初等数论 第1讲

孙智伟

南京大学数学学院

邮箱：zwsun@nju.edu.cn

个人主页：http://maths.nju.edu.cn/~zwsun

2024年8月5日

第一讲：整除性、素数与算术基本定理

§1.1 整除性与素数

§1.2 算术基本定理

§1.3 Chebyshev不等式与素数定理

§1.4 最大公因数与最小公倍数

串值归纳法

我们用$\mathbb{N}$表示自然数集$\{0, 1, 2, \ldots\}$. 用$\mathbb{Z}^+$表示正整数集$\{1, 2, 3, \ldots\}$.

数学归纳法是关于自然数系统的Peano算术五条公理之一，是非常有用的工具。

串值归纳法. 任给关于自然数n的一阶公式$P(n)$. 假设$P(0)$成立，而且对任何$n \in \mathbb{N}$由$P(0), \ldots, P(n)$都成立可得$P(n+1)$成立，则对所有$n \in \mathbb{N}$都有$P(n)$.

证明: 对$n \in \mathbb{N}$让$\psi(n)$表示$P(0)$ & $\cdots$ & $P(n)$. 则$\psi(0)$成立，且有$\psi(n) \Rightarrow \psi(n+1)$. 于是依数学归纳法知对所有$n \in \mathbb{N}$都有$\psi(n)$, 从而也有$P(n)$.

最小数原理

对于自然数m, n, 如果$\exists d \in \mathbb{N}(m + d = n)$, 则说$m$小于或等于$n$, 记为$m \leqslant n$. 可证$\leqslant$是$\mathbb{N}$上的线性序（全序），即它满足自反性、反对称、传递性、可比性。

最小数原理. 自然数集$\mathbb{N}$的任一个非空子集必有最小元。

证明: 反设有$\mathbb{N}$的非空子集S不含最小元，我们来证任何自然数不属于S, 从而矛盾。

显然$0 \notin S$, 不然0是S的最小元了。

假设$n \in \mathbb{N}$且$0, \ldots, n$都不属于S. 如果$n + 1 \in S$, 则$n + 1$不是S的最小元，从而有$m \leqslant n$使得$m \in S$, 这与归纳假设矛盾。因此$n + 1 \notin S$.

由上，依串值归纳法，任何自然数都不属于S, 这与S非空矛盾。

§1.1 整除性与素数

我们用$\mathbb{Z}$表示整数集$\{0, \pm 1, \pm 2, \ldots\}$.

定义. 对于$a, b \in \mathbb{Z}$, 如果有$q \in \mathbb{Z}$使得$aq = b$, 则称a**整除**b, 记为$a \mid b$. 此时也说b被a整除，a是b的**因子（或因数）**(divisor), b是a的**倍数**(multiple). a整除b不成立时，我们说a**不整除**b, 记为$a \nmid b$.

例子：$-3 \mid 15$, $4 \nmid 6$, $0 \nmid 1$, $-5 \mid 0$.

被2整除的数叫**偶数**(even number), 不被2整除的数叫**奇数**(odd number).

自然数集$\mathbb{N}$上的整除关系是个半序，即满足自反性、反对称与传递性。

$\mathbb{Z}$上整除关系的基本性质

(1) ± 1与$\pm a$都整除a.

(2) $a \mid b \iff |a| \mid |b|$.

(3) $a \mid 0$, $a \neq 0$时$0 \nmid a$.

(4) $a \mid b$且$b \neq 0$时, $|a| \leqslant |b|$.

(5) $(a \mid b \ \& \ b \mid a) \iff |a| = |b|$.

(6) $(a \mid b \ \& \ b \mid c) \Rightarrow a \mid c$.

(7) $ac \mid bc \iff (a \mid b$ 或 $c = 0$.

(8) $(a \mid b \ \& \ a \mid c) \Rightarrow a \mid b \pm c$.

一道国际奥数题

例题 (2007年国际奥数题). 设a, b为正整数且$4ab-1 \mid (4a^2-1)^2$, 证明$a=b$.

证明：由于$(4a^2-1)b-(a-b)=a(4ab-1)$, 我们看到

$$4ab-1 \mid (4a^2-1)^2b^2-(a-b)^2.$$

而$4ab-1 \mid (4a^2-1)^2$, 故$4ab-1 \mid (a-b)^2$.

假如有不同的正整数a, b使得$4ab-1 \mid (a-b)^2$. 取这样的一对正整数(a, b) $(a>b)$使得a达到最小. 写$(a-b)^2=(4ab-1)q$ (其中$q \in \mathbb{Z}^+$), 则$x_1=a$满足二次方程$x^2-(4q+2)bx+b^2+q=0$. 此方程另一个根为$x_2=(4q+2)b-a=(b^2+q)/a \in \mathbb{Z}^+$, 而且$(x_2-b)^2=(4x_2b-1)q$. 依$a$的选取知$x_2 \geqslant a$, 从而$q=ax_2-b^2 \geqslant a^2-b^2$. 于是

$$(a-b)^2=(4ab-1)q \geqslant (4ab-1)(a^2-b^2),$$

从而$a-b \geqslant (4ab-1)(a+b) \geqslant a+b>a-b$. 矛盾。

素数与合数

设$n > 1$为整数，显然1与n为n的（平凡）因子。如果正整数d整除n且$1 < d < n$, 则称d为n的**真因子**(proper divisor). 如果n有真因子，即有大于1的整数c, d使得$cd = n$, 则称n为**合数**(composite number)，n无真因子时称n为**素数**或质数(prime).

2是仅有的偶素数，因为对于整数$n > 1$偶数$2n = 2 \times n$为合数。

100以下的素数依次为

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,$$

$$53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97.$$

整除n的素数叫n的**素因子**(prime divisor). 例如：3与5都是45的素因子。

例题

例1.1. 对于整数$n > 1$, $n^4 + 4$为合数。

证明: 显然

$$n^4 + 4 = (n^2 + 2)^2 - (2n)^2 = (n^2 + 2n + 2)(n^2 - 2n + 2),$$

且

$$n^2 \pm 2n + 2 = (n \pm 1)^2 + 1 > 1.$$

故$n^4 + 4$为合数。

例题

例1.2. 证明无穷整数序列

$$10001,\ 100010001,\ 1000100010001,\ \cdots$$

中每一项都是合数。

证明: 此序列为

$$1+10^4,\ 1+10^4+10^8,\ 1+10^4+10^8+10^{12},\ldots.$$

令$x=10^2=100$, 则首项$1+x^2=73\times 137$为合数。对于$n>2$,

$$1+x^2+x^4+\cdots+x^{2(n-1)}=\frac{(x^2)^n-1}{x^2-1}$$

$$=\begin{cases}\frac{x^n+1}{x+1}\cdot\frac{x^n-1}{x-1} & \text{如果 } 2\nmid n,\\ (x^n+1)\frac{(x^2)^{n/2}-1}{x^2-1} & \text{如果 } 2\mid n.\end{cases}$$

故通项$1+10^4+10^8+\cdots+10^{4(n-1)}$为合数。

最小素因子

引理1.1. 设$n > 1$为整数，则$p = \min\{d > 1 : \ d \mid n\}$必为素数（它叫$n$的最小素因子）。

证明：如果p为合数，则p有真因子d, 从而$1 < d < p$且$d \mid n$, 矛盾。

对于整数$n > 1$, 我们用$p(n)$表示n的最小素因子。

素数有无穷多个

定理1.1 (Euclid). 素数有无穷多个。

证明：反设素数只有有限个，由小到大依次是$p_1, \ldots, p_n$. 令$N = p_1 \cdots p_n + 1$, 则$p(N) \in \{p_1, \ldots, p_n\}$, 从而$N$与$p_1 \cdots p_n$都是$p(N)$倍数。这样

$$1 = N - p_1 \cdots p_n$$

也必须是$p(N)$倍数，矛盾!

