1. Primes

1.1 Divisibility

Definition 1.1 Let a and b be integers. We say that

$$\text{“}a \textit{ divides } b\text{”} \quad \text{or} \quad \text{“}b \textit{ is divisible by } a\text{”}$$

if there exists an integer x such that

$$b = ax.$$

We usually write $a \mid b$ if a divides b. Otherwise, if a does not divide b, we write $a \nmid b$.

■ **Example 1.1** Since $18 = 2 \times 9$, we have $2 \mid 18$; since $35 = 7 \times 5$, we have $7 \mid 35$. ■

Definition 1.2 If $a \mid b$, then a is called a *divisor* of b. In particular, a positive divisor of b which is different from b is called a *proper divisor*.

Theorem 1.1 Assume that all variables in this theorem are integers.

(i) $1 \mid a$, $a \mid a$ and $a \mid 0$;
(ii) If $a \mid b$, then $a \mid bc$;
(iii) If $a \mid b$ and $b \mid c$, then $a \mid c$;
(iv) If $a \mid b$, then $ac \mid bc$;
(v) If $a \mid b_i$ for $i = 1 \ldots, r$, then $a \mid (m_1 b_1 + \cdots + m_r b_r)$.

Proof. (i). Since $a = 1 \cdot a = a \cdot 1$, we have $1 \mid a$ and $a \mid a$; since $0 = a \cdot 0$, we have $a \mid 0$.

(ii). Note that $a \mid b$ implies that $b = ax$ for some integer x. Thus, $bc = (ax) \cdot c = a \cdot (cx)$, implying that $a \mid bc$.

(iii). Note that $a \mid b$ implies that $b = ax$ and that $b \mid c$ implies that $c = by$. Thus, $c = by = (ax) \cdot y = a \cdot (xy)$, implying that $a \mid c$.

(iv). Note that $a \mid b$ implies that $b = ax$. Thus, $bc = (ax) \cdot c = (ac) \cdot x$, implying that $ac \mid bc$.

(v). Note that $a \mid b_i$ implies that $b_i = ax_i$. Thus,

$$m_1 b_1 + \cdots + m_r b_r = \sum_{i=1}^{r} m_i \cdot (ax_i) = a \sum_{i=1}^{r} m_i x_i,$$

implying that $a \mid (m_1 b_1 + \cdots + m_r b_r)$. ■

1.2 Primes

Definition 1.3 A positive integer p is a *prime* if
(i) $p \geq 2$;
(ii) p has no positive divisors other than 1 and p.
A positive integer *greater than* 1 that is not prime is a *composite*.

R 1 is neither prime nor composite.

■ **Example 1.2** The sequence of primes starts with

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

The sequence of composites starts with

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, \ldots$$

■

1.3 Infinitude of primes

Now, there is a natural question:

Question 1.1 Will the sequence of primes terminate at some place? Or is it infinite?

The first answer to this question was given over 2,000 years ago by Euclid (c. 300 BCE).

Theorem 1.2 (Euclid). The number of primes is infinite.

Proof (of Euclid). Let $\{p_1, \ldots p_k\}$ be a finite set of primes. Consider

$$n = p_1 p_2 \cdots p_k + 1.$$

Then $p \geq 3$. Note that n has a prime factor p. But p is not one of p_i's; otherwise, we have $p \mid p_1 \cdots p_k$ and since $p \mid n$, it follows that $p \mid (n - p_1 \cdots p_k)$. Thus, $p \mid 1$, leading to a contradiction.

Therefore, for any finite set of primes, we are always able to generate a new prime. In other words, a finite set of primes cannot cover all primes. ■

The idea of the above proof is very natural. In fact, one may modify it to establish other interesting results.

Theorem 1.3 The number of primes of the form $4s+3$ is infinite.

Proof. Let $\{p_1, \ldots p_k\}$ be a finite set of primes. Consider

$$n = 4p_1 p_2 \cdots p_k - 1.$$

Note that n is of the form $4s+3$. We claim that n has at least one prime factor p of the form $4s+3$. Otherwise, if all prime factors of n are of the form $4s+1$, then so is their product, namely, n, leading to a contradiction. Further, the above p is not one of 2, p_1, ..., p_k by a similar argument to that for Theorem 1.2. Thus, we arrive at a new prime of the form $4s+3$ from the set $\{p_1, \ldots p_k\}$, thereby implying the infinitude of primes of the form $4s+3$. ■

Theorem 1.4 The number of primes of the form $6s+5$ is infinite.

