第一章 整数的可除性

1.1 整除的概念、欧几里得除法

1. $a=q\cdot b \longrightarrow b|a$

b整除a (a被b整除)

$30=15\times2=10\times3$

$2|30$, $15|30$, $10|30$, $3|30$

2. $b|a$, 则$\pm b|\pm a$ 都成立

传递性: $b|a$, $c|b \longrightarrow c|a$

$7|42$, $42|84 \longrightarrow 7|84$

加减性: $c|a$, $c|b$ $\begin{cases}\longrightarrow c|(a+b)\\ \longrightarrow c|(a-b)\end{cases}$

$a=q_1c$, $b=q_2c$

$a+b=(q_1+q_2)c$, $a-b=(q_1-q_2)c$

$c|a$, $c|b \longrightarrow c|(s\cdot a+t\cdot b)$

推论

$7|14$, $7|21 \longrightarrow 7|(21-14)=7|7$

$7|(3\times21-4\times14)=7|7$ ...

$7|(3\times21+4\times14)=7|119$

再推论: $c|a$, $c|b$, 若有 $s\cdot a+t\cdot b=1$, 则 $c=\pm1$

即 $c|(s\cdot a+t\cdot b)=c|1$

只有 $c=\pm1$ 的可能了

再推论: $c\neq0$, $a_1a_2\cdots a_n$ 的 c 的倍数

即 $c|a_n$, 有任意 n 个整数 $s_1\cdots s_n$

$s_1a_1+s_2a_2+\cdots+s_na_n$ 为 c 的倍数

显然成立.

$7|14,\ 7|21,\ 7|35$

$\Rightarrow 7|(5\times2(+4\times14-3\times35)=7|56$

3. $a|b,\ b|a \rightarrow a=\pm b$

由整除引出 $\begin{cases}\text{素数}(\text{因数只有}\pm1\text{和}\pm n)\\ \text{合数}(\text{非素数})\end{cases}$

$\Downarrow$

每个合数必有素因子 $\Rightarrow$ 合数能分解为素数乘积

反证：对于合数来说，必有因子 P，$1<P<$ 该合数，为最小的因子

若 P 为素，成立。

P 为合，则有更小因子，与假设矛盾。

综上，对于合数来说，必有最小因子为素数。

4. Eratosthenes 筛法 $\rightarrow$ 找素数

其实就是把素数列出来。

① 素数 2 $\rightarrow$ 去掉 $2\times2,\ 2\times3,\ 2\times4\cdots$

② 素数 3 $\rightarrow$ 去 $2\times3,\ 3\times3,\ 4\times3,\ 5\times3\cdots$

③ 素数 5 $\rightarrow$ 去 $2\times5,\ 3\times5,\ 4\times5\cdots$

④ 7 $\rightarrow$ $2\times7,\ 3\times7\cdots$

对于 100 以内的，找到算的多了

10 以内，1 2 3 4 5 6 7 8 9，其余要是合数，也是素×单位数，早排除掉了

$11\times13>100$，理解

补证明：素数有无穷多个。

反证：有限，最大素为 P。

则把前面所有素数相乘 $+1=Q$

① Q 为素，矛盾前提 ② Q 为合，前面没有一个满足的素因子，$P\nmid Q$

5. 欧几里得除法——最小非负余数——带余除法.

$a = q \cdot b + r$, $0 \le r < b$ 余数一定大于0.

$b \mid a$ a与r是唯一的.

$\cdots -3b, -2b, -b, 0, b, 2b, 3b \cdots$

引: a必落在这个轴上的一区间内, 对应的q与r只有一个.

$a = q_1 \cdot b + r_1$

$a = q_2 \cdot b + r_2$

$\Rightarrow (q_1 - q_2)b + (r_1 - r_2) = 0$

$\therefore$唯一性

$(q_1 - q_2)b = -(r_1 - r_2)$

$|\quad| \ge b$ $\quad 0 \le r_1, r_2 < b$ 残差.

$b \mid a$ 充要: a被b除的余数$r = 0$

$[x]$ 取x的整 $[x] \le x < [x] + 1$

$q = \left[\frac{a}{b}\right]$ $\quad r = a - q \cdot b = a - \left[\frac{a}{b}\right] \cdot b$

$[3.14] = 3$, $[-3.14] = -4$ → 保证余数为正

6. 素数的平凡判别.

判断N, 依次除$\le \sqrt{N}$的所有素数若都不能整除该数素.

