1 Infinity of Prime Numbers

1.1 Euler Product

We consider the following product

$$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} = \prod_{p\in\mathbb{P}} \sum_{k=0}^{+\infty} \frac{1}{p^{ks}} \tag{1}$$

As every integer can be represented as

$$n = \prod_{\substack{p_i\in\mathbb{R}\\ \alpha_i\geq 0}} p_i^{\alpha_i} \longrightarrow \frac{1}{n^s} = \prod_{\substack{p_i\in\mathbb{P}\\ \alpha_i\geq 0}} \frac{1}{p_i^{\alpha_i s}} \tag{2}$$

Then

$$\prod_{p\in\mathbb{P}} \sum_{k=0}^{+\infty} \frac{1}{p^{ks}} = \sum_{n=1}^{+\infty} \frac{1}{n^s} \tag{3}$$

1.2 Infinity of Prime Numbers

Assume that there are a finite number of prime numbers, denoted as $\mathbb{P} = \{p_1, p_2, \ldots, p_s\}$, then

$$\sum_{n=1}^{N} \frac{1}{n} < \sum_{n=1}^{+\infty} \frac{1}{n} = \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} = \prod_{p_i}^{s} \frac{1}{1-\frac{1}{p_i^s}} \tag{4}$$

As $N \to \infty$, the harmonic series diverges. Hence the inequality contradicts with the fact that the RHS is a constant. Thus we can conclude that $s = \infty$, i.e. prime numbers are infinite many.

2 The Greatest Common Divisor Theory

We only give an important lemma of the GCD theory.

2.1 Lemma 2.1

$$\operatorname{lcm}(a_1, a_2)\gcd(a_1, a_2) = a_1 a_2 \tag{5}$$

Proof It is intuitive that

$$\gcd\left(\frac{a_1}{\gcd(a_1,a_2)}, \frac{a_2}{\gcd(a_1,a_2)}\right) = 1 \to \operatorname{lcm}\left(\frac{a_1}{\gcd(a_1,a_2)}, \frac{a_2}{\gcd(a_1,a_2)}\right) = \frac{a_1}{\gcd(a_1,a_2)} \cdot \frac{a_2}{\gcd(a_1,a_2)}$$

Then

$$\gcd(a_1,a_2)^2 \operatorname{lcm}\left(\frac{a_1}{\gcd(a_1,a_2)}, \frac{a_2}{\gcd(a_1,a_2)}\right) = a_1 a_2 = \operatorname{lcm}(a_1,a_2)\gcd(a_1,a_2) \tag{6}$$

2.2 Fermat's Little Theorem

Fermat's little theorem states that if p is a prime number, then

$$p \mid a^p - a, \quad a \in \mathbb{Z} \tag{7}$$
$$p \mid a^{p-1} - 1, \quad a \in \mathbb{Z}, \quad \gcd(a, p) = 1 \tag{8}$$

Proof

Lemma 2.2 For integer $1 \le j \le p-1$,

$$p \,\Bigg|\, \binom{p}{j} \tag{9}$$

As p is a prime number, then for $1 \le j \le p-1$,

$$\gcd(p, j) = 1 \quad \to \quad \gcd(p, j) = \gcd(p, p-j) = 1 \quad \to \quad \gcd(p, j!(p-j)!) = 1 \tag{10}$$

As the combinatorial number is an integer,

$$\binom{p}{j} \in \mathbb{Z} \quad \to \quad j!(p-j)! \mid p! \quad \to \quad j!(p-j)! \mid (p-1)! \tag{11}$$

Then we can conclude that

$$p \,\Bigg|\, \frac{p!}{j!(p-j)!} = \binom{p}{j} \tag{12}$$

Then we may use mathematical induction in proving. For $a = 1$, $p \mid 0$ holds. Assume that for $a = n$ the theorem holds, then for $a = n+1$,

$$(n+1)^p - (n+1) = \sum_{i=0}^{p} \binom{p}{j} n^j - n - 1 = n^p - n + \sum_{j=1}^{p-1} \binom{p}{j} n^j \tag{13}$$

Applying the condition and the lemma,

$$p \mid n^p - p, \; p \,\Bigg|\, \binom{p}{j} \quad \to \quad p \mid (n+1)^p - (n+1)$$