Proof. Exercise. ■

R In general, let a and m be positive integers such that $1 \leq a \leq m$ and $(a,m) = 1$. Then number of primes of the form $ms+a$ is infinite. Furthermore, let $\pi_{a,m}(x)$ count the number of primes $\leq x$ that are of the form $ms+a$. For fixed m, let a_1 and a_2 be such that $1 \leq a_1, a_2 \leq m$ and $(a_1,m) = (a_2,m) = 1$. Then

$$\lim_{x\to\infty} \frac{\pi_{a_1,m}(x)}{\pi_{a_2,m}(x)} = 1.$$

This is known as *Dirichlet's theorem on primes in arithmetic progressions.*

1.4 Fermat numbers and the second proof of the infinitude of primes

Definition 1.4 *Fermat numbers* are those of the form $F_n = 2^{2^n}+1$ with $n = 0,1,2,\ldots$

Pierre de Fermat wrote to Marin Mersenne on December 25, 1640 that:

> If I can determine the basic reason why
>
> $$3,5,17,257,65537,\ldots,$$
>
> are prime numbers, I feel that I would find very interesting results, for I have already found marvelous things [along these lines] which I will tell you about later.

However, Fermat's conjecture that all F_n are primes is unfortunately proved incorrect as Euler discovered in 1732 that

$$F_5 = 4294967297 = 641 \times 6700417.$$

Furthermore, the known prime Fermat numbers, also known as *Fermat primes* are still the five numbers $F_0,\ldots,F_4$ examined by Fermat. As of 2014, it is known that F_n is composite for $5 \leq n \leq 32$. The largest Fermat number known to be composite is $F_{18233954}$, and its prime factor $7 \times 2^{18233956}+1$ was discovered in October 2020. It is now conjectured that just the first 5 Fermat numbers are primes.

Theorem 1.5 For $n \geq 1$,

$$F_n - 2 = \prod_{i=0}^{n-1} F_i.$$

Proof. We prove this result by induction on n. First, it is true for $n = 1$ since $F_1 - 2 = 3 = F_0$. Next, we assume that it is true for $n = k$ for some $k \geq 1$. Thus,

$$F_k - 2 = \prod_{i=0}^{k-1} F_i.$$

Now, we have

$$F_{k+1} - 2 = (2^{2^{k+1}}+1) - 2 = 2^{2^{k+1}} - 1 = (2^{2^k}+1)(2^{2^k}-1)$$

$$= F_k(F_k - 2) = F_k \cdot \prod_{i=0}^{k-1} F_i$$
$$= \prod_{i=0}^{k} F_i,$$

implying that the statement is also valid for $n = k+1$. ■

Corollary 1.6 Any two distinct Fermat numbers have no common divisor greater than 1.

Proof. Assume that a prime p divides both F_m and F_n with $0 \le m < n$. Since $p \mid F_m$, we have $p \mid \prod_{i=0}^{n-1} F_i$. Now, $p \mid F_n$ implies that $p \mid \left(F_n - \prod_{i=0}^{n-1} F_i\right)$, and thus $p \mid 2$ by Theorem 1.5. Thus, $p = 2$. But this is impossible since all Fermat numbers are odd. ■

Now we are in a position to present the second proof of the infinitude of primes.

Second Proof of Theorem 1.2. Note that the sequence of Fermat numbers is infinite. We collect prime factors of these Fermat numbers, and by Corollary 1.6, they are pairwise distinct. Therefore, there are infinite primes. ■

1.5 Fundamental theorem of arithmetic

Theorem 1.7 Every integer $n \ge 2$ is a product of primes.

Proof. We prove by induction on n. First, 2 is a prime itself, and thus the statement is true for $n = 2$. Assume that the statement is true for $n = 2 \ldots, k$ for some $k \ge 2$. Then if $n = k+1$ is prime, there is nothing to prove. If $n = k+1$ is composite, then we may write $k+1 = x \cdot y$ such that $1 < x, y < k+1$. By our assumption, both x and y are products of products, so is their product $xy = k+1$. Hence, the statement is also true for $n = k+1$. ■

Now, a natural question is *how many representations are there to factorize $n \ge 2$ as a product of primes?* This question is answered by the *Fundamental Theorem of Arithmetic*, also known as the *Unique Factorization Theorem*.

Theorem 1.8 (Fundamental Theorem of Arithmetic). Every integer $n \ge 2$ has a unique (up to order of factors) representation as a product of primes.

This theorem, although intuitionistic, is far more than trivial. We will give its proof in the next lecture.

1.6 Divergence of $\sum_p \frac{1}{p}$ and the third proof of the infinitude of primes

Now, we have a straightforward consequence of the Fundamental Theorem of Arithmetic. Consider

$$\prod_{\substack{p \text{ prime} \\ p \le n}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right).$$

If we expand the product, then for each i with all its prime factors at most n, we have that $\frac{1}{i}$ appears as exactly one of the terms. In particular, such i's include all integers $m \le n$.