例. $N = 137$ $\sqrt{137}$取12: 2, 3, 5, 7, 11

$2 \nmid 137$, $3 \nmid 137$, $5 \nmid 137$, $7 \nmid 137$, $11 \nmid 137$ 故137为素.

为什么是$\sqrt{N}$ →

$\sqrt{N} \times \sqrt{N} = N$ (左$\sqrt{N}$, 右$\sqrt{N}$)

$a \times b = N$

$c \times d = N$

往后一定是一大一小乘积为N

于所有的合一定能化为对应于$\sqrt{N}$的素, 无需担心.

7. 欧几里得除法——一般余数

$a = q \cdot b + r$, $C \le r < b + C$ 一般将余数取为其他形式

同理也是存在且唯一的.

C对应不同值有以下几种对法: $(C\le b\le b+C-1)$

① $C=0$, 最小非负余数 $0\le r<b$

② $C=1$, 最小正余数 $1\le r<b$

③ $C=-b+1$, 最大非正余数 $-b<r\le 0$

④ $C=-b$, 最大负余数 $-b\le r\le -1$

⑤ 还有 $-\frac{b}{2}\le r<\frac{b}{2}$, $-\frac{b}{2}<r\le\frac{b}{2}$ … 绝对值最小余数…

1.2 整数的表示

1. 各种进制表示, 略

2. 算法复杂度, 略

大O, 小o符号

$f(n)=n^2+n+5$

$f(n)=O(n^2)$ → 可自行查O与o区别.

$f(n)=o(e^n)$

3. 进制算术, 略.

1.3 最大公因数与广义欧几里得除法

1. 对于整数 $a_1, a_2 \cdots a_n$, 若有整数 d

$d|a_1, d|a_2, d|a_3 \cdots d|a_n$, 则 d 为一个公因数

最大的 d 就是最大公因数了. 记作 $gcd(a_1, a_2 \cdots a_n)$

当 $gcd(a_1 \cdots a_n)=1$ 时, 称其互素.

2. $d=(a,b)$ 是 $\{sa+tb\}$ 中的最小正整数.

↓

d 是集合 $\{s_1\cdot a_1+s_2\cdot a_2+\cdots+s_n a_n \mid s_1, s_2 \cdots s_n \in Z\}$ 中的最小正整数.

① $gcd(a,b)=gcd(b,a)$

$b|a$ 则 $(a,b)=b$

② p为素，若 $p \nmid a$，则 a, p 互素.

3. $a_1, \cdots a_n$ 与 $|a_1|, \cdots |a_n|$ 的公因数相同.

$\gcd(a_1, a_2 \cdots a_n) = \gcd(|a_1|, |a_2| \cdots |a_n|)$

① 若 $d \mid a_i$ 则有 $d \mid |a_i|$，故左因也为右因.

② 若 $d \mid |a_i|$，则有 $d \mid a_i$，故右因也为左因.

例：$(a, b) = (a, -b) = (-a, b) = (-a, -b) = (|a|, |b|)$

4. $(0, b) = |b|$ 最大公约数和最小公倍数是在自然数范围内讨论的，当然不存在负数的说法.

5. $a = q \cdot b + c$，则有 $(a, b) = (b, c)$

证：画图分理解

$d = (a, b)$ 最大公因数

$\Leftarrow$ 则 $d \mid a, d \mid b \to d \mid a + (-q)b = c \to d$ 为 b, c 公因数 $\to d \le d'$

同理 $d' = (b, c)$，则 $d' \mid b, d' \mid c \to d' \mid qb + c = a \to d'$ 为 a, b 公因数 $\to d' \le d$

故 $d = d'$，有 $(a, b) = (b, c)$

$1573 = 5 \times 286 + 143$　$\gcd(1573, 286) = (286, 143) = 143$

6. 广义欧几里得除法及计算最大公因数.

关键建：$(a, b) = (b, c)$ 一直化简就行.