Eratosthenes筛法

定理1.2 (爱拉托色尼). 设$m, N \in \mathbb{Z}^+$且$m \in (\sqrt{N}, N]$, 则m为素数当且仅当不超过$\sqrt{N}$的素数都不整除m.

假如m为素数，对于素数$p \leqslant \sqrt{N}$, 显然$p < m$, 从而$p \nmid m$.

如果m为合数，则有整数$q > 1$使得$m = p(m)q$, 于是$m \geqslant p(m)^2$, 从而$p(m) \leqslant \sqrt{m} \leqslant \sqrt{N}$, 于是$p(m)$是$m$的不超过$\sqrt{N}$的素因子。证毕。

爱拉托色尼筛法可用来造素数表。

例子：$10 < m \leqslant 100$时，m为素数当且仅当m不被$2, 3, 5, 7$（10以下的素数）中任一个所整除。

Fermat数

设$a > 1$为整数。如果$n \in \mathbb{Z}^+$有奇素因子p,
则$a^n + 1 = (a^{n/p})^p + 1$有真因子$a^{n/p} + 1$. 因此$a^n + 1$为素数时，$n$必为2的幂次。

1640年Fermat引入今天所说的**Fermat数**：

$$F_n = 2^{2^n} + 1 \quad (n = 0, 1, 2, \ldots).$$

Fermat观察到

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

都是素数，于是他猜测F_n永远是素数。

1732年Euler发现F_5是个合数：

$$F_5 = 2^{32} + 1 = 641 \times 6700417.$$

Fermat数(续)

Pepin判别法（1877）：Fermat数$F_n = 2^{2^n} + 1$为素数当且仅当F_n整除$3^{(F_n-1)/2} + 1$.

使用Pepin判别法与现代计算机，已知$F_6, \ldots, F_{32}$象F_5那样都是合数。人们没有发现前五个之外的Fermat素数。目前已知的最大的Fermat合数为$F_{2747497}$ (2013年发现).

Gauss: 正$n \geq 3$边形可用圆规直尺作出当且仅当n是一些不同Fermat素数与2幂次(包括$2^0 = 1$)之积。特别地，正17边形可用圆规直尺作出.

Fermat数两两无公共素因子

引理1.2. Fermat数两两无公共素因子。

证明：任给正整数n, 我们有

$$\begin{aligned}\prod_{k=0}^{n-1} F_k =&(2^{2^0}-1)(2^{2^0}+1)F_1F_2\cdots F_{n-1}\\ =&(2^{2^1}-1)(2^{2^1}+1)F_2\cdots F_{n-1}\\ =&(2^{2^2}-1)(2^{2^2}+1)F_3\cdots F_{n-1}\\ =&\cdots=(2^{2^{n-1}}-1)(2^{2^{n-1}}+1)=2^{2^n}-1=F_n-2.\end{aligned}$$

如果F_k与F_n $(0\leqslant k<n)$有公共素因子p, 则p整除$F_n-F_0F_1\cdots F_{n-1}=2$, 这与$F_n$为奇数矛盾。因此Fermat数两两无公共素因子。

第n个素数的上界

定理1.3. 对于正整数n, 有小到大排列的第n个素数p_n不超过$2^{2^{n-1}}$.

证明：显然$p_1 = 2 \leqslant 2^{2^{1-1}}$. 下设$n \geqslant 2$. 由上面引理，诸

$$2,\ p(F_0),\ p(F_1),\ \ldots,\ p(F_{n-2})$$

为两两不同的素数且都不超过F_{n-2}. 因此

$$p_n \leqslant F_{n-2} = 2^{2^{n-2}} + 1 \leqslant 2^{2^{n-2}+1} \leqslant 2^{2^{n-1}}.$$

Mersenne素数

设$a > 1$与$n > 1$为整数。如果$a > 2$, 则$a^n - 1$有真因子$a - 1$. 如果n有真因子d, 则$2^n - 1 = (2^d)^{n/d} - 1$有真因子$2^d - 1$. 所以，$a^n - 1$为素数时必定$a = 2$且$n$是个素数。

当p为素数时，$M_p = 2^p - 1$叫梅森(Mersenne)数。十七世纪法国人Mersenne(1588-1648)研究怎样的这样数是素数。
$M_p = 2^p - 1$为素数时，则称M_p是个梅森素数（Mersenne prime）
.

梅森注意到$p = 2, 3, 5, 7, 13, 17, 19, 31$时$M_p$为素数。
但Mersenne数并不总是素数, 例如：

$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89.$$

Mersenne素数（续）

1876年E. Lucas证明了M_{127}是个素数，他使用了下述判别法。

Lucas判别法: 设$S_1 = 4,\ S_{n+1} = S_n^2 - 2\ (n = 1, 2, 3, \ldots)$. 对于素数$p$, M_p为素数当且仅当$M_p \mid S_{p-1}$.

目前已知有51个梅森素数，最大的一个$M_{82589933}$（2018年12月发现）有24862048位，这也是目前已知的最大素数。

GIMPS (Great Internet Mersenne Prime Search)是利用互联网专门搜索梅森素数的项目，网址为https://www.mersenne.org/

§1.2 算术基本定理

定理2.1 (算术基本定理，Gauss). 任何整数$n > 1$可表成有限个素数的乘积，不计因子顺序的话这样的分解还是唯一的。

证明：我们使用串值归纳法。

如果n是个素数（如$n = 2$），则n是一个素数的乘积，且不能写成至少两个素数的乘积。

下设n为合数且$2, \ldots, n-1$都可唯一分解成素数的乘积。写$n = n_1 n_2$, 这里n_1与n_2为大于1的整数。依归纳假设，n_1与n_2都可写成有限个素数的乘积，于是$n = n_1 n_2$也是有限个素数的乘积。

唯一性的证明

再证n分解成素数乘积的方式唯一。假设

$$n = p_1 \cdots p_r = q_1 \cdots q_s,\ p_1 \leqslant \cdots \leqslant p_r,\ q_1 \leqslant \cdots \leqslant q_s,$$

这里诸p_i与q_j均为素数，且$p_1 \geqslant q_1$. 我们要证$r = s$且$p_i = q_i\ (i = 1, \ldots, r)$.

假如$p_1 > q_1$, 则

$$m := (p_1 - q_1)p_2 \cdots p_r = q_1 \cdots q_s - q_1 p_2 \cdots p_r = q_1(q_2 \cdots q_s - p_2 \cdots p_r)$$

有两种不同的素数分解方式，一种含q_1, 另一种不含q_1. (注意$q_1 \nmid p_1 - q_1$且$q_1 < p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$.) 而$m < n$, 故这与归纳假设矛盾。

由上$p_1 = q_1$, 从而$p_2 \cdots p_r = q_2 \cdots q_s = n/p_1$. 依归纳假设, $n/p_1 < n$的素数分解方式唯一，故$r = s$且$p_i = q_i\ (i = 2, \ldots, r)$.