When a, p are coprime,

$$p \mid a^p - a = a(a^{p-1} - 1) \quad \to \quad p \mid a^{p-1} - 1 \tag{14}$$

Thus we prove the **Fermat's little theorem**. ■

2.3 Lemma 2.2 (Existence of Modular Multiplicative Inverse)

① If $m \ge 2$, $\gcd(m, a) = 1$, then integer $d \le m-1$ exists, such that $m | a^d - 1$.
Proof For every integer $1 \le j \le m$, the pseudo-division gives

$$a^j = q_j m + r_j \;\leftrightarrow\; a^j \equiv r_j \pmod{m}, \; r_j \ne 0 \tag{15}$$

As there are $j-1$ possible values for $a^j \bmod m$, and j numbers of residual r_j, then there must exists $k, b \in [1, m]$, such that

$$\begin{cases} a^k = q_k m + r_k \\ a^b = q_b m + r_b \end{cases}, \quad r_k = r_b \tag{16}$$

Assume that $k > b$, then

$$a^k - a^b = a^b(a^{k-b} - 1) = (q_k - q_b)m \tag{17}$$

As $\gcd(m, a) = 1$, it is easy to prove that $\gcd(m, a^b) = 1$. Hence,

$$(q_k - q_b)m \mid a^b(a^{k-b} - 1) \quad \to \quad m \mid (a^{k-b} - 1) \quad \xrightarrow{d=k-b} \quad m \mid a^d - 1 \tag{18}$$

② If d_0 is the least integer in the set of d in ①, called the **modular exponentiation** of a to m, then $m | a^h - 1$ if and only if $d_0 | h$.

Proof

Sufficiency If $d_0 | h$, then

$$h = qd_0 \quad \to \quad a^h - 1 = a^{qd_0} - 1 = (a^{d_0} - 1)\sum_{i=0}^{q-1} a^{id_0} \equiv 0 \pmod{m} \tag{19}$$

Necessity The pseudo-division gives

$$h = qd_0 + r \quad 0 \le r < d_0 \tag{20}$$

Substitute in we obtain

$$a^h - 1 = a^{qd_0+r} - 1 = a^r(a^{qd_0} - 1) + a^r - 1 \tag{21}$$

If $a^h - 1 \equiv 0 \pmod{m}$, then $m | a^r - 1$. As $0 \le r < d_0$, and the condition that d_0 is the least integer, the only value r can take is $r = 0$. Thus $d_0 | h$. ■

3 Fundamental Theorem of Arithmetic

3.1 Content

3.1.1 Theorem 1

If p is a prime number, and $p \mid \prod_{i=1}^{k} a_i$, then

$$p \mid a_j \quad 1 \le j \le k \tag{22}$$

holds for at least one j.

3.1.2 Theorem 2

Any integer $a > 1$ can be uniquely represented as

$$a = p_1 p_2 \cdots p_s \tag{23}$$

where p_j $1 \le j \le s$ are all prime numbers.
Proof Assume that the prime numbers are arranged in non-decreasing order, i.e. $p_1 \le p_2 \le \cdots \le p_s$. If there is another decomposition

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r \quad 1 \le 2 \le \cdots \le q_r \tag{24}$$

As $q_1 \mid a,\ p_1 \mid a$, then

$$\begin{cases} q_1 \mid p_1 p_2 \cdots p_s \ \rightarrow \ \exists\ p_i,\ q_1 \mid p_i \quad 1 \le i \le r \ \rightarrow \ p_i = q_1 \\ p_1 \mid q_1 q_2 \cdots q_r \ \rightarrow \ \exists\ q_j,\ p_1 \mid q_j \quad 1 \le j \le s \ \rightarrow \ p_1 = q_j \end{cases} \longrightarrow \ p_1 \le p_i = q_1 \le q_j = p_1 \tag{25}$$

Hence $p_1 = q_1$. Likewise we can derive that $p_i = q_i$ for $1 \le i \le \min(r, s)$. Assume that $r \ge s$, then

$$q_{s+1} q_{s+2} \cdots q_r = 1 \tag{26}$$

which contradicts with the assumption that q_i is a prime number, unless $r = s$. ■

