§3.4 整数与整除

一．整除 (Division)

1. 整除

定义：设 a 和 b 是整数且 $a \neq 0$, 我们说a 整除 b (a divides b)，是说，存在整数 c 使得 b=ac。当 a 整除 b, 我们说 a 是 b 的因子(factor)并且 b 是 a 的倍数(multiple of a)，记作$a|b$。若 a 不能整除 b, 记作$a \nmid b$。

2. 例子：

例 1：判定是否有$3|7$ 和 $3|12$。

解：因为 7/3不是整数，所以$3 \nmid 7$，而$\frac{12}{3} = 4$,故$3|12$。

例 2：设 n 和 d 是正整数。问有多少个不超过 n 的正整数可以被 d 整除？

解：能被 d 整除的正整数具有形式 dk，其中 k 是正整数，不超过n 可以被d 整除的正整数的个数，就是满足$0 < \mathrm{dk} \leq \mathrm{n}$的 k 的个数，也就是满足$0 < k \leq n/d$的 k 的个数，即$\lfloor \mathrm{n}/\mathrm{d} \rfloor$。

3. 整除的性质

定理 1：设 a, b, c 是整数，那么

(i)如果$a|b$ 且 $a|c$，那么$a|(b+c)$；

(ii)如果$a|b$，那么 $a|bc$ 对所有整数 c 成立；

(iii)如果$a|b$且$b|c$，那么$a|c$。

证明：(i) 假设$a|b$且$a|c$，那么由定义知，存在整数 s 和 t，使得 b=as，c=at，故 b+c=as+at=a(s+t)。从而$a|(b+c)$。

(ii)和(iii)的证明类似。

推理 1：如果 a, b, c 是整数且$a|b$和$a|c$，那么$a|(mb+nc)$，其中 m, n 是任意整数。

二．除算法 (The Division Algorithm)

定理 2：（除算法）设 a 是整数，d 是一个正整数，那么存在唯一的整数 q 和 r 且$0 \le r < d$，有$a = dq + r$。

定义：在除算法中，d 称为除数(divisor)，a 称为被除数(dividend), q 称为商(quotient), r 称为余数(remainder)。商和余数记为：$q = a \operatorname{div} d, \quad r = a \bmod d$。

例 3：101 除以 11，商和余数是多少？

解：101 = $11 \cdot 9 + 2$，商是 9，余数是 2。

例 4：-11除以 3，商和余数是多少？

解：$-11 = 3 \cdot (-4) + 1$, 故商是-4，余数是 1.

注意：余数必须是非负数，不能写成$-11 = 3 \cdot (-3) - 2$。

三．模算术 (Modular Arithmetic)

1. 模和余数

设 a 和 b 是整数，m 是正整数，那么 a 和 b 模 m 同余 (a is congruent to b modulo m)，是说 m 整除$a-b$，记为$a \equiv b \pmod m$。若 a 和 b 模 m 不同余，记为$a \not\equiv b \pmod m$。

2. 模 m 同余的充要条件

定理 3：设 a 和 b 是整数，m 是正整数。那么$a \equiv b \pmod m$当且仅当 $a \bmod m = b \bmod m$。

例 5：判定 17 和 5 是否模 6 同余？24 和 14 是否模 6 同余？

解：因为 $17 \bmod 6 = 5 = 5 \bmod 6$，故$17 \equiv 5 \pmod 6$。

又因为$24 - 14 = 10$不能被 6 整除，故$24 \not\equiv 14 \pmod 6$。

定理 4：设 m 是正整数。整数 a 和 b 模 m 同余当且仅当存在整数 k 使得$a = b + km$。

证明：设$a \equiv b \pmod m$。那么$m|(a-b)$。故存在整数 k，使得$(a-b) = km$，从而有$a = b + km$。

反过来，假设$a = b + km$，对某个整数 k 成立，那么$a - b = km$，从而有$m|(a-b)$。故$a \equiv b \pmod m$。

3. 模运算的性质

定理 5：设 m 是正整数。如果$a \equiv b \pmod m$且$c \equiv d \pmod m$，那么$a + c \equiv b + d \pmod m$且$ac \equiv bd \pmod m$。

证明：因为$a \equiv b \pmod m$和$c \equiv d \pmod m$，因而存在整数 s 和 t，使得$b = a + sm$且$d = c + tm$。因此

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

且 $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$

因此$a + c \equiv b + d \pmod m$且$ac \equiv bd \pmod m$。

例 6：因为$7 \equiv 2 \pmod 5$且$11 \equiv 1 \pmod 5$，由定理知

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$$

且 $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod 5$。

推论 2：设 m 是正整数，且 a 和 b 是整数。那么

$$(a + b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$$

且 $ab \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m$。

证明：因为$a \equiv (a \bmod m) \bmod m, b \equiv (b \bmod m) \bmod m,$

由定理 5 知，

$$(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$$

且 $ab \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m$。

四．同余的应用

1. 凯撒密码 (密码学(Cryptology))