算术基本定理归纳证毕。

标准素数分解式

对于整数$n > 1$, 可写$n = p(n)q$, 其中$q \in \mathbb{Z}^+$. 如果$q > 1$, 则可把q写成素数的乘积。因此$p(n)$必出现在n的素数分解式中。

整数$n > 1$可唯一地写成

$$p_1^{a_1} \cdots p_r^{a_r}$$

的形式，这儿$p_1 < \ldots < p_r$为不同素数，$a_1, \ldots, a_r \in \mathbb{Z}^+$. 这叫$n$的标准素数分解式。$p_1$实际上就是$n$的最小素因子$p(n)$.

例子:

$$360 = 2^3 \times 3^2 \times 5.$$

素数的一个特征性质

推论2.1. 设p为素数，$a_1, \ldots, a_n \in \mathbb{Z}$. 则

$$p \mid a_1 \cdots a_n \iff p \mid a_1 \text{或} p \mid a_2 \text{或} \cdots \text{或} p \mid a_n.$$

证明：$\Leftarrow$：此方向显然。

$\Rightarrow$：如果$\{a_1, \ldots, a_n\}$含0, 则结论显然。下设$a_1, \ldots, a_n$都非零，不妨假定它们都是正整数。由于$p \mid a_1 \cdots a_n$, $m = a_1 \cdots a_n$有个素数分解式含p. 假如$a_1, \ldots, a_n$都不被p整除，则诸$a_i > 1$的素数分解式中都不含p, 从而$m = a_1 \cdots a_n$有个素数分解式不含p. m有两种不同的素数分解方式，这与算术基本定理矛盾。

注记：p为素数且$k \in \{1, \ldots, p-1\}$时,
由$p \mid k!\binom{p}{k} = p(p-1)\cdots(p-k+1)$可得$p \mid \binom{p}{k}$.

$4k-1$形素数有无穷多个

推论2.2. $4k-1$ $(k \in \mathbb{Z}^+)$形素数有无穷多个

证明：假如只有有限个$4k-1$形素数，他们依次为$p_1, \ldots, p_n$. 依算术基本定理，

$$N = 4p_1 \cdots p_n - 1$$

可表成一些奇素数的乘积。N分解式中素数不可能都是$4k+1$形（否则N也是$4k+1$形了），故有$4k-1$形素数p整除N.
因$p \in \{p_1, \ldots, p_n\}$, 又有$p \mid p_1 \cdots p_n$. 于是$1 = 4p_1 \cdots p_n - N$为$p$倍数，矛盾。

类似可证$6k-1$形素数也有无穷多个。

整数在素数处的阶

设p为素数，a为非零整数。显然$p^0 \mid a$, 但n足够大时$p^n > |a|$从而$p^n \nmid a$. 故有唯一的$n \in \mathbb{N}$使得$p^n \mid a$但$p^{n+1} \nmid a$. 此时，我们写$p^n \| a$, 并称n为a在素数p处的**阶**(order), 记为$n = \mathrm{ord}_p a$. 为方便期间，我们约定$\mathrm{ord}_p 0 = +\infty$.

定理2.5. 设p为素数，$a, b \in \mathbb{Z}$. 则

$$\mathrm{ord}_p(ab) = \mathrm{ord}_p a + \mathrm{ord}_p b.$$

证明：a, b之一为0时上式两边都是无穷大。

下设$ab \neq 0$, $\alpha = \mathrm{ord}_p a$且$\beta = \mathrm{ord}_p b$. 写$a = p^\alpha c$, $b = p^\beta d$, 这儿$c, d \in \mathbb{Z}^+$. 显然$p \nmid c$且$p \nmid d$, 于是$p \nmid cd$. 注意$ab = p^{\alpha+\beta} cd$. 故

$$\mathrm{ord}_p(ab) = \alpha + \beta = \mathrm{ord}_p a + \mathrm{ord}_p b.$$

推论2.3

推论2.3. 设$n = p_1^{a_1} \cdots p_r^{a_r}$, 这儿$p_1, \ldots, p_r$为不同素数，$a_1, \ldots, a_r \in \mathbb{N}$. 则

$$\mathrm{ord}_{p_1} n = a_1, \ \ldots, \ \mathrm{ord}_{p_r} n = a_r.$$

证明：$1 \leqslant i \leqslant r$时

$$\mathrm{ord}_{p_i} n = \sum_{j=1}^{r} \mathrm{ord}_{p_i}(p_j^{a_j}) = \sum_{j=1}^{r} a_j \mathrm{ord}_{p_i}(p_j) = a_i.$$

据此推论，我们可更好地理解算术基本定理，原来n分解式中素数p用多少次由$\mathrm{ord}_p n$决定。

$\sqrt[n]{m}$的无理性

例题：设m, n都是大于1的整数，且m不是整数的n次方，试证$\sqrt[n]{m}$为无理数。

证明：假如$\sqrt[n]{m} = a/b$, 这里$a, b \in \mathbb{Z}^+$. 则$a^n = b^n m$. p为素数时，

$$\mathrm{ord}_p m = \mathrm{ord}_p(a^n) - \mathrm{ord}_p(b^n) = n(\mathrm{ord}_p a - \mathrm{ord}_p b).$$

由此知m的素数分解式形如

$$p_1^{na_1} \cdots p_r^{na_r} = (p_1^{a_1} \cdots p_r^{a_r})^n,$$

其中$p_1, \ldots, p_r$为不同素数，$a_1, \ldots, a_r \in \mathbb{N}$. 这与$m$不是整数的$n$次方矛盾。

由此例题知，$\sqrt{2}, \sqrt{3}, \sqrt[3]{6}$等等都是无理数。

一道涉及无理数的例题

例题：证明有正无理数a与b使得a^b为有理数。

证明：已知$\sqrt{2}$为无理数。如果$\sqrt{2}^{\sqrt{2}}$为有理数，则可取$a = b = \sqrt{2}$.

假如$\sqrt{2}^{\sqrt{2}}$为无理数，则可取$a = \sqrt{2}^{\sqrt{2}}$与$b = \sqrt{2}$, 因为

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2.$$

无平方因子正整数

对于整数m, 如果没有整数$d > 1$使得$d^2 \mid m$, 我们就说m **无平方因子**(squarefree). 整数$n > 1$无平方因子当且仅当它是不同素数的乘积。

50以下的无平方因子正整数：

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23,$$

$$26, 29, 30, 31, 33, 34, 35, 37, 38, 39\,41, 42, 43, 46, 47.$$

偶数$2m$与$2m+2$之间有唯一的奇数$2m+1$. 奇数形如$2m+1$ $(m \in \mathbb{Z})$.

由算术基本定理易见，非零整数可唯一地表成ab^2的形式，这儿a是无平方因子整数，$b \in \mathbb{Z}^+$. 例如：

$$2400 = 2^5 \times 3 \times 5^2 = (2^2 5)^2 \times 2 \times 3 = 20^2 \times 6.$$

第n个素数不超过4^n

对$x > 0$, 让$\pi(x)$表示不超过x的素数个数$\sum_{p \leqslant x} 1$求和号中p一般指素数。由于素数有无穷多个，$x \to +\infty$时$\pi(x) \to +\infty$.

