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 $am + bn = c(c_1 m + c_2 n) = cc_3$ 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 $p_1, \ldots, p_n$ 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. □

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 $\sqrt{n}$. $\diamond$

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 $2 \le m \le n+1$, 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. $\square$

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 $\le 70,000,000$. 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 $\le x$ denoted by $\pi(x)$ goes to $\frac{x}{\log(x)}$.
Or, the "probability" that $n \le x$ is prime is $\frac{\pi(x)}{x} \sim \frac{1}{\log(x)}$

Note. This was proven independently in 1896

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

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.