$a = q \cdot b + c$

记 $r_{-2} = a$，$r_{-1} = b$，$r_0 = c$

$r_{-2} = q_0 \cdot r_{-1} + r_0$，$0 < r_0 < r_{-1}$

$r_{-1} = q_1 \cdot r_0 + r_1$，$0 < r_1 < r_0$

$r_0 = q_2 \cdot r_1 + r_2$，$0 < r_2 < r_1$

$\vdots$

$r_{n-1} = q_{n+1} \cdot r_n + r_{n+1}$，$r_{n+1} = 0$

$0 = r_{n+1} < r_n < r_{n-1} < \cdots < r_1 < r_0 < r_{-1} = b$

步骤 $n \le 5\log b$ 用数学归纳法

当 $a>b$ 时，计算 (a,b) 的时间为 $O(\log n)$

例：$a=-1859$，$b=1573$，(a,b)？

$(-1859,1573)=(1859,1573)$

$1859=1\cdot 1573+286$

$1573=5\cdot 286+143$　　$(-1859,1573)=143$

$286=2\cdot 143+0$

7. Bezout (贝祖) 等式

$s\cdot a+t\cdot b=(a,b)$

$(a,b)=143=1573-5\times 286$

$=1573-5\times(1859-1573)$

$=-5\times \underbrace{1859}_{a}+6\times \underbrace{1573}_{b}$

求贝祖等式：① 又好简单的，先用广义欧几里德算出来，再回推。

② 复杂的，上表格。

$\begin{pmatrix} r_{-2} \\ r_{-1} \end{pmatrix}=\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix}$　　$\frac{r_{-2}}{a}=q_0\cdot\frac{r_{-1}}{b}+r_0$

$\begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix}=\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$　　$r_{-1}=q_1\cdot r_0+r_1$

$\vdots$

$\begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix}=\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$　　$r_{n-2}=q_n\cdot r_{n-1}+r_n$

$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}=\begin{pmatrix} q_{n+1} & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix}$ → 最大因数　　$r_{n-1}=q_{n+1}\cdot r_n+r_{n+1}$

$\| 0$

串起来有 $\begin{pmatrix} r_{-2} \\ r_{-1} \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_{j+1} & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix}$

A_j = 其倒数 $= \begin{pmatrix} s_j & t_j \\ u_j & v_j \end{pmatrix}$

$\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = A_j \begin{pmatrix} r_{-2} \\ r_{-1} \end{pmatrix}$ 由原数求最大公因数

⇓

$s_n a + t_n b = (a, b)$

对于 $j = 0, 1, 2 \cdots, n-1, n$, 有

$$\begin{cases} s_{-2}=1,\ s_{-1}=0,\ s_j = (-q_j)s_{j-1} + s_{j-2} \\ t_{-2}=0,\ t_{-1}=1,\ t_j = (-q_j)t_{j-1} + t_{j-2} \end{cases} \quad j = 0, 1, 2 \cdots, n-1, n$$

$q_j = \left[\frac{r_{j-2}}{r_{j-1}}\right]$

因此可否表求简单了.

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				a
-2	1	0		b
-1	0	1	q_0	r_0
0	s_0	t_0	q_1	r_1
1				
$\vdots$				
$n-2$				
$n-1$				
n	s_n	t_n	q_{n+1}	$r_{n+1}=0$

$$\begin{cases} s_j = (-q_j)s_{j-1} + s_{j-2} \\ t_j = (-q_j)t_{j-1} + t_{j-2} \\ q_{j+1} = \left[\frac{r_{j-1}}{r_j}\right] \\ r_{j+1} = (-q_{j+1})r_j + r_{j-1} \end{cases}$$

其实都一样

例: $a = 1859,\ b = 1573$, 求 $sa + tb = (a, b)$

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				1859
-2	1	0		1573
-1	0	1	1	286
0	1	-1	5	143
1	-5	6	2	0

$\therefore s = -5,\ t = 6$

$(-5) \times 1859 + 6 \times 1573 = 143$

更多例子参书 P31

8. a.b互素充要条件是存在整数s.t使

$sa+tb=1$

记住充要就行了.

充：互素 $\to (a,b)=1 \to sa+tb=1$

要：$sa+tb=1$，$d=(a,b) \to d|a, d|b$

$d|(sa+tb)=1 \to d=1$

推论：$ad-bc=1$

$(a,b)=1$，$(a,c)=1$，$(d,b)=1$，$(d,c)=1$

9. 最大公因数的进一步性质

① $gcd(a,b)=d \Leftrightarrow \begin{cases} d|a, d|b \\ \text{若 } e|a, e|b \text{ 则有 } e|d \end{cases}$

② $(m\cdot a, m\cdot b)=m\cdot(a,b)$，$m$为任整

③ $d|a, d|b$，则 $\left(\frac{a}{d},\frac{b}{d}\right)=\frac{(a,b)}{|d|}$

推论 $\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$

例：$a=11\cdot 200306$　　求 (a,b)