定理2.6. $\pi(n) \geqslant \frac{1}{2}\log_2 n$且$p_n \leqslant 4^n$, 这里$p_n$表示第$n$个素数。

证明：不超过n的素数为$p_1, \ldots, p_r$, 这里$r = \pi(n)$.

$1 \leqslant k \leqslant n$时$k$可表成$m_k^2 \prod_{\in I} p_i$的形式，这儿$m_k \in \mathbb{Z}^+$且$I \subseteq \{1, \ldots, r\}$. 显然$m_k \leqslant \sqrt{k} \leqslant \sqrt{n}$. 因此

$$|\{1, \ldots, n\}| \leqslant |\{m \in \mathbb{Z}^+ : \ m \leqslant \sqrt{n}\}| \times |\{I : \ I \subseteq \{1, \ldots, r\}\}| \leqslant \sqrt{n} 2^r,$$

从而$2^r \geqslant \sqrt{n}$, $\pi(n) = r \geq \frac{1}{2}\log_2 n$.

应用上述结果知，$n = \pi(p_n) \geqslant \frac{1}{2}\log_2 p_n$, 从而$p_n \leqslant 2^{2n} = 4^n$.

$n!$在素数处的阶

对于实数x, 地板函数$\lfloor x \rfloor$表示不超过x的最大整数（也叫x的整数部分），天花板函数$\lceil x \rceil$表示不小于x的最小整数。

定理2.7. 设$n \in \mathbb{Z}^+$且p为素数，则

$$\mathrm{ord}_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

证明:

$$\begin{aligned} \mathrm{ord}_p(n!) &= \sum_{k=1}^{n} \mathrm{ord}_p(k) = \sum_{k=1}^{n} \sum_{\substack{i=1 \\ p^i \mid k}}^{k} 1 \\ &= \sum_{i=1}^{n} \sum_{\substack{k=1 \\ p^i \mid k}}^{n} 1 = \sum_{i=1}^{n} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor . \end{aligned}$$

例题

例题. 100!的十进制表示中最后有连续多少个零?

解: $10 = 2 \times 5$. 由上述定理,

$$\mathrm{ord}_2(100!) = \sum_{i=1}^{6} \left\lfloor \frac{100}{2^i} \right\rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97,$$

且

$$\mathrm{ord}_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 20 + 4 = 24.$$

因此

$$10^{24} = 2^{24}5^{24}$$

整除100!, 但$10^{25} \nmid 100!$, 故答案为24.

Legendre定理

定理2.8 (Legendre). 对于素数p与$n \in \mathbb{Z}^+$, 我们有

$$\mathrm{ord}_p(n!) = \frac{n - \sigma_p(n)}{p-1},$$

这里$\sigma_p(n)$是n的p进制表示中各位数之和.

证明: 写$n = \sum_{i=0}^{k} a_i p^i$, 其中$a_i \in \{0, 1, \ldots, p-1\}$. 对于$i = 1, \ldots, k$, 我们有

$$n = p^i \sum_{j=i}^{k} a_j p^{j-i} + r_i, \text{ 其中 } r_i = \sum_{j=0}^{i-1} a_j p^j \leqslant \sum_{j=0}^{i-1} (p-1)p^j = p^i - 1.$$

因此

$$\begin{aligned}\mathrm{ord}_p(n!) &= \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^{k} \sum_{j=i}^{k} a_j p^{j-i} \\ &= \sum_{j=1}^{k} a_j \sum_{i=1}^{j} p^{j-i} = \sum_{j=1}^{k} a_j \frac{p^j - 1}{p-1} = \frac{n - \sigma_p(n)}{p-1}.\end{aligned}$$

Kummer定理

设p为素数. 对$a, b \in \mathbb{N}$, 我们让$\tau_p(a, b)$表示p进制的a与b相加时向前进位的位个数。例如：$\tau_2(9, 3) = \tau_2(1001_2, 11_2) = 2$.

定理2.9 (E. Kummer). 设p为素数，$a, b \in \mathbb{N}$. 则

$$\tau_p(a, b) = \mathrm{ord}_p \binom{a+b}{a} = \frac{\sigma_p(a) + \sigma_p(b) - \sigma_p(a+b)}{p-1}.$$

证明：固定$i \in \mathbb{N}$并写

$$a = p^{i+1} \left\lfloor \frac{a}{p^{i+1}} \right\rfloor + a', \ b = p^{i+1} \left\lfloor \frac{b}{p^{i+1}} \right\rfloor + b',$$

这里$a', b' \in \{0, \ldots, p^{i+1} - 1\}$. p进制的a与b相加时在右数i位（最右边叫第0位）向前进位当且仅当$a' + b' \geqslant p^{i+1}$ (即$\lfloor (a' + b')/p^{i+1} \rfloor = 1$). 注意

$$\frac{a+b}{p^{i+1}} = \left\lfloor \frac{a}{p^{i+1}} \right\rfloor + \left\lfloor \frac{b}{p^{i+1}} \right\rfloor + \frac{a' + b'}{p^{i+1}}.$$

Kummer定理的证明

于是

$$\left\lfloor \frac{a'+b'}{p^{i+1}} \right\rfloor = \left\lfloor \frac{a+b}{p^{i+1}} \right\rfloor - \left\lfloor \frac{a}{p^{i+1}} \right\rfloor - \left\lfloor \frac{b}{p^{i+1}} \right\rfloor .$$

由上可见，

$$\begin{aligned}
\tau_p(a,b) =& \sum_{i=0}^{\infty} \left(\left\lfloor \frac{a+b}{p^{i+1}} \right\rfloor - \left\lfloor \frac{a}{p^{i+1}} \right\rfloor - \left\lfloor \frac{b}{p^{i+1}} \right\rfloor \right) \\
=& \sum_{i=0}^{\infty} \left\lfloor \frac{a+b}{p^{i+1}} \right\rfloor - \sum_{i=0}^{\infty} \left\lfloor \frac{a}{p^{i+1}} \right\rfloor - \sum_{i=0}^{\infty} \left\lfloor \frac{b}{p^{i+1}} \right\rfloor \\
=& \operatorname{ord}_p((a+b)!) - \operatorname{ord}_p(a!) - \operatorname{ord}_p(b!) = \operatorname{ord}_p \frac{(a+b)!}{a!b!} \\
=& \frac{a+b-\sigma_p(a+b)}{p-1} - \frac{a-\sigma_p(a)}{p-1} - \frac{b-\sigma_p(b)}{p-1} \\
=& \frac{\sigma_p(a)+\sigma_p(b)-\sigma_p(a+b)}{p-1}.
\end{aligned}$$

§1.3 Chebyshev不等式

素数定理(The Prime Number Theorem).

$$\pi(x) \sim \frac{x}{\log x}, \text{ 即 } \lim_{x\to+\infty} \frac{\pi(x)}{x/\log x} = 1.$$

此结果由Legendre与Gauss各自独立猜出，1896年被Hadamard与Poussin各自独立地运用复变函数论所证明。1949年Selberg与Erdős发现了初等的不用复变函数的证明。

定理3.1 (i) (Chebyshev, 1852) 有正常数c_1与c_2使得对任何$x \geqslant 2$有不等式

$$c_1 \frac{x}{\log x} \leqslant \pi(x) \leqslant c_2 \frac{x}{\log x}.$$

(ii) (Bertrand假设，由Chebyshev所证明). 任给$x \geqslant 1$, 区间$(x, 2x]$中必有素数。

Erdős的一个结果

定理3.2 (Erdős). 对于$n = 2, 3, \ldots,$ 不超过n的素数之积$\prod_{p\leqslant n} p$ (其中p为素数)小于4^n.

