初等数论基础及其应用
习题课及作业

2024,4, 8

南京大学计算机科学与技术系

内容提要-素数

整除

设 a,b 是两个整数,且 $b\neq 0$. 如果存在整数 c 使 $a=bc$,那么称 a 被 b 整除,或 b 整除 a,记作 $b\mid a$. 此时,又称 a 为 b 的倍数,b 是 a 的因子. 把 b 不整除 a 记作 $b\nmid a$.

带余除法

设 a,b 是两个整数,且 $b\neq 0$,则存在唯一的整数 q 和 r,使得

$$a=qb+r,\ \text{其中}0\leqslant r<|b|,$$

这个式子称作带余除法,记余数 $r=a \bmod b$.

定义 4.1.1 设 a 是大于 1 的正整数,如果 a 的正因子只有 1 和 a,那么称 a 为素数或质数;否则,称 a 为合数.

定理 4.1.1 (算术基本定理) 设 $a>1$,则

$$a=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k},$$

其中 $p_1,p_2,\cdots,p_k$ 是互不相同的素数,$r_1,r_2,\cdots,r_k$ 是正整数,并且在不计顺序的情况下,该表示是唯一的.

定理 4.1.2 有无穷多个素数.

定理 4.1.3 (素数定理) $\lim\limits_{n\to+\infty}\dfrac{\pi(n)}{n/\ln n}=1.$

定理 4.1.4 若 a 是一个合数,则 a 必有一个小于等于 $\sqrt{a}$ 的真因子,从而 a 必有一个小于等于 $\sqrt{a}$ 的素因子.

厄拉多塞(Eratosthene)筛法

10 以内的素数是 2,3,5,7,用它们除 100 以内大于 10 的数,删去所有能被它们整除的数,剩下的(含 2,3,5,7 在内)就是 100 以内的所有素数. 再用这些素数除 $100^2=10\,000$ 以内大于 100 的数,删去所有能被它们整除的数,可以得到 10 000 以内的所有素数. 重复这个做法可以得到任意给定的正整数以内的所有素数. 这个方法称作厄拉多塞(Eratosthene)筛法.

内容提要-最大公因数与最小公倍数

最大公因数

设 a 和 b 是两个整数，如果 $d\mid a$ 且 $d\mid b$，那么称 d 为 a 与 b 的公因数，或公约数. 除 0 之外，任何整数只有有限个因子. 因而，两个不全为 0 的整数 a 和 b 只有有限个公因子，其中最大的称作最大公因数，或最大公约数. 记作 $\gcd(a,b)$.

最小公倍数设 a 和 b 是两个非零整数，如果 $a\mid m$ 且 $b\mid m$，那么称 m 为 a 与 b 的公倍数. a 与 b 有无穷多个公倍数，其中最小的正公倍数称作最小公倍数. 记作 $\mathrm{lcm}(a,b)$.

定理 4.1.5

(1) 若 $a\mid m, b\mid m$，则 $\mathrm{lcm}(a,b)\mid m$.

(2) 若 $d\mid a, d\mid b$，则 $d\mid \gcd(a,b)$.

设 $a=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，$b=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}$，其中 $p_1,p_2,\cdots,p_k$ 是互不相同的素数，$r_1,r_2,\cdots,r_k,s_1,s_2,\cdots,s_k$ 是非负整数，则

$$\gcd(a,b)=p_1^{\min(r_1,s_1)}p_2^{\min(r_2,s_2)}\cdots p_k^{\min(r_k,s_k)},$$
$$\mathrm{lcm}(a,b)=p_1^{\max(r_1,s_1)}p_2^{\max(r_2,s_2)}\cdots p_k^{\max(r_k,s_k)}.$$

辗转相除法(又称欧几里得算法)

定理 4.1.6 设 $a=qb+r$，其中 a,b,q,r 都是整数，则 $\gcd(a,b)=\gcd(b,r)$.

设整数 a,b，且 $b\neq 0$. 做带余除法

$$a=q_1b+r_2,\quad 0\leqslant r_2<|b|.$$

若 $r_2>0$，再对 b 和 r_2 做带余除法，得

$$b=q_2r_2+r_3,\quad 0\leqslant r_3<r_2.$$

重复上述过程. 由于 $|b|>r_2>r_3>\cdots\geqslant 0$，必存在 k 使 $r_{k+1}=0$. 于是，有

$$\begin{aligned}
a&=q_1b+r_2, & 1\leqslant r_2<|b|;\\
b&=q_2r_2+r_3, & 1\leqslant r_3<r_2;\\
r_2&=q_3r_3+r_4, & 1\leqslant r_4<r_3;\\
&\vdots\\
r_{k-2}&=q_{k-1}r_{k-1}+r_k, & 1\leqslant r_k<r_{k-1};\\
r_{k-1}&=q_kr_k.
\end{aligned}\tag{①}$$

根据定理 4.1.6，有

$$\gcd(a,b)=\gcd(b,r_2)=\cdots=\gcd(r_{k-1},r_k)=r_k.$$

这就是辗转相除法，又称作欧几里得(Euclid)算法.

定理 4.1.7 设 a 和 b 不全为 0，则存在整数 x 和 y 使得 $\gcd(a,b)=xa+yb$.

互素

定义 4.1.2 如果 $\gcd(a,b)=1$，那么称 a 和 b 互素.

如果整数 $a_1,a_2,\cdots,a_n$ 中的任意两个都互素，那么称它们两两互素.

定理 4.1.8 整数 a 和 b 互素的充分必要条件是存在整数 x 和 y 使得 $xa+yb=1$.

