数论简介、素数、算术基本定理

李 辉

Table of Contents

数论简介

名人名言

- (Johann Carl Friedrich **Gauss** 1777.4–1855.2)
- Mathematics is the **queen** of sciences and number theory is the **queen** of mathematics. She often condescends to render service to astronomy and other natural sciences, but in all relations she is entitled to the first rank.
- From “Gauss zum Gedächtniss”. Book by Wolfgang Sartorius von Waltershausen, 1856.

相关科学与技术

- Algebra
- geometry
- analysis
- logic
- topology
- computer science

数的演化

- 自然数N -> 取反
- 整数Z -> 除
- 有理数Q -> 实分析/Dedekind Cut
- 实数R -> 负数开方
- 复数C

Theorem $\sqrt{2}$ is an irrational number.

Proof.

Assume that $\sqrt{2}$ is a rational number. Then

$$\sqrt{2} = a/b,$$

where a and b are coprime integers.

$$a^2/b^2 = 2$$
$$a^2 = 2b^2$$

So, a must be even.

Let $a = 2k$.

$$2b^2 = (2k)^2$$
$$b^2 = 2k^2$$

So, b must be even, which contradicts that a/b is irreducible. ■

从自然数开始

自然数的基本性质

- Successor Operation
  - $s(n) = n + 1$
- PMI (Principle of Mathematical Induction)
  - $p(1)$ is true and $p(n) \Rightarrow p(n+1)$, then $p(n)$ is true for all natural numbers.
- WOP (Well Ordering Principle)
  - Every nonempty subset of natural number has a smallest element.

Excise 001

Prove (PMI):

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

.

整除、带余除法和互素

Divisibility

$$a|b \quad if\ \ b = ax\ \ for\ \ a, b, x \in Z\ \ and\ \ a \neq 0$$

$$\forall n \in N, \quad n|0$$

$$a|b, b|c \rightarrow a|c$$

$$a|b, a|c \rightarrow a|bx + cy\ \forall x, y \in Z$$

Example

$$3|6,6|36 \rightarrow 3|36$$

$$7|14,7|35 \rightarrow 7|(14 \times 3 + 35 \times 2 = 112)$$

Division with Remainder

$Theorem$ 1: Given $a, b \in Z$ with $a > 0$,
$\exists q, r \in Z$, such that $b = aq + r, 0 \leq r < a$

Proof:

$$Let\ S = \{b + ka : k \in Z, b + ka \geq 0\}$$

$$S\ is\ notempty: \begin{cases} b > 0 & then \quad b + 0a \in S \\ b < 0 & then \quad adding\ a\ enough\ times \\ & to\ make\ it\ positive \end{cases}$$

Since S is nonempty, it has a smallest element $r = b + ka$ for some k (WOP).

Setting $q = -k$ results in $r = b - qa$.

$r \geq 0$ because it is in S, and $r < a$ because if not, then $b + (k-1)a$ would be smallest element in S. ■

Example

$$311 = ? \times 13 + ?\ (a = 13)$$

$$-21 = ? \times 11 + ?\ (a = 11)$$

$Definition$ **GCD**(**Greatest Common Divisor**)

If a and b are not both 0, then $gcd(a, b)$ or (a, b) is the greatest common divisor of a and b.

Example

$$gcd(24{,}38) = 2$$

Excise002

$$gcd(148{,}111111) = ?$$

$Theorem$ 2. Let $g = gcd(a, b)$, then $\exists v_0, y_0 \in Z$ such that $g = ax_0 + by_0$.

Proof. Let $S = \{ax + by: x, y \in Z, ax + by > 0\}$, and assume a, b not both 0. Assume $a \neq 0$,

$$S\ is\ notempty: \begin{cases} a > 0 & \Rightarrow a \in S \\ a < 0 & \Rightarrow -a \in S \end{cases}$$

Since S is notempty, it has a smallest element $g = ax + by$.

- Prove $g|a$ (by contradiction):

$$a = gq + r, \qquad 0 < r < g$$
$$r = a - gq = a - q(ax + by) = a(1 - qx) - b(qy)$$
$$\Rightarrow r \in S$$

However, $r < g$, so g isn't the smallest.

- Prove g is largest common:

If $d|a$ and $d|b$, then $d|ax + by = g$. Since $g|a$,$g|b$, and g is largest common divisor, then g is $gcd(a, b)$. ■

Excise003

$$gcd(24,34) = 2$$

$$2 = 24x + 34y,\ x, y \in Z$$

$$x = ?\ ,\ y = ?$$

$Definition$ **Coprime**

If gcd(a,b)=1, then a and b are coprime.

Example

- 10 and 9 are coprime
- 10 and 12 are not coprime

$Corollary$: If $gcd(a,m) = 1$ and $gcd(b,m) = 1$, then $gcd(ab,m) = 1$.

Proof.

$$1 = ax + my, ax = 1 - my$$
$$1 = bx' + my', bx' = 1 - my'$$
$$abxx' = (1 - my)(1 - my')$$
$$= 1 - my - my' + m^2yy'$$
$$= 1 + m(-y - y' + myy')$$
$$1 = ab(xx') + m(y + y' - myy')$$

Example

$$gcd(5{,}24) = 1\ gcd(7{,}24) = 1$$

$$gcd(35{,}24) = 1$$

$Corollary$: If $c|ab$ and $gcd(c, a) = 1$, then $c|b$.