证明：$n = 2$时，$\prod_{p\leqslant n} p = 2 < 4^2$.

设$n > 2$且对$m = 2, \ldots, n-1$已有$\prod_{p\leqslant m} p < 4^m$. 如果$n$为合数，则$\prod_{p\leqslant n} p = \prod_{p\leqslant n-1} p < 4^{n-1} < 4^n$.

下设n为素数。这时$2 \leqslant m = \frac{n+1}{2} < n$. 依归纳假设, $\prod_{p\leqslant m} p < 4^m = 2^{2m} = 2^{n+1}$. 如果素数$p$满足$m < p \leqslant n$, 则$p$整除

$$n(n-1)\cdots m = \frac{n!}{(m-1)!} = \frac{n!}{(n-m)!} = m!\binom{n}{m},$$

从而$p \mid \binom{n}{m}$. 因此

$$\prod_{m<p\leqslant n} p \leqslant \binom{n}{m} = \frac{1}{2}\left(\binom{n}{m} + \binom{n}{n-m}\right) = \frac{1}{2}\sum_{k=0}^{n}\binom{n}{k} = 2^{n-1}.$$

于是$\prod_{p\leqslant n} p = \prod_{p\leqslant m} p \times \prod_{m<p\leqslant n} p \leqslant 2^{n+1}2^{n-1} = 4^n$.

Chebyshev θ-函数

1852年，Chebyshev引入θ-函数

$$\theta(x) = \sum_{p \leq x} \log p \ (p\text{为素数}),$$

并证明了素数定理等价于$\theta(x) \sim x$.

推论3.1. $x \geqslant 2$时$\theta(x) < (2\log 2)x$且$\pi(x) \leq 5\frac{x}{\log x}$. 此外，第$n$个素数$p_n$大于$\frac{n}{5}\log n$.

证明：

$$\prod_{p \leqslant x} p = \prod_{p \leq \lfloor x \rfloor} p < 4^{\lfloor x \rfloor} \leqslant 4^x = 2^{2x},$$

取对数得

$$\theta(x) = \sum_{p \leqslant x} \log p < (2\log 2)x.$$

继续证明

由于

$$\theta(x) \geqslant \sum_{\sqrt{x}<p\leqslant x} \log p \geqslant (\pi(x)-\pi(\sqrt{x}))\log\sqrt{x} \geqslant (\pi(x)-\sqrt{x})\log\sqrt{x},$$

我们有

$$\pi(x) \leqslant \sqrt{x} + \frac{\theta(x)}{\log\sqrt{x}} \leqslant \sqrt{x} + \frac{(2\log 2)x}{(\log x)/2}.$$

因$e^{\sqrt{2x}} \geqslant (\sqrt{2x})^2/2! = x$, 我们有$\sqrt{2x} \geqslant \log x$, 从而$\sqrt{x} \leqslant \sqrt{2}x/(\log x)$. 因此

$$\pi(x) \leqslant (\sqrt{2} + 4\log 2)\frac{x}{\log x} < 5\frac{x}{\log x}.$$

由

$$n = \pi(p_n) < 5\frac{p_n}{\log p_n} \leqslant 5\frac{p_n}{\log n},$$

我们得到$p_n > \frac{1}{5} n\log n$.

更精细的不等式

素数定理$\pi(x) \sim \frac{x}{\log x}$也等价于$p_n \sim n \log n$, 这儿$p_n$表示第$n$个素数。

P. Dusart [Math. Comp. 68(1999)]: (i) 对任何$x > 1$有

$$\pi(x) \leqslant \frac{x}{logx}\left(1 + \frac{1.2762}{\log x}\right).$$

对任何$x \geqslant 599$有

$$\pi(x) \geqslant \frac{x}{\log x}\left(1 + \frac{0.992}{\log x}\right).$$

(ii) $n \geqslant 2$时$p_n \geqslant n(\log n + \log\log n - 1)$. 当$n \geqslant 6$时，$p_n \leqslant n(\log n + \log\log n)$.

(iii) 对任何$x \geqslant 3275$, 必有素数p使得

$$x \leqslant p \leqslant x + \frac{x}{2\log^2 x}.$$

Legendre猜想与Redmond-Sun猜想

Legendre猜想. 任给正整数n, n^2与$(n+1)^2$之间必有素数(这也等价于$\sqrt{p_{n+1}}-\sqrt{p_n}<1$).

我们用$f(x)=O(g(x))$(或$f(x)\ll g(x)$)表示有常数$C>0$使得$|f(x)|\leqslant C|g(x)|$. 2001年R.C. Baker, G. Harman与J. Pintz证明了$p_{n+1}-p_n=O(p_n^{0.525})$.

Legendre猜想与Catalan猜想都是下述猜想的特殊情形。

Redmond-Sun猜想 (2006). 形如$[x^m,y^n]$ $(x,y,m,n\in\{2,3,\ldots\}$且$x^m<y^n)$的区间中含有素数，除了有限个例外。具体说来，这些例外区间如下：

$$[2^3,3^2],\ [5^2,3^3],\ [2^5,6^2],\ [11^2,5^3],\ [3^7,13^3],$$
$$[5^5,56^2],\ [181^2,2^{15}],\ [43^3,282^2],\ [46^3,312^2],\ [22434^2,55^5].$$

此猜测已被验证到4.5×10^{18}, 参见http://oeis.org/A116086.

§1.4 最大公因数与最小公倍数

定理4.1 ($\mathbb{Z}$上的带余除法). 设$a, b \in \mathbb{Z}$且$b \neq 0$, 则有唯一的一对整数q与r使得$a = bq + r$且$0 \leqslant r < |b|$ (其中r叫a被b除所得的**最小非负余数**).

证明：x与b同号且$|x|$充分大时，$bx \geqslant |a|$. 因此集合$S = \{a + bx : x \in \mathbb{Z}\}$包含自然数。设$S$中最小的自然数为$r = a - bq$, 这儿$q \in \mathbb{Z}$. 如果$r \geqslant |b|$, 则$r_0 = r - |b| \in S$且$0 \leqslant r_0 < r$, 这与$r$的选取矛盾。因此$0 \leqslant r < |b|$.

如果还有$a = bq' + r'$ (其中$q', r' \in \mathbb{Z}$且$0 \leqslant r' < |b|$), 则$|b(q - q')| = |r' - r| < |b|$, 从而$q = q'$且$r = r'$. 证毕。

注记. $a \in \mathbb{Z}$且$b \in \mathbb{Z}^+$时，作带余除法$a = bq + r$ (其中$q \in \mathbb{Z}$且$r \in \{0, \ldots, b-1\}$)，则

$$\frac{a}{b} = q + \frac{r}{b}, \ \left\lfloor \frac{a}{b} \right\rfloor = q, \ \left\{ \frac{a}{b} \right\} = \frac{r}{b}.$$

绝对最小剩余

推论4.1. 设$a, b \in \mathbb{Z}$且$b \neq 0$, 则有唯一的$q_0, r_0 \in \mathbb{Z}$使得$a = bq_0 + r_0$且$-|b|/2 < r_0 \leqslant |b|/2$.

