Number Theory

Aamod Varma

MATH - 3235, 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 $a \nmid b$ 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 $-5 = 3 \cdot -2 + 1$ ◇

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 $N = p_1 p_1 \dots p_n +$ 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 $p_i|p_1 p_2 \dots, p_n$. 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,

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

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 $(24, 60) = 12$ $\diamond$

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,

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

$\square$

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 $p|b$. $\square$