To show that 3 is a primitive root, need to check 3^i for $i \mid \phi(43) = 42$. So $i = 1, 2, 3, 6, 7, 14, 21, 42$. So have,

$$3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 27, 3^6 \equiv -2, 3^7 \equiv -6, \ldots, 3^{42} \equiv 1$$

So 3 is a primitive root as it's 1 only for 42.

Now we want i such that,

$$14 = ord_{43}(3^i) = \frac{ord_{43}3}{ord_{43}3, i} = \frac{42}{(42, 1)}$$

So, $(42, i) = 3$. The values of i are $3, 9, 15, 27, 33, 39$. The elements with order 14 are represented by $3^3, 3^9, \ldots, 3^{39}$. ◇

Theorem 5.9. Let p be a prime and $d \in \mathbb{Z}, d > 0, d \mid p - 1$. Then there are exactly $\phi(d)$ incongruent integers having order d modulo p.

Proof. Given $d \mid p-1$, let $f(d)$ be the number of integers among $1, 2, \ldots, p-1$ that have order d modulo p. We wish to show that $f(d) = \phi(d)$

We'll first who that if $f(d) \neq 0$, then $f(d) = \phi(d)$. Then we'll show that $f(d) \neq 0$ for all $d \mid p-1$.

Suppose that $f(d) > 0$. There exists a with order d. Note, the integers $a^1, a^2, \ldots, a^d$ are incongruent modulo p as if they were congruent i.e $a^i \equiv a^j \pmod{p}$ for some $i > j$ then $a^{i-j} \equiv 1 \pmod{p}$, but $i - j < d$, contradicting ${}_pa = d$. Note that $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p}$ so each is a solution of $x^d - 1 \equiv 0 \pmod{p}$. Since this congruence has exactly d solutions, these are given by $a^1, a^2, \ldots, a^d$. Any integer has order d modulo p must be congruent to one of these. Point is any element of order d must be a power of a.

Recall Prop 5.4, $ord_p(a^i) = \frac{ord_p a}{(ord_p a, i)}$. Thus $ord_p(a^i) = d$ if and only if $\frac{ord_p(a)}{(ord_p(a), i)} = d$ but we know $ord_p a = d$ so this means that $(ord_p a, i) = 1$ or $(d, i) = 1$ thus there are exactly $\phi(d)$ values of i which satisfy this. Hence we have $f(d) = \phi(d)$

We show that now $f(d)$ cannot be 0. Note that any integer b with $1 \leq b \leq p-1$ must have an order that divides $p-1$. Thus any such b is counted by exactly $f(d)$. Thus,

$$\sum_{d \mid p-1} f(d) = p - 1 = \sum_{d \mid p-1} \phi(d) \quad \text{from prev proposition}$$

Rearranging $\sum_{d \mid p-1} (\phi(d) - f(d)) = 0$. If $f(d) \neq 0$. Now if $f(d) \neq 0$ then we have $f(d) = \phi(d)$. In this case we have $\phi(d) - f(d) = 0$. Thus,

$$0 = \sum_{d \mid p-1} \phi(d)$$

for some d. But $\phi(d)$ is non-negative and hence there are no d such that $f(d) = 0$ and therefore $f(d) = \phi(d)$ for all $d \mid p-1$. □

Corollary 5.10. Let p be a prime. Then there are exactly $\phi(p-1)$ primitive roots modulo p .

Note. The theorem gives no way to construct these primitive roots.

Example. Let $p = 7$. Theorem 5.9 implies that there exists residues of orders $1, 2, 3, 6$ since $\phi(7)$ is 6. ◇

Exercise. Construct table w order and residues for $p = 13$. We have $\phi(13) = 12$ and orders dividing 12 are $1, 2, 3, 4, 6, 12$.

Example. Find all incongruent integers having order $6, 7$ modulo 19. Note there are 0 with order 7 as $7 \nmid 19 - 1 = 18$. To find elements of order 6 we need a primitive root.

To show that 2 is a primitive root. By prop 5.1, we need to check that $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^6 = 7, 2^9 = 18, 2^{18} = 1$. So 2 is a primitive root. Thus 2 is a primitive root.