注记. 此推论中的r_0叫做a被b除所得的**绝对最小剩余**。

推论4.1的证明：作带余除法$a = bq + r$, 这儿$q \in \mathbb{Z}$且$0 \leqslant r < |b|$.

如果$r \leqslant |b|/2$, 可取$q_0 = q$, $r_0 = r$.

如果$r > |b|/2$, 可取$q_0 = q + |b|/b$, $r_0 = r - |b|$. 显然$a = bq_0 + r_0$且$-|b|/2 < r_0 \leqslant |b|/2$.

绝对最小剩余

再证唯一性。假定还有$q_1, r_1 \in \mathbb{Z}$使得$a = bq_1 + r_1$且$-|b|/2 < r_1 \leqslant |b|/2$, 则

$$r_1 - r_0 = (a - bq_1) - (a - bq_0) = b(q_0 - q_1).$$

如果$|r_0| = |r_1| = |b|/2$, 则$r_1 = r_0 = |b|/2$. 如果$|r_0|$与$|r_1$不全是$|b|/2$, 则

$$|r_1 - r_0| \leqslant |r_1| + |r_0| < \frac{|b|}{2} + \frac{|b|}{2} = |b|,$$

从而也有$r_1 = r_0$. 既然$r_1 = r_0$, 自然也有$q_1 = q_0$.

例题

例题： 求-2与7被4除所得的最小非负剩余与绝对最小剩余。

解：$-2 = 4 \times (-1) + 2$, 故-2被4除的最小非负剩余与最小绝对剩余都是2.

$7 = 4 \times 1 + 3 = 4 \times 2 - 1$, 故7被4除的最小非负剩余与最小绝对剩余分别时3与-1.

例题： 求奇数的平方被8除所得的最小非负余数。

解：任给整数m, 显然$m(m+1)$为偶数，三角数$T_m = \frac{m(m+1)}{2} \in \mathbb{Z}$. 于是

$$(2m+1)^2 = 4m^2 + 4m + 1 = 4m(m+1) + 1 = 8T_m + 1$$

被8除余1.

最大公因数与最小公倍数

设$a_1, \ldots, a_n$为整数.

如果$d \in \mathbb{Z}$整除$a_1, \ldots, a_n$中每一个，则称d为$a_1, \ldots, a_n$ 的**公因数** (common divisor). 如果$d \in \mathbb{N}$为$a_1, \ldots, a_n$的公因数且$a_1, \ldots, a_n$的任何公因数都整除d，则称d为$a_1, \ldots, a_n$ 的**最大公因数** (greatest common divisor).

如果$m \in \mathbb{Z}$被$a_1, \ldots, a_n$中每一个所整除，我们就称m为$a_1, \ldots, a_n$ 的**公倍数**. 如果$m \in \mathbb{N}$ 为$a_1, \ldots, a_n$的公倍数且它整除$a_1, \ldots, a_n$的任何公倍数，则称m为$a_1, \ldots, a_n$ 的**最小公倍数** (least common multiple).

最大公因数与最小公倍数基本性质

定理4.2. 任给整数$a_1, \ldots, a_n$, 它们的最大公因数存在且唯一（记为$(a_1, \ldots, a_n)$), 它们的最小公倍数也存在且唯一（记为$[a_1, \ldots, a_n]$).

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = \{a_1x_1 + \cdots + a_nx_n : \ x_1, \ldots, x_n \in \mathbb{Z}\}$$

等于$(a_1, \ldots, a_n)\mathbb{Z}$, 且$a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z} = [a_1, \ldots, a_n]\mathbb{Z}$.

证明：我们只针对最大公因数来证明所要结论。显然集合$S = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$包含0. 如果$S$中没有非零数，则$S = 0\mathbb{Z}$. 假定$S$中有非零整数，则其中必有正整数（因为$a \in S$时$-a \in S$）。让$d$表示$S$中最小的正整数，则$d\mathbb{Z} \subseteq S$. 任给$s \in S$, 作带余除法$s = dq + r$, 其中$q \in \mathbb{N}$且$r \in \{0, \ldots, d-1\}$. 由于$s, d \in S$, 我们有$r = s - dq \in S$. 如果$0 < r < d$, 则与$d$为$S$中最小元矛盾。因此$r = 0$, $d = dq \in d\mathbb{Z}$.

由上，有$d \in \mathbb{N}$使得$d\mathbb{Z} = S$. $1 \leqslant i \leqslant n$时$a_i \in S = d\mathbb{Z}$, 从而$d$为$a_1, \ldots, a_n$的公因子。如果$c$为$a_1, \ldots, a_n$的公因数，则$S$中每个元(包括$d$)都是$c$倍数。因此$d$恰为$a_1, \ldots, a_n$的最大公因数。如果$d'$也是$a_1, \ldots, a_n$的最大公因数，则$d \mid d'$且$d' \mid d$, 从而$d = d'$.

最大公因数与最小公倍数基本性质

$$(aa_1, \ldots, aa_n) = |a|(a_1, \ldots, a_n),$$
$$[aa_1, \ldots, aa_n] = |a|[a_1, \ldots, a_n].$$

$$(a_1, \ldots, a_n, 0) = (a_1, \ldots, a_n) \text{ 且 } [a_1, \ldots, a_n, 0] = 0.$$

$$(a_1, \ldots, a_n) = ((a_1, \ldots, a_k), (a_{k+1}, \ldots, a_n)),$$
$$[a_1, \ldots, a_n] = [[a_1, \ldots, a_k], [a_{k+1}, \ldots, a_n]].$$

$$[(a, b), c] = ([a, c], [b, c]),$$
$$([a, b], c) = [(a, c), (b, c)].$$

整数的互素

如果1是$a, b \in \mathbb{Z}$的最大公因子，即$a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, 则称$a$与$b$互素(coprime或者relatively prime).

定理4.3. (i) 设$a, b, c \in \mathbb{Z}$, 且a与b互素，那么$(a, bc) = (a, c)$, 特别地$a \mid bc \iff a \mid c$.

(ii) 对于$a, b \in \mathbb{Z}$, 我们有

$$(a, b)[a, b] = |ab|.$$

(i)的证明：这是因为

$$a\mathbb{Z} + bc\mathbb{Z} = (a\mathbb{Z} + ac\mathbb{Z}) + bc\mathbb{Z} = a\mathbb{Z} + (a\mathbb{Z} + b\mathbb{Z})c = a\mathbb{Z} + c\mathbb{Z}.$$

于是

$$a \mid bc \iff (a, bc) = |a| \iff (a, c) = |a| \iff a \mid c.$$

第二部分的证明

(ii)的证明：如果$a = b = 0$,

则$(a, b)[a, b] = (0, 0)[0, 0] = 0 \times 0 = |ab\|$.

下设a, b不全为0, 于是$d = (a, b) > 0$. 显然

$$\frac{ab}{d} = a\frac{b}{d} = \frac{a}{d}b$$

是a, b的公倍数。如果$m \in \mathbb{Z}$是a与b的公倍数，则ab整除am与bm, 于是ab整除am, bm最大公因子dm, 从而$\frac{ab}{d} \mid m$. 因此$|ab/d| = [a, b]$, 即$(a, b)[a, b] = |ab|$.