3.2 Corollary 1

If $p_1, p_2, \ldots, p_s$ are all prime integers, and

$$a = \prod_{i=1}^{s} p_i^{\alpha_i} \qquad b = \prod_{i=1}^{s} p_i^{\beta_i} \tag{27}$$

then

$$\begin{aligned} \gcd(a,b) &= \prod_{i=1}^{s} p_i^{\delta_i} \qquad \delta_i = \min(\alpha_i, \beta_i) \\ \mathrm{lcm}(a,b) &= \prod_{i=1}^{s} p_i^{\gamma_i} \qquad \gamma_i = \max(\alpha_i, \beta_i) \end{aligned} \tag{28}$$

Additionally, the summation of the divisors of integer a, denoted as $\sigma(a)$, can be written as

$$\sigma(a) = \prod_{i=1}^{s} \sigma(p_i^{\delta_i}) = \prod_{i=1}^{s} \sum_{j=0}^{\sigma_i} p_i^j = \prod_{i=1}^{s} \frac{p^{\sigma_i+1} - 1}{p_i - 1} \tag{29}$$

4 The Exponent of Prime Factors

For an integer n, the integer α for prime number p such that $p^\alpha \parallel n!$ can be written as

$$\alpha(p, n) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right] \tag{30}$$

4.1 Derivation

Denote the magnitude of the set $\{x|x \bmod p^i = 0,\ 1 \le x \le n\}$ as c_i. Then the magnitude of the set $\{x|\ p^i \parallel x,\ 1 \le x \le n\}$ is $d_i = c_i - c_{i+1}$. We can conclude that

$$d_i = c_i - c_{i+1} = \left[\frac{n}{p^i}\right] - \left[\frac{n}{p^{i+1}}\right] \tag{31}$$

Thus

$$\alpha(p,n) = \sum_{i=0}^{\infty} i d_i = \sum_{i=1}^{k} \left[\frac{n}{p^i}\right] = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right], \quad p^k \parallel n \tag{32}$$

5 Corollary 1

One conclusion can be drawn that

$$n!(m!)^n \ \mid \ (mn)! \tag{33}$$

Proof Consider an arbitrary prime factor of the integer m. We need to prove that

$$\alpha(p,n) + n\alpha(p,m) \le \alpha(p,mn) \ \Leftrightarrow\ \sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right] + n\sum_{j=1}^{\infty}\left[\frac{m}{p^j}\right] \le \sum_{j=1}^{\infty}\left[\frac{mn}{p^j}\right] \tag{34}$$

Consider $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p^l \cdots p_s^{\alpha_s}$, then write $m = cp^l$. For $j \le l$, we have

$$\left[\frac{mn}{p^j}\right] = cnp^{l-j} = n\left[\frac{m}{p^j}\right] \ \rightarrow\ \sum_{j=1}^{l}\left[\frac{mn}{p^j}\right] = \sum_{j=1}^{l} n\left[\frac{m}{p^j}\right] \tag{35}$$

For $j > l$, we have the pseudo-division $m = q_j p^j + r_j$, where $r_j \in [1, p^j - 1]$. Thus

$$\begin{aligned} \left[\frac{mn}{p^j}\right] = \left[nq_j + n\frac{r_j}{p^j}\right] = nq_j + \left[\left\{\frac{m}{p^j}\right\} n\right] \ge n\left[\frac{m}{p^j}\right] + \left[\frac{n}{p^{j-l}}\right] \\ \rightarrow \sum_{j>l}\left[\frac{mn}{p^j}\right] \ge n\sum_{j>l}\left[\frac{m}{p^j}\right] + \sum_{j-l>0}\left[\frac{n}{p^{j-l}}\right] \end{aligned} \tag{36}$$

Sum the two equations up we obtain ∎

$$\sum_j \left[\frac{mn}{p^j}\right] \ge n\sum_j\left[\frac{m}{p^j}\right] + \sum_j\left[\frac{n}{p^j}\right]$$