$b=23\cdot 200306$

$(11,23)=1$

$(11\cdot 200306, 23\cdot 200306)=200306\cdot(11,23)=200306=(a,b)$

④ $(a,c)=1 \Rightarrow (ab,c)=(b,c)$

推论：$a_1,\cdots a_n$，$(a_i,c)=1$，则 $(a_1a_2\cdots a_n, c)=1$

⑤ $\begin{cases} a=q\cdot u+r\cdot v \\ b=s\cdot u+t\cdot v \end{cases}$ 若 $q\cdot t-r\cdot s=1$，则 $(a,b)=(u,v)$

证：$d=(a,b)$

$d'=(u,v)$　　$d'|u$，$d'|v \Rightarrow d'|q\cdot v+r\cdot v=a$，$d'|s\cdot u+t\cdot v=b$

$\therefore d'|d$　　$d'|a$，$d'|b$

条件用在这里

反：$u=t\cdot a+(-s)\cdot b$，$v=(-r)\cdot a+q\cdot b$　　同理 $d|d'$

$\therefore d=d'$

10. 多个整数的最大公因数计算

$a_1, a_2, a_3 \cdots a_n$ 为 n 个整数.

$(a_1, a_2) = d_2$, $(d_2, a_3) = d_3$, $\cdots$, $(d_{n-1}, a_n) = d_n$

则 $(a_1, a_2 \cdots a_n) = d_n$

↳ 有 $s_1 \cdot a_1 + s_2 \cdot a_2 + s_3 \cdot a_3 + \cdots + s_n \cdot a_n = d_n$ 成立

例: 求 $(120, 150, 210, 35)$

$(120, 150) = (150, 120) = (120, 30) = 30$

$(30, 210) = 30$

$(30, 35) = (35, 30) = (30, 5) = 5$

$\therefore (120, 150, 210, 35) = 5$

推论: $d \mid a_1, d \mid a_2 \cdots d \mid a_n \iff d = (a_1, a_2 \cdots a_n)$ 充要

若 $e \mid a_1, e \mid a_2 \cdots e \mid a_n$, 则 $e \mid d$

11. 形为 $2^a - 1$ 整数的 gcd.

计算 $(2^a - 1, 2^b - 1)$

↓

最大公因数为 $2^{(a,b)} - 1$

$2^r\left((2^b)^q - 1\right) + 2^r - 1$

$= q_1 (2^b - 1) + 2^r - 1$ ★这一步妙.

$q_1 = 2^r\left((2^b)^{q-1} + (2^b)^{q-2} + \cdots + 2^b + 1\right)$

$\therefore$ 对于 $a = q \cdot b + r$, 有 $2^a - 1 = q_1 (2^b - 1) + 2^r - 1$

1.4 整除的进一步性质及最大公因数

1. 整除的进一步性质

① 若 $c \mid ab$, $(a, c) = 1$, 则 $c \mid b$

② p 为素数, 若 $p \mid ab$, 则 $p \mid a$ 或 $p \mid b$

推论：n个整数 $a_1, a_2 \cdots a_n$ 两两互素，若 $p \mid a_1 a_2 a_3 \cdots a_n$ 则 p 一定整除其中一个 a_k.

2. 最小公倍数(LCM)

$LCM[a_1, a_2 \cdots, a_n] = D$

1) $a_i \mid D$ 2) 若 $a_i \mid D'$，则 $D \mid D'$

$D = [a, b] \in \{c \mid c \in \mathbb{Z}, a \mid c, b \mid c\}$

a, b 互素正整数，则

1) 若 $a \mid D$, $b \mid D$, 则 $a \cdot b \mid D$

2) $[a, b] = a \cdot b$

3. gcd 与 LCM.

① a, b 两个正整数.

1) 若 $a \mid D$, $b \mid D$, 则 $[a, b] \mid D$

2) $[a, b] \cdot (a, b) = a \cdot b$ ☆

$a = 2^{a_1} 3^{a_2} 5^{a_3} \cdots$

$b = 2^{b_1} 3^{b_2} 5^{b_3} \cdots$

$lcm[a, b] = 2^{\max(a_1, b_1)} 3^{\max(a_2, b_2)} \cdots$

$gcd(a, b) = 2^{\min(a_1, b_1)} 3^{\min(a_2, b_2)} \cdots$

4. 多个整数的 LCM

$[a_1, a_2] = D_2$, $[D_2, a_3] = D_3$, $\cdots$ $[D_{n-1}, a_n] = D_n$

例：$LCM[120, 150, 210, 35]$

$[120, 150] = \frac{120 \times 150}{(120, 150)} = \frac{120 \times 150}{30} = 600$

$[600, 210] = 4200$

$[4200, 35] = 4200$

补证：$a_1 \mid D$, $a_2 \mid D$, $a_3 \mid D \cdots a_n \mid D$

则 $[a_1, a_2, a_3 \cdots, a_n] \mid D$

1.5 整数分解

整数分解定理.