Now to find the integers w order 6 we calculate $6 = ord_{19}(2^a) = \frac{ord_{19} 2}{(ord_{19} 2, a)} = \frac{18}{(18, a)}$. Thus $(18, a) = \frac{18}{6} = 3$. Thus $a = 3, 15$ and $2^3 = 8$ and $2^{15} = 2^{72} \cdot 2 = 3$. Thus $3, 8$ have order 6 modulo 19.

◇

The frequency with which 2 appears as a primitive root motivates the following conjecture.

Conjecture: There are infinitely many primes p for which 2 is a primitive root modulo p.

Conjecture: If r is any non-square integer other than -1, the there are infinitely many primes p for which r is a primitive root.

Heath-Brown proved in 1986 that there are at most two integers r for which the conjecture is false.

5.3 Primitive Root Theorem

The following two propositions, limit the cases we consider.

Proposition 5.11. There are no primitive roots modulo 2^n where $n \geq 3 \in \mathbb{Z}$.

Proof. Note that any primitive root modulo 2^n must be odd and have $\phi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$. Let a be an odd integer. To prove that there are no primitive roots, it suffices to show that $a^{2^{n-2}} \equiv 1 \pmod 2^n$.

Do induction on n. Base case $n = 3$. Note for $a = 1, 3, 5, 7$ numbers coprime to 8 squared are equal to 1. This gives the base case.

Now suppose that $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ for some $n \geq 3$. We'll show the same congruence with $n + 1$ in place of n. Now by assumption we have,

$$a^{2^{n-2}} = b \cdot 2^n + 1$$

Note that squaring yields $a^{2^{n-1}} = b^2 2^{2n} + 1 + b2^{n+1}$

$$\begin{aligned} a^{2n-1} &= b^2 2^{2n} + 1 + b2^{n+1} \\ &= 2^{n+1}(b^2 2^{n-1} + b) + 1 \\ &= 2^{n+1}k + 1 \end{aligned}$$

So we have $a^{2^{n-1}} \equiv 1 \pmod 2^{n+1}$ □

5.4 Index Arithmetic and Power Residues

Recall if r is a primitive root mod m, then the set,

$$\{r, r^2, r^3, \ldots, r^{\phi(m)}\}$$

is a reduced residue system.

Definition. Let r be a primitive root modulo m. If $(a, m) = 1$, then the *index of a relative to r*, denoted $ind_r a$, is the least positive integer n for which,

$$r^n \equiv a \pmod m$$

Note. The $ind_r a$ always exists and satisfies $1 \leq ind_r a \leq \phi(m)$.

Example. 3 is a primitive root modulo 7. So we have,

$$3^1 \equiv 3, \ldots, 3^6 \equiv 1 \pmod 7$$

So we have $ind_3 3 = 1, ind_3 2 = 2, \ldots, ind_3 1 = 6$ ◇

If a, b are co prime to m and $a \equiv b \pmod m$ then,

$$ind_r a = ind_r b$$

Indices enjoy properties of logarithms,

Proposition 5.12. Let r be a primitive root modulo m and $a, b \in \mathbb{Z}$ s.t $(a, b) = 1$. We have the following,

1. $ind_r 1 \equiv 0 \pmod{\phi(m)}$
2. $ind_r r \equiv 1 \pmod{\phi(m)}$
3. $ind_r(ab) \equiv ind_r a + ind_r b \pmod{\phi(m)}$
4. $ind_r(a^n) \equiv n\ ind_r a \pmod{\phi(m)}$

Proof. (a) and (b) are clear. For (c), by definition we have,

$$r^{ind_r a} \equiv a \pmod{m} \text{ and } r^{ind_r b} \equiv b \pmod{m}$$

So we have,

$$r^{ind_r a + ind_r b} \equiv ab \equiv r^{ind_r(ab)} \pmod{m}$$

Now using Prop 5.2 we have $ind_r a + ind_r b \equiv ind_r(ab) \pmod{\phi(m)}$

For (d) we have by definition,

$$r^{ind_r(a^n)} \equiv a^n \pmod{m} \text{ and } r^{n ind_r a} \equiv r^{ind_r a n} \equiv a^n \pmod{m}$$

So again by Prop 5.2 we have,

$$n\ ind_r a \equiv ind_r(a^n) \pmod{\phi(m)}$$

□

Example. Working mod 7 with primitive root 3.