将英文字母表中所有字母向前移 3 个位置，最前面的 3 个字母移到最后面 3 个位置。用字母表

D,E,F,G,H, I, J,K,L,M,N,O,P, Q,R,S,T,U,V,W,X,Y,Z,A,B,C 对应

A,B,C,D,E,F,G,H,I, J, K, L,M,N,O,P,Q,R,S,T, U,V,W,X,Y,Z,

进行编码。

例如： MEET YOU IN THE PARK 编码为

PHHW BRX LQ WKH SDUN

假设用 0, 1, 2,⋯, 25 给 26 个字母编号，凯撒密码用公式表示为： f(p)= (p+3)mod 26， $p \in \{0,1,2,\cdots,25\}$.

f(p)为加密函数(encryption function).

解密函数(decryption function)为：$f^{-1}(p)$ =(p−3)mod 26。

凯撒密码可以推广到更一般的形式：

$$f(p) = (ap + b) \bmod 26，$$

其中 a,b 为整数，经过选取 a,b，使得 f(p)为$\{0,1,\cdots,25\} \to \{0,1,\cdots,25\}$的双射函数。

§3.5 素数和最大公因子

一．素数 (primes)

1. 定义：一个大于 1 的正整数 p 被称为素数，是说，p 只有正因子 p 和 1。一个大于 1 的正整数 q 如果不是素数，则 q 被称为合数(composite)。

例 1：整数 7 是素数，因为它只有因子 7 和 1，而整数 9 是合数，因为它有因子 3 且 $3\neq 1,9$.

定理 1（算术基本定理）：每一个大于 1 的正整数可以表示成一个素数，或可以表示成两个或更多的素数的乘积，其中这些素因子可以写成非递减的顺序。

例 2：给出 100，641，999 和 1024 的素因子分解。

解：$100=2\cdot 2\cdot 5\cdot 5=2^2\cdot 5^2$

$641=641$

$999=3\cdot 3\cdot 3\cdot 37=3^3\cdot 37$

$1024=2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2=2^{10}$ 。

定理 2：如果 n 是一个合数，那么 n 有一个小于或等于$\sqrt{n}$的素因子。

证明：假设 n 是合数，那么 n 有一个因子 a，$1<a<n$，并且 n 可以写成 n=ab，其中 b 是大于 1 的正整数。这时，有$a\leq\sqrt{n}$或$b\leq\sqrt{n}$。假若不然，有$a>\sqrt{n}$且$b>\sqrt{n}$，那么 $n=ab>\sqrt{n}\sqrt{n}=n$，矛盾。故有$a\leq\sqrt{n}$或$b\leq\sqrt{n}$。因为 a 和 b 都是 n

的因子，故 n 有一个不大于$\sqrt{n}$的因子 a（或 b）。而 a（或 b）要么是一个素数，要么由算术基本定理，a（或 b）有一个小于 a（或 b）的素因子，在两种情况下，n 都有一个小于或等于$\sqrt{n}$的素因子。

例 3：证明 101 是素数。

证明：只要证 101 没有小于或等于$\sqrt{101}$的素因子即可。因为小于或等于$\sqrt{101}$的素数只有 2,3,5,7，而 2,3,5,7 都不是 101 的因子，故 101 是素数。

2. 求整数 n 的素数因子分解

对于任一整数 n，从最小的素数 2 开始，用从小到大不超过$\sqrt{n}$的素数去除 n，若求得一个素因子 p，那么再对n/p，从 p 开始从小到大求不超过$\sqrt{n/p}$的素因子。如果又求得素因子 q，再对$n/(pq)$，从 q 开始，从小到大求不超过$\sqrt{n/(pq)}$的素因子，如此进行下去。最后可求出 n 的所有素因子。

例 4：求 7007 的素因子分解。

解：从 2 开始，用从小到大的素数去除 7007. 2,3,5 都不能整除 7007. 而 7 可以整除 7007. 7 是第一个素因子。再从 7 开始用素数去除$\frac{7007}{7}=1001$，这时有$7|1001$。故 7 是第 2 个素因子。再从 7 开始用素数去除$\frac{1001}{7}=143$，这时找到$11|143$，故 11 是第 3 个素因子。再从 11 开始用素数去除$\frac{143}{11}=13$，求出 13 是最后一个素因子。故 7007 的素因子分解为：

7007=$7\cdot 7\cdot 11\cdot 13=7^2\cdot 11\cdot 13$。

3. 素数的无穷性 (The infinitude of primes)