一个例题

例题. 设a与b为互素的正整数，且$ab = z^n$, 这儿$z \in \mathbb{Z}^+$. 证明有互素的正整数x与y使得$a = x^n$, $b = y^n$, 且$xy = z$.

证明：任给素数p, 如果$p \nmid a$, 则$\mathrm{ord}_p a = 0$为n倍数。如果$p \mid a$, 则$p \nmid b$, 从而

$$\mathrm{ord}_p a = \mathrm{ord}_p a + \mathrm{ord}_p b = \mathrm{ord}_p ab = n\,\mathrm{ord}_p z.$$

可见总有$n \mid \mathrm{ord}_p a$. 同理, $n \mid \mathrm{ord}_p b$.

令$x = \prod_p p^{(\mathrm{ord}_p a)/n}$, $y = \prod_P^{(\mathrm{ord}_p b)/n}$, 则$x, y \in \mathbb{Z}^+$, $x^n = a$, $y^n = b$. 由于$(x^n, y^n) = (a, b) = 1$, 我们有$(x, y) = 1$. 考虑到$(xy)^n = ab = z^n$, 又有$xy = z$.

注记：由此例题可证方程$x^2 + y^2 = z^2$ $(2 \mid y)$的整数通解为

$$x = k(m^2 - n^2),\ y = 2kmn,\ z = k(m^2 + n^2)\ (\text{其中} k, m, n \in \mathbb{Z}).$$

利用素数分解式求两个整数最大公因数

定理4.4. 设$a_i = p_1^{a_{i1}} \cdots p_r^{a_{ir}}$ $(i = 1, \ldots, n)$, 这儿$p_1, \ldots, p_r$为不同素数，$a_{i1}, \ldots, a_{ir} \in \mathbb{N}$. 则

$$(a_1, \ldots, a_n) = \prod_{j=1}^{r} p_j^{\alpha_j}, \quad [a_1, \ldots, a_n] = \prod_{j=1}^{r} p_j^{\alpha'_j},$$

其中$\alpha_j = \min\{a_{1j}, \ldots, a_{nj}\}$, $\alpha'_j = \max\{a_{1j}, \ldots, a_{nj}\}$.

证明：$\beta_1, \ldots, \beta_r \in \mathbb{N}$时，$\prod_{j=1}^{r} p_j^{\beta_j}$为$a_1, \ldots, a_n$公因子当且仅当对$i = 1, \ldots, n$都有$\beta_j \leqslant a_{ij}$, 从而当且仅当$\beta_j \leqslant \alpha_j$ $(j = 1, \ldots, r)$. 因此$(a_1, \ldots, a_n) = \prod_{j=1}^{r} p_j^{\alpha_j}$. 类似可证$[a_1, \ldots, a_n] = \prod_{j=1}^{r} p_j^{\alpha'_j}$.

利用素数分解式求两个整数最大公因数

例题：求36与40的最大公因数与最小公倍数。

解：$36 = 2^2 \times 3^2$, $40 = 2^3 \times 5$. 亦即

$$36 = 2^2 \times 3^2 \times 5^0, \quad 40 = 2^3 \times 3^0 \times 5.$$

故

$$(36, 40) = 2^{\min\{2,3\}} 3^{\min\{2,0\}} 5^{\min\{0,1\}} = 2^2 \times 3^0 \times 5^0 = 4,$$

$$[36, 40] = 2^{\max\{2,3\}} 3^{\max\{2,0\}} 5^{\max\{0,1\}} = 2^3 \times 3^2 \times 5^1 = 360.$$

一道美国奥数题

例题：对于整数a, b, c, 证明

$$\frac{[a,b,c]^2}{[a,b][b,c][c,a]} = \frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}.$$

证明：写

$$a = p_1^{a_1} \cdots p_n^{a_n},\ b = p_1^{b_1} \cdots p_n^{b_n},\ c = p_1^{c_1} \cdots p_n^{c_n},$$

其中$p_1, \ldots, p_n$为不同素数，诸a_i, b_i, c_i为非负整数. 则

$$\begin{aligned}\frac{[a,b,c]^2}{[a,b][b,c][c,a]} &= \prod_{i=1}^{n} \frac{(p_i^{\max\{a_i,b_i,c_i\}})^2}{p_i^{\max\{a_i,b_i\}} p_i^{\max\{b_i,c_i\}} p_i^{\max\{c_i,a_i\}}} \\ &= \prod_{i=1}^{n} p_i^{2\max\{a_i,b_i,c_i\} - (\max\{a_i,b_i\} + \max\{b_i,c_i\} + \max\{c_i,a_i\})}\end{aligned}$$

继续证明

同理,

$$\frac{(a,b,c)^2}{(a,b)(b,c)(c,a)} = \prod_{i=1}^{n} p_i^{2\min\{a_i,b_i,c_i\}-(\min\{a_i,b_i\}+\min\{b_i,c_i\}+\min\{c_i,a_i\})}.$$

故只要对$i = 1, \ldots, n$说明

$$\begin{aligned} &2\max\{a_i,b_i,c_i\} - (\max\{a_i,b_i\} + \max\{b_i,c_i\} + \max\{c_i,a_i\}) \\ &= 2\min\{a_i,b_i,c_i\} - (\min\{a_i,b_i\} + \min\{b_i,c_i\} + \min\{c_i,a_i\}). \end{aligned}$$

由对称性，不妨设$a_i \geqslant b_i \geqslant c_i$, 于是上式化为

$$2a_i - (a_i + b_i + a_i) = 2c_i - (b_i + c_i + c_i).$$

这是显然的。

辗转相除法

定理4.5. 任给$r_0 \in \mathbb{Z}$与$r_1 \in \mathbb{Z}^+$, 在作辗转相除如下：

$$\begin{aligned}
r_0 &= q_0 r_1 + r_2,\ 0 < r_2 < r_1;\\
r_1 &= q_1 r_2 + r_3,\ 0 < r_3 < r_2;\\
&\cdots\cdots\cdots\cdots\\
r_{k-2} &= q_{k-2} r_{k-1} + r_k,\ 0 < r_k < r_{k-1};\\
r_{k-1} &= q_{k-1} r_k + r_{k+1},\ r_{k+1} = 0.
\end{aligned}$$

则r_k是r_0与r_1的最大公因数，而且利用$r_i = r_{i-2} - q_{i-2} r_{i-1}$ $(k \geqslant i > 1)$可找到一组$x, y \in \mathbb{Z}$使得$r_k = r_0 x + r_1 y$.

定理4.5的证明

证明：由于r_1下没有无穷多个正整数，辗转相除总在进行有穷步后结束。

任给$1 \leqslant i \leqslant k$, 由于$r_{i-1} - r_{i+1} = q_{i-1}r_i$, 我们有

$$r_{i-1}\mathbb{Z} + r_i\mathbb{Z} = r_i\mathbb{Z} + r_{i+1}\mathbb{Z}.$$

因此

$$r_0\mathbb{Z}+r_1\mathbb{Z} = r_1\mathbb{Z}+r_2\mathbb{Z} = \cdots = r_{k-1}\mathbb{Z}+r_k\mathbb{Z} = r_k\mathbb{Z}+r_{k+1}\mathbb{Z} = r_k\mathbb{Z},$$

从而r_k就是r_0与r_1的最大公因子。

r_k可表成r_{k-1}, r_{k-2}的线性组合$r_{k-2} - q_{k-2}r_{k-1}$.
而$r_{k-1} = r_{k-3} - q_{k-3}r_{k-2}$, 故$r_k$可表成$r_{k-2}, r_{k-3}$的线性组合。如此一直倒着利用$r_i = r_{i-2} - q_{i-2}r_{i-1}$ $(k \geqslant i > 1)$，最终可将r_k表成r_0与r_1的线性组合，即找到$x, y \in \mathbb{Z}$使$r_0x + r_1y = r_k$.

