Number Theory

Aamod Varma

MATH - 4150, Fall 2025

Contents

1 Divisibility and Factorization **2**
1.1 Divisibility 2
1.2 Prime Numbers 4
1.3 Greatest Common Divisors 6
1.4 The fundamental Theorem of Arithmetic 8

2 Congruences **12**
2.1 Congruences 12
2.2 Calculations 13
2.3 Linear Congruences in one variable 14
2.4 Chinese Remainder Theorem 16

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.

$\diamond$

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 $a|c$ $\square$

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 $-5 = 3 \cdot -2 + 1$ ◇

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 ◇

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. □

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 $p_1, \dots, p_n$ be the finite primes. Now consider $N = p_1p_1 \dots p_n + 1$, 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 $p_i|p_1p_2 \dots, p_n$. This means $p_i|N - p_1, \dots, p_n$ or $p_i|1$ which is false. Hence, by contradiction our assumption is wrong and there are infinitely many primes. □

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 $p \leq a \leq \sqrt{n}$. □

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,

$$a = dq + r, \quad \theta \leq r < d$$

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,

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

$\square$

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,

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

$\diamond$

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 $p|b$. $\square$

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 $1 \leq 1 \leq n + 1$. $\square$

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. □

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 $2^2 3^3 5^1 7^2 = 26460$ ⋄

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 $x > y$. □

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,

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

□

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. □

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

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

Consider the integer $N = 4p_1 \ldots p_r + 3$. 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 $3|p_1 \ldots p_r$, contradiction.
Case 2. $p_i|N$ for some $1 \leq i \leq r$ then $p_i|N - 4p_1 \ldots p_r$ so $p_i|3$, contradiction.
Therefore there are ∞ many primes such that $p = 4n+3$ □

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 $\{0, 1, \ldots, m-1\}$ 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 $r_1, r_2 \in \{0, 1, \ldots, m-1\}$. 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 $\{0, 1, \ldots, m-1\}$ 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,

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

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 $a = \overline{a}$. $\square$

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,

$$5, 13, 563.$$

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

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