给定合数 $n>1$，若存在 a,b 使得

$$n \mid a^2-b^2,\ n \nmid a+b,\ n \nmid a-b$$

则 $(n,a-b)$ 与 $(n,a+b)$ 都是 n 的真因数

除自身以外的因数

6 因数有 1,2,3,6

真因数

反证：$(n,a-b)$ 不为真因子为 n.

$(n,a-b)=n$ 则 $n \mid a-b$ 矛盾

同理 $(n,a+b)$ 也为真因.

为旧时，$(n,a-b)=1$

由 $n \mid a^2-b^2=(a+b)(a-b)$ 得

$n \mid a$ 也矛盾

例：$n=167\times 227=37909$

有 $a=16355$，$b=11$，满足

$n \mid a^2-b^2$，$n \nmid a-b$，$a \nmid a+b$

$(n,a-b)=227$，$(n,a+b)=167$ 都是真因数

1.6 素数的算术基本定理

1. 算术基本定理：任一整数 $n>1$ 都可以表示为素数的乘积.

$$n=p_1\cdots p_s,\ p_1\le\cdots\le p_s \text{（任一）}\quad p_i \text{为素数}$$

数归证明：任意 $n>1$ 都能表示

（强归纳）

① 对于 $n=2$ 显然成立.

② 假设对于 $<n$ 的都成立.

③ 对于等于 n 的 { 为素数 ✓

为合数，必存在 $n=n_1n_2$，$n_1<n$，$n_2<n$ ✓

于是证得.

2. 更好的表示：$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，$\alpha_i>0$ $i=1,\cdots,s$

标准化分解式

3. 定理的应用：① $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$

d 是 n 的正因数当且仅当

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad 0 \le \beta_i \le \alpha_i$$

② 因此，n 的因数个数为 $(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_s)$

③ $(a,b) = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ $\quad \gamma_i = \min(\alpha_i, \beta_i)$

$[a,b] = p_1^{\delta_1} \cdots p_s^{\delta_s}$, $\quad \delta_i = \max(\alpha_i, \beta_i)$

故 $(a,b)[a,b] = ab \Rightarrow \gamma_i + \delta_i = \alpha_i + \beta_i$

例：算 120, 150, 210, 35 的 gcd 与 lcm.

$120 = 2^3 \cdot 3 \cdot 5$ $\quad 210 = 2 \cdot 3 \cdot 5 \cdot 7$

$150 = 2 \cdot 3 \cdot 5^2$ $\quad 35 = 5 \cdot 7$

$(120, 150, 210, 35) = 2^{\min(3,1,1,0)} 3^{(1,1,0,1)} \cdots$ 略.

④ 整数 a, b 必存在 $a' \mid a$, $b' \mid b$ 使得

$a' \cdot b' = [a,b]$, $(a', b') = 1$ 一般理解

例：

$a = 79\,720\,245\,000 = 2^3 \cdot 5^4 \cdot 11^6 \cdot 3^2 \cdot 7^0$

$b = 93\,187\,531\,596 = 2^2 \cdot 5^0 \cdot 11^3 \cdot 3^6 \cdot 7^4$

取 $a' = 2^3 \cdot 5^4 \cdot 11^6$ $\quad (a', b') = 1$

$b' = 3^6 \cdot 7^4$ $\quad [a,b] = a' \cdot b'$

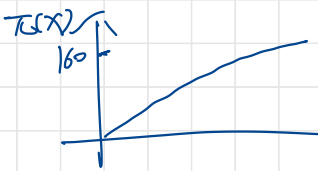
⑤ n 为合，p 为一个素因子

设 $p^\alpha \| n$ (即 $p^\alpha \mid n$, 但 $p^{\alpha+1} \nmid n$)

则有 $p^\alpha \nmid \binom{n}{p} = \dfrac{n(n-1)\cdots(n-p+1)}{p!}$

1.7 素数定理

$\pi(x)$ 表示不超过 x 的素数个数



大概有 $\dfrac{\ln 2}{3} \dfrac{x}{\ln x} < \pi(x) < 6 \ln 2 \dfrac{x}{\ln x}$

契比雪夫不等式

$\dfrac{1}{6\ln 2} n \ln n < p_n < \dfrac{6}{\ln 2} n \ln 2$

素数定理：$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\ln x}}=1$

P_n表示第n个素数