例题

例题： 求整数771与426的最大公因数以及方程$771x + 426y = (771, 426)$的一组整数解。

解：作辗转相除如下：

$$\begin{aligned}
771 =& 1 \times 426 + 345,\ 426 = 1 \times 345 + 81,\\
345 =& 4 \times 81 + 21,\ 81 = 3 \times 21 + 18,\\
21 =& 1 \times 18 + 3,\ 18 = 6 \times 3 + 0.
\end{aligned}$$

故$(771, 426) = 3$.

$$\begin{aligned}
3 =& 21 - 18 = 21 - (81 - 3 \times 21) = 4 \times 21 - 81\\
=& 4(345 - 4 \times 81) - 81 = 4 \times 345 - 17 \times 81\\
=& 4 \times 345 - 17(426 - 345) = 21 \times 345 - 17 \times 426\\
=& 21(771 - 426) - 17 \times 426 = 21 \times 771 - 38 \times 426.
\end{aligned}$$

故方程$771x + 426y = 3$有解$x = 21,\ y = -38$.

$a^m - 1$与$a^n - 1$的最大公因子

定理4.6. 设$a \in \mathbb{Z}$, $m, n \in \mathbb{N}$. 则

$$(a^m - 1, a^n - 1) = |a^{(m,n)} - 1|.$$

证明：$mn = 0$时结论显然. 例如，
$a^{(0,n)} - 1 = a^n - 1$是$a^0 - 1 = 0$与$a^n - 1$最大公因子。

下设$r_0 = m$与$r_0 = n$都是正整数。作辗转相除如下：

$$r_{i-1} = q_i r_i + r_{i+1} \ (i = 1, \ldots, k),$$

其中$q_1, \ldots, q_k, r_2, \ldots, r_k \in \mathbb{N}$且

$$r_1 > r_2 > \cdots > r_k > r_{k+1} = 0.$$

继续证明定理4.6

注意

$$(x-1)(x^{q-1}+\cdots+x+1)=x^q-1\ (q=1,2,3,\ldots).$$

故$1\leqslant i\leqslant k$时

$$\begin{aligned}a^{r_{i-1}}-1=&a^{q_i r_i+r_{i+1}}-1=a^{r_{i+1}}((a^{r_i})^{q_i}-1)+a^{r_{i+1}}-1\\=&(a^{r_i}-1)?+a^{r_{i+1}}-1,\end{aligned}$$

从而

$$(a^{r_{i-1}}-1)\mathbb{Z}+(a^{r_i}-1)\mathbb{Z}=(a^{r_i}-1)\mathbb{Z}+(a^{r_{i+1}}-1)\mathbb{Z}.$$

于是

$$\begin{aligned}&(a^m-1)\mathbb{Z}+(a^n-1)\mathbb{Z}=(a^{r_0}-1)\mathbb{Z}+(a^{r_1}-1)\mathbb{Z}\\=&\cdots=(a^{r_k}-1)\mathbb{Z}+(a^{r_{k+1}}-1)\mathbb{Z}=(a^{(m,n)}-1)\mathbb{Z},\end{aligned}$$

因此$|a^{(m,n)}-1|$就是a^m-1与a^n-1的最大公因数。

推论

对于整数$a > 1$与$m, n \in \mathbb{N}$,

$$\begin{aligned} a^m - 1 \mid a^n - 1 &\iff (a^m - 1, a^n - 1) = a^m - 1 \\ &\iff a^{(m,n)} - 1 = a^m - 1 \\ &\iff (m, n) = m \\ &\iff m \mid n. \end{aligned}$$

再谈Mersenne数

定理4.7. (i) Mersenne数两两互素。

(ii) 对于素数p, $M_p = 2^p - 1$的素因子被p除余1.

证明：(i) 设p与q为不同的素数，则

$$(2^p - 1, 2^q - 1) = 2^{(p,q)} - 1 = 2^1 - 1 = 1.$$

(ii) 设q为M_p的素因子，则q整除$2^p - 1$. 注意

$$2^q - 2 = (1+1)^q - 1 - 1 = \sum_{k=1}^{q} \binom{q}{k} \in q\mathbb{Z},$$

而q为奇数，故q整除$2^{q-1} - 1$. 于是q整除

$$(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1,$$

从而$(p, q-1) > 1$, $p \mid q - 1$.

偶完全数的刻画

正整数n为完全数(perfect number)指它的因子和$\sigma(n) = 2n$, 即

$$\sum_{\substack{d|n \\ 1\leqslant d<n}} d = n.$$

例如：$6 = 1 + 2 + 3$, 于是6是完全数。

定理4.8. 正整数n为偶完全数 $\Longleftrightarrow$ n形如$2^{p-1}M_p$, 这儿p与$M_q = 2^p - 1$为素数。

证明：$\Leftarrow$ (Euclid): 设p与$q = 2^p - 1$为素数，$n = 2^{p-1}q$的所有因子和为

$$\begin{aligned}\sigma(n) =& 1 + 2 + 2^2 + \cdots + 2^{p-1} + q + 2q + \cdots + 2^{p-1}q \\ =& (1 + 2 + \cdots + 2^{p-1})(q + 1) = (2^p - 1)2^p = 2n.\end{aligned}$$

故n为偶完全数。

另一方向的证明

$\Leftarrow$ (Euler): 设$n = 2^a m$为偶完全数，这儿$a \in \mathbb{Z}^+$, m为正奇数。注意

$$\sigma(n) = \sum_{b=0}^{a} \sum_{d|m} 2^b d = \sum_{b=0}^{a} 2^b \sum_{d|m} d = \frac{2^{a+1}-1}{2-1}\sigma(m).$$

于是

$$2^{a+1}m = 2n = \sigma(n) = (2^{a+1}-1)\sigma(m),$$

有$d \in \mathbb{Z}^+$使得$\sigma(m) = 2^{a+1}d$, 从而$m = (2^{a+1}-1)d$. 注意

$$\sigma(m) = 2^{a+1}d = m + d,$$

从而d, m是m仅有的不同因子。因此m为素数且$d = 1$.

由$2^{a+1} - 1 = m$为素数知$p = a + 1$为素数

且$m = M_p$为Mersenne素数。注意$n = 2^a m = 2^{p-1}M_p$.

Graham猜想

R. L. Graham (1935-2019) 在1970年提出如下猜测。

Graham猜想：任给不同的正整数$a_1, \ldots, a_n$, 必有$1 \leqslant i, j \leqslant n$使得

$$\frac{a_i}{(a_i, a_j)} \geqslant n.$$

1986年，Szegedy证明了n充分大时成立。

1996年Soundarajan等彻底证实了这一猜想。

参考书

孙智伟，基础数论入门，哈尔滨工业大学出版社，2014.

谢谢!