Proof.
$gcd(a, c) = 1 \Rightarrow 1 = ax + cy \Rightarrow b = abx + bcy$

$$c|ab, c|bc \Rightarrow c|(abx + bcy) = b$$

Example

$$35|1050,\ gcd(35,6) = 1$$

$$35|175$$

Euclidean GCD Algorithm (辗转相除法):
Given $a, b \in Z$, not both 0, one can find $gcd(a, b)$ as follows.

1. If $a, b < 0$, replace with negative.
2. If $a > b$, switch a and b.
3. If $a = 0$, return b.
4. Since $a > 0$, write $b = aq + r$ with $0 \leq r < a$. Replace $gcd(a, b)$ with $gcd(r, a)$ and go to step 3.

Proof. Step 1 and 2 do not affect the GCD. So only need to prove $gcd(a, b) = gcd(r, a)$ where $b = aq + r$. Let $d = gcd(r, a)$ and $e = gcd(a, b)$,

$$
\begin{aligned}
d = gcd(r, a) \quad & \Rightarrow d|a, d|r \\
& \Rightarrow d|aq + r = b \\
& \Rightarrow d|a, b \\
& \Rightarrow d|gcd(a, b) = e
\end{aligned}
$$

$$
\begin{aligned}
e = gcd(a, b) \quad & \Rightarrow e|a, e|b \\
& \Rightarrow e|b - aq = r \\
& \Rightarrow e|r, a \\
& \Rightarrow e|gcd(r, a) = d
\end{aligned}
$$

Since d and e are positive and divide each other, and thus being equal. ■

Excise002 again

$$gcd(148,111111) =?$$

$Definition$: **Prime number**

A **prime number** is an integer $p > 1$ such that it cannot be written as $p = ab$ where $a, b > 1$.

Example

- 11 is a prime number
- 111 is not a prime number

Theorem 3 (**Fundamental Theorem of Arithmetic**) Every positive integer can be written as a product of primes (possibly with repetion) and any such expression is unique up to a permutation of the prime factors.

Example

$$72 = 2^3 \times 3^2$$

$$999999 = 3^3 \times 7 \times 11 \times 13 \times 37$$

Proof of Existence (by contradiction):

Let S be the set of numbers which cannot be written as a product of primes. Assume S is not empty, it has a smallest element n by WOP. $n = 1$ is not possible by definition, so $n > 1$. n cannot be prime, since if so it'd be a product with one term, and so wouldn't be in S.

Hence, $n = ab$ with $a, b > 1$.

Also, $a, b < n$ so they cannot be in S by minimality of n, and so a and b are the product of primes. n is the product of the two, and so is also a product of primes, and so cannot be in S, and hence S is empty.

Proof of Uniqueness.

Lemma: If p is prime and $p|ab$, then $p|a$ or $p|b$.

Proof. Assume $p \nmid a$, and let $g = gcd(p, a)$, since p is prime, $g = 1$ or p, and g cannot be p because $g|a$ and $p \nmid a$, so $g = 1$. So, $p|b$.

$Corollary$: If $p|a_1a_2 \cdots a_n$, then $p|a_i$ for some i.

Proof. If $n = 1$ then the corollary is true. Suppose it holds for $n = k$. Let $n = k + 1$,

$$p|\underbrace{a_1a_2 \cdots a_k}_{A}\underbrace{a_{k+1}}_{B}$$

$$p|AB \Rightarrow \begin{cases} p|A & = p|a_1a_2 \cdots a_k \\ & \Rightarrow p|a_i\, for\, some\, i \\ p|B & \Rightarrow p|a_{k+1} \end{cases}$$

Proof of Uniqueness. Suppose $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, $p_1 | n = q_1 q_2 \cdots q_s$, so $p_1 | q_i$ for some i. Since p_1 and q_i are prime, $p_1 = q_i$.

Canceling one by one, one can obtain $r = s$ and $p_1 p_2 \cdots p_r$ is permutation of $q_1 q_2 \cdots q_s$. ■

Theorem 4: There are infinitely many primes.

Proof. Suppose there are finitely many primes $p_1, p_2, \cdots, p_n$, with $n \geq 1$. consider $N = p_1 p_2 \cdots p_n + 1$, and so by the Fundamental Theorem of Arithemtic there must be a prime q dividing N. Using Euclidean gcd algorithm, $(p_i, p_1 p_2 \cdots p_n + 1) = (p_i, 1) = 1$, and so $p_i \nmid N$. So, $q \neq p_i$ for any i, and q is a new prime. ■

Another proof by Euler***

$$1+\left(\frac{1}{p}\right)+\left(\frac{1}{p}\right)^2+\left(\frac{1}{p}\right)^3+\cdots=\frac{1}{1-1/p},$$

$$\prod_p \frac{1}{1-1/p} = \prod_p \left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right).$$

After expanding Σ, we can pick out any combination of terms to obtain

$$\prod_p \frac{1}{1-1/p} = \left(\cdots\frac{1}{p_1^{e_1}}\cdots\right)\left(\cdots\frac{1}{p_2^{e_2}}\cdots\right)\cdots\left(\cdots\frac{1}{p_m^{e_m}}\cdots\right)\cdots = \sum_{n=1}^{\infty}\frac{1}{n}$$

与素数相关的著名猜想

- Goldbach Conjecture
- Twin Prime Conjecture
- Mersenne Prime Conjecture