定理 3：存在无穷多个素数。

证明：反证法。假设只有有穷多个素数，设$p_1, p_2, \cdots, p_n$是所有的素数，那么令$Q = p_1 p_2 \cdots p_n + 1$。由算术基本定理，Q应能表示成$p_1, p_2, \cdots, p_n$中某些素数的因子分解。但对任意$p_i\,(1 \le i \le n)$，$p_i \nmid Q$。这因为，假若$p_i | Q$，又有$p_i | p_1 p_2 \cdots p_n$，故有$p_i | (Q - p_1 p_2 \cdots p_n)$。即$p_i | 1$，矛盾。故 Q 是一个素数且$Q \ne p_i$，i=1,2,$\cdots$，n。这与$p_1, p_2, \cdots, p_n$是所有素数的假设矛盾。

*因为素数有无穷多个，人们试图列出尽可能大的素数（在密码学中有用）。已知的最大素数具有这样的表达式：$2^p - 1$，其中 p 是一个素数，这种素数称为梅森数(Mersenn primes)。但并不是所有具有表达式$2^p - 1$的数都是素数。

例 5：$2^2 - 1 = 3$，$2^3 - 1 = 7$，$2^5 - 1 = 31$都是梅森数，但$2^{11} - 1 = 2047$不是梅森数，因为 2047=23·89.

*目前已知的最大的梅森数是$2^{30,402,457} - 1$，这是一个 9 百万位 10 进位的数字。

定理 4（素数定理）：不超过 x 的素数个数的频率是x/lnx（当 x 趋于无穷）。

*其中 ln x 是 x 的自然对数。

二．关于素数的公开问题与猜想

1. 哥德巴赫猜想：

任何一个大于 5 的奇数可以表示成 3 个素数的和。

等价命题：任何一个大于 2 的偶数可以表示成 2 个素数的和。

目前已知的最好结果：

（Ramare1995）：任何一个大于 2 的偶数可以表示成至多 6 个素数的和。

（陈景润 1966）：任何一个大于 2 的偶数可以表示成两个素数之和或一个素数和两个素数的乘积之和。

2. 孪生素数猜想：

有无穷多个孪生素数 p 和 p+2。

例如：3 和 5， 5 和 7，11 和 13，17 和 19，4967 和 4969 等。

三．最大公因子和最小公倍数

1. 最大公因子 (greatest common divisors)

定义：设 a 和 b 都是非零整数。最大整数 d 满足: $d|a$且$d|b$，称为 a 和 b 的最大公因子，记作 d=gcd(a, b)。

例 10：24 和 36 的最大公因子是什么？

解：24 和 36 的正的公因子有 1,2,3,4,6 和 12。因此 gcd(24,36)=12。

例 11：17 和 22 的最大公因子是什么？

解：17 和 22 的公因子只有 1. 故 gcd(17,22)=1。

2. 两个整数互素

定义：如果两个整数 a, b，满足 gcd(a, b)=1，那么称 a 和 b 互素(relatively prime)。

例如：例 11 中，17 和 22 互素。

定义：整数$a_1, a_2, \cdots, a_n$两两互素是说$\gcd(a_i, a_j) = 1(1 \le i < j \le n)$。

例 13：10, 17, 21 两两互素。

3. 求最大公因子的方法

已知两个整数 a 和 b，由算术基本定理，a, b 可表示成

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},\ \ b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

其中a_i和b_j可能为 0.

那么$\gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$

*首先，上式右边的数可以整除 a 和 b，其次，更大的数不能整除 a 或 b。

例 14：求 120 和 500 的最大公因子。

解：$120=2^3 \cdot 3 \cdot 5$，$500 = 2^2 \cdot 5^3$

$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)}$

$= 2^2 \cdot 3^0 \cdot 5^1 = 20$

4. 最小公倍数(least common multiple)

定义：正整数 a 和 b 的最小公倍数是能够被 a 和 b 整除的最小正整数。记作：lcm(a, b).

假设

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},\ \ b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

那么

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

例 15：求$2^3\cdot3^5\cdot7^2$和$2^4\cdot3^3$的最小公倍数。

解：

$\mathrm{lcm}(2^3\cdot3^5\cdot7^2,2^4\cdot3^3)=2^{\max(3,4)}\cdot3^{\max(5,3)}\cdot7^{\max(2,0)}$

$=2^4\cdot3^5\cdot7^2$ 。

定理 5：设 a, b 是正整数，那么$a\cdot b=\gcd(a,b)\mathrm{lcm}(a,b)$。

作业：

1. 证明：如果 a, b 是整数，并且$a|b$且$b|a$，那么 a=b 或 a=−b。
2. 证明：如果$a\equiv b(\mathrm{mod}\ m)$且$c\equiv d(\mathrm{mod}\ m)$，其中 a,b,c 是整数，m 是正整数，那么$(a-c)\equiv(b-d)(\mathrm{mod}\ m)$。
3. 找出以下数字的素因子分解：

（1）126　　（2）729　　（3）143

4. 求以下数对的最大公因子：

（1）$2\cdot3\cdot5\cdot7\cdot11\cdot13$；　$2^{11}\cdot3^9\cdot11\cdot17^{14}$

（2）66；　126

5. 证明：对每一个正整数 n，存在 n 个连续的合数。