We have $ind_3 2 = 2, ind_3 3 = 1$ so $ind_3 6 \equiv ind_3(2 \cdot 3) = ind_3(2) + ind_3(3) = 3 \pmod{6}$

◇

Suppose r is a primitive root modulo m and $(a, m) = (b, m) = 1$ and consider for $n > 0$,

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

The congruence above is equivalent to,

$$ind_r(ax^n) \equiv ind_r b \pmod{\phi(m)}$$

So can write this as,

$$\begin{aligned} ind_r(a) + n\ ind_r(x) &\equiv ind_r(b) \pmod{\phi(m)} \\ n\ ind_r(x) &\equiv ind_r(b) - ind_r(a) \pmod{\phi(m)} \end{aligned}$$

Example. Find solutions to,

$$6x^4 \equiv 3 \pmod{7}$$

As 3 is a primitive root we have,

$$\begin{aligned} &4\ ind_3(x) \equiv ind_3(3) - ind_3(6) \pmod{6} \\ &4\ ind_3(x) \equiv 4 \pmod{6} \end{aligned}$$

We can rewrite this as,

$$2y \equiv 2 \pmod 3$$

and we get $y \equiv 1 \pmod 3$ which is $y \equiv 1, 4 \pmod 6$, thus $x \equiv 3$ and $x \equiv 3^4 \equiv 4 \pmod 7$ would be solutions. ◇

Definition. Let $a, m, n \in \mathbb{Z}$ with $m, n > 0$ and $(a, m) = 1$. Then a is an $n'th$ power residue modulo m if the congruence $x^n \equiv a \pmod m$ has a solution x.

Example. 6 is a third power residue modulo 7. 3 is a $4'th$ power residue modulo 13. ◇

Theorem 5.13. Let $a, m, n \in \mathbb{Z}$, $m, n > 0$ and $(a, m) = 1$. If m has a primitive root, then a is an $n'th$ power residue modulo m if and only if,

$$a^{\phi(m)/d} \equiv 1 \pmod m$$

where $d = (n, \phi(m))$. Furthermore, in this case, the congruence $x^n \equiv a \pmod m$ has exactly d solutions modulo m.

Proof. Let r be a primitive root modulo m. Then then congruence $x^n \equiv a \pmod m$ is equivalent,

$$n\ ind_r x \equiv ind_r a \pmod{\phi(m)}$$

this is solvable if and only if $d = (n, \phi(m))$ divides $ind_r a$ which if true will give us d incongruent solutions.

The condition that $d \mid ind_r a$ is equivalent to,

$$\frac{\phi(m)}{d} ind_r a \equiv 0 \pmod{\phi(m)}$$

which is the same as,

$$a^{\phi(m)/d} \equiv 1 \pmod m$$

□

Corollary 5.14. Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then a is a quadratic residue if and only if,

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

Moreover, there are exactly 2 incongruent solutions in this case.

Example. Let $a = 6, m = 7, n = 3$. A primitive root exist, namely $r = 3$. The congruence,

$$x^3 \equiv 6 \pmod{()7}$$

has $d = (3, 6) = 3$ solutions. ◇

Example. Find all 15'th power residues modulo 9. Since it has a primitive root by PRT, the congruence $x^{15} \equiv a \pmod 9$ is equivalent to,

$$a^{\phi(9)/d} \equiv 1 \pmod 9$$

So we have $d = (15, 6) = 3$. Thus we must have,

$$a^{6/3} \equiv a^2 \equiv 1 \pmod 9$$

Then $a \equiv \pm 1 \pmod 9$. ◇

Chapter 6

Diophantine Equations

Definition. Any equation with one or more variables to be solved in the integers.