6 Euclid Algorithm

6.1 Content

If two integers u_0, u_1, $u_1 \nmid u_0$. Then we can give the following pseudo-division method

$$\begin{aligned} &u_0 = q_0 u_1 + u_2, \quad 0 < u_2 < |u_1| \\ &u_1 = q_1 u_2 + u_3, \quad 0 < u_3 < u_2 \\ &\ \vdots \\ &u_{k-1} = q_{k-1}u_k + u_{k+1}, \quad 0 < u_k < u_{k-1} \\ &u_k = q_k u_{k+1} \end{aligned} \tag{37}$$

And

$$u_{k+1} = \gcd(u_0, u_1) \tag{38}$$

Or

$$\gcd(u_i, u_j) = \gcd(u_j, u_i \bmod u_i) \tag{39}$$

The equations above indicates that the greatest common divisor of integers $a_1, a_2, \dots, a_k$, the coefficients $x_1, x_2, \dots, x_k$ exists, such that

$$\gcd(a_1, a_2, \dots, a_k) = a_1x_1 + a_2x_2 + \dots + a_kx_k \tag{40}$$

6.2 Lemma 1.1

A lemma can be given that

$$\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m,n)} - 1 \tag{41}$$

Proof As

$$m = qn + r \quad \rightarrow \quad 2^m - 1 = 2^{qn+r} - 2^r + 2^r - 1 = 2^r(2^{qn} - 1) + 2^r - 1 \tag{42}$$

Hence

$$\gcd(2^m - 1, 2^n - 1) = \gcd(2^r - 1, 2^n - 1) = \gcd(2^n - 1, 2^{\gcd(m,n)} - 1) = \dots = 2^{\gcd(\mathrm{m,n})} - 1$$

7 Extended Euclidean Algorithm

Based on the Euclidean algorithm, the extended one solve the equation

$$ax + by = \gcd(a, b) \tag{43}$$

and calculates the modular multiplicative inverse at the same time.

7.1 Implementation

7.1.1 Particular Solution

Assume that there are two equations, where

$$\begin{cases} ax_0 + by_0 = \gcd(a, b) \\ bx_1 + (a \bmod b)y_1 = \gcd(b, a \bmod b) = \gcd(a, b) \end{cases} \tag{44}$$

Then we can conclude that

$$ax_0 + by_0 = bx_1 + (a \bmod b)y_1 = bx_1 + (a - b\lfloor\frac{a}{b}\rfloor)y_1 \tag{45}$$

As a, b are arbitrary integers, we have

$$b(x_1 - \lfloor\frac{a}{b}\rfloor y_1 - y_0) = a(y_1 - x_0) \ \rightarrow \ \begin{cases} x_0 = y_1 \\ y_0 = x_1 - \lfloor\frac{a}{b}\rfloor y_1 \end{cases} \tag{46}$$

Then by recursively repeating the bottom-up recursion that

$$\begin{cases} x_k = y_{k+1} \\ y_k = x_{k+1} - \lfloor \frac{a_k}{b_k} \rfloor y_{k+1} \end{cases} \quad \begin{cases} a_{k+1} = b_k \\ b_{k+1} = a_k \bmod b_k \\ \gcd(a_{k+1}, b_{k+1}) = \gcd(a_k, a_k) \end{cases} \tag{47}$$

The terminal state is the equation $ax_n + by_n = \gcd(a_n, b_n) = \gcd(a, b)$, where $b_n = 0$. We instantly solve that $x_n = 1, y_n = 0, a_n = \gcd(a, b), b_n = 0$. If we assign the terminal value to the bottom variables, then the traceback in every step will calculate the particular solution (x_0, y_0) for the original equation.

7.1.2 Complementary Solution

From the particular solution the complementary solution can be derived. Consider the original equation

$$ax_0 + by_0 = \gcd(a, b) \ \rightarrow \ a\left(x_0 - \frac{b}{\gcd(a, b)}t\right) + b\left(y_0 - \frac{a}{\gcd(a, b)}t\right) = \gcd(a, b) \tag{48}$$

Hence, we conclude that the complementary solution for the equation is

$$\begin{cases} x = x_0 - \dfrac{b}{\gcd(a, b)}t \\ y = y_0 - \dfrac{a}{\gcd(a, b)}t \end{cases} \tag{49}$$

8 Non-zero / Positive Solution to Diphantine Equation