Therefore,

$$\prod_{\substack{p \text{ prime} \\ p \le n}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \ge \sum_{m=1}^{n} \frac{1}{m}.$$

Then,

$$\prod_{p \le n} \frac{1}{1 - \frac{1}{p}} = \prod_{p \le n} \sum_{k=0}^{\infty} \frac{1}{p^k} > \sum_{m=1}^{n} \frac{1}{m} > \int_1^n \frac{dt}{t} = \log n.$$

On the other hand,

$$\begin{aligned}
\log \prod_{p \le n} \frac{1}{1 - \frac{1}{p}} &= \sum_{p \le n} \log \frac{1}{1 - \frac{1}{p}} = \sum_{p \le n} \sum_{k=1}^{\infty} \frac{1}{k \cdot p^k} = \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \sum_{k=2}^{\infty} \frac{1}{k \cdot p^k} \\
&< \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \sum_{k=2}^{\infty} \frac{1}{2p^2 \cdot p^{k-2}} = \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \frac{1}{2p^2} \sum_{k=0}^{\infty} \frac{1}{\cdot p^k} \\
&= \sum_{p \le n} \frac{1}{p} + \sum_{p \le n} \frac{1}{2p^2} \frac{p}{p-1} \le \sum_{p \le n} \frac{1}{p} + \frac{1}{2} \sum_{m=2}^{n} \frac{1}{m(m-1)} \\
&< \sum_{p \le n} \frac{1}{p} + \frac{1}{2}.
\end{aligned}$$

Thus,

$$\sum_{p \le n} \frac{1}{p} + \frac{1}{2} > \log \prod_{p \le n} \frac{1}{1 - \frac{1}{p}} > \log \log n.$$

Theorem 1.9 We have

$$\sum_{\substack{p \text{ prime} \\ p \le n}} \frac{1}{p} > \log \log n - \frac{1}{2}. \tag{1.1}$$

In particular, $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

This result gives the third proof of the infinitude of primes.

Third Proof of Theorem 1.2. If there are finitely many primes, then $\sum_p \frac{1}{p}$ is also finite, which contradicts to the divergence of $\sum_p \frac{1}{p}$ established in Theorem 1.9. ■

R In fact, as $x \to \infty$,

$$\sum_{p \le x} \frac{1}{p} \sim \log \log x,$$

or more precisely,

$$\sum_{p \le x} \frac{1}{p} = \log \log x + B + o(1),$$

where B is a constant.

1.7 Erdős's proof of the divergence of $\sum_p \frac{1}{p}$

The previous proof of the divergence of $\sum_p \frac{1}{p}$ has, more or less, an analytic flavor. What will be provided here is an elegant elementrary attack due to Paul Erdős (*Mathematica, Zutphen. B.* **7** (1938), 1–2).

Theorem 1.10 The series $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

Proof. We prove by contradiction. That is, we assume that $\sum_p \frac{1}{p}$ converges. Let $\{p_1, p_2, \ldots\}$ be the sequence of primes in increasing order.

First, given an arbitrary positive integer n and an index K, we denote by $N_K(n)$ the number of positive integers $m \le n$ such that the prime factors of m are exclusively from $p_1, \ldots, p_K$. Note that by the Fundamental Theorem of Arithmetic, each integer a can be uniquely written as $a = s^2 \cdot t$ where t has no square factor greater than 1. Meanwhile, the squares no greater than n are 1^2, 2^2, ..., $\lfloor \sqrt{n} \rfloor^2$ where $\lfloor x \rfloor$ denotes the largest integer not exceeding a real x. Also, there are 2^K integers of the form $\prod_{i=1}^K p_i^{\varepsilon_i}$ with $\varepsilon_i \in \{0,1\}$. Now, if we write integers m counted by $N_K(n)$ as $m = s^2 \cdot t$, then s^2 comes from the above squares and t comes from the above $\prod_{i=1}^K p_i^{\varepsilon_i}$. Hence, $N_K(n) \le 2^K \sqrt{n}$.

On the other hand, the assumption of the convergence of $\sum_p \frac{1}{p}$ means that the index K may be choosen so that $\frac{1}{p_{K+1}} + \frac{1}{p_{K+2}} + \cdots < \frac{1}{2}$. Now, we observe that the number $N'_K(n)$ of integers $m' \le n$ with at least one prime factor among $p_{K+1}, p_{K+2}, \ldots$ is bounded by

$$N'_K(n) \le \frac{n}{p_{K+1}} + \frac{n}{p_{K+2}} + \cdots < \frac{n}{2}.$$

Noting that $N_K(n) + N'_K(n) = n$, we obtain that the following holds true for any positive integer n:

$$n < 2^K \sqrt{n} + \frac{n}{2}.$$

However, it fails when $n = 2^{2K+2}$, thereby giving a contradiction. Hence, $\sum_p \frac{1}{p}$ diverges. ∎