内容提要-同余

同余的概念及性质

定义 4.1.3 设 m 是正整数，a 和 b 是整数. 若 $m \mid a-b$，则称 a 模 m 同余于 b，或 a 与 b 模 m 同余，记作 $a \equiv b \pmod{m}$. 若 a 与 b 模 m 不同余，则记作 $a \not\equiv b \pmod{m}$.

命题 4.1.1 同余关系是等价关系，即同余关系具有：

(1) 自反性：$a \equiv a \pmod{m}$.

(2) 对称性：若 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$.

(3) 传递性：若 $a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$，则 $a \equiv c \pmod{m}$.

命题 4.1.2

(1) 若 $a \equiv b \pmod{m}$，$c \equiv d \pmod{m}$，则 $a \pm c \equiv b \pm d \pmod{m}$，$ac \equiv bd \pmod{m}$，$a^k \equiv b^k \pmod{m}$，其中 k 是非负整数.

(2) 设 $d \geqslant 1$，$d \mid m$，若 $a \equiv b \pmod{m}$，则 $a \equiv b \pmod{d}$.

(3) 设 $d \geqslant 1$，则 $a \equiv b \pmod{m}$ 当且仅当 $da \equiv db \pmod{dm}$.

(4) 设 c 与 m 互素，则 $a \equiv b \pmod{m}$ 当且仅当 $ca \equiv cb \pmod{m}$.

模 m 等价类及其运算

整数 a 在模 m 同余关系下的等价类记作 $[a]_m$，称作 a 的模 m 等价类. 在不会引起混淆的情况下，可以略去下标 m，简记作 $[a]$，有时也会直接记作 a. 把整数集 $\mathbb{Z}$ 在模 m 同余关系下的商集记作 $\mathbb{Z}_m$. 可以在 $\mathbb{Z}_m$ 上定义加法和乘法如下：对任意的整数 a, b，

$$[a] \oplus [b] = [a+b], \quad [a] \otimes [b] = [ab].$$

内容提要--一次同余方程

一次同余方程及其有解的条件设 $m>0$,方程

$$ax \equiv c \pmod{m}$$

称作一次同余方程,使方程 (4.1.1) 成立的整数称作方程的解.

定理 4.1.9　方程 (4.1.1) 有解的充分必要条件是 $\gcd(a,m) \mid c$.

模 m 逆

定义 4.1.4　如果 $ab \equiv 1 \pmod{m}$,那么称 b 为 a 的模 m 逆,记作 $a^{-1} \pmod{m}$ 或 a^{-1}.

定理 4.1.10

(1) a 的模 m 逆存在的充分必要条件是 a 与 m 互素.

(2) 设 a 与 m 互素,则在模 m 下 a 的模 m 逆是唯一的,即 a 的任意两个模 m 逆都模 m 同余.

内容提要-欧拉定理和费马小定理

欧拉函数

欧拉函数 ϕ 是数论中的一个重要函数，定义如下：设 n 是正整数，$\phi(n)$ 表示 $\{1,2,\cdots,n\}$ 中与 n 互素的元素个数.

定理 4.1.11 (欧拉定理) 设 a 与 n 互素，则

$$a^{\phi(n)} \equiv 1 \pmod{n}. \tag{4.1.2}$$

定理 4.1.12 (费马小定理) 设 p 是素数，a 与 p 互素，则

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4.1.3}$$

定理的另一种形式是，设 p 是素数，则对任意的整数 a，

$$a^{p} \equiv a \pmod{p}. \tag{4.1.4}$$

基本要求

- 1. 熟练掌握整除、素数、合数的概念及其性质，掌握算术基本定理，能够熟练地进行（较小的）整数素因子分解，
- 会判断一个（较小的）数是否是素数，掌握厄拉多塞（Eratosthene）筛法.
- 2. 熟练掌握最大公因数和最小公倍数的概念及其性质，会求最大公因数和最小公倍数，掌握辗转相除法.
- 3. 熟练掌握互素的概念及其性质.
- 4. 熟练掌握同余的概念及其性质，掌握一次同余方程的解的概念及存在的充分必要条件，掌握模 m 逆的概念及存在的充分必要条件，会求一次同余方程的解和模 m 逆.
- 5. 掌握欧拉定理和费马小定理.

题型一：基本概念和素因子分解

1. 判断下列命题的真假.

(1) $3\mid -12$; (2) $3\mid 8$; (3) $-5\mid 45$; (4) $0\mid 8$; (5) $-21\mid 0$.

2. 给出下列整数的素因子分解.

(1) 585; (2) $20!! = 2\times 4\times 6\times\cdots\times 20$.

3. 判断下列整数是素数,还是合数. (1) 111; (2) 2 299.

4. 如果一个正整数等于它的除自身外的所有正因子之和,那么称这个正整数是完全数.

(1) 验证 6 和 28 是完全数.

(2) 证明:当 2^p-1 是素数时,$2^{p-1}(2^p-1)$ 是完全数.

解答与分析

1. (1) 真; (2) 假; (3) 真; (4) 假; (5) 真.

注意:0 不能做除数,故 $0\mid 8$ 为假. 而任何数都可以整除 0,故 $-21\mid 0$ 为真.

2. (1) $585 = 3^2\times 5\times 13$.

(2) $20!! = 2^{10}\times 10! = 2^{10}\times 2\times 3\times 2^2\times 5\times(2\times 3)\times 7\times 2^3\times 3^2\times(2\times 5) = 2^{18}\times 3^4\times 5^2\times 7$.

3. (1) $\sqrt{111}<11$,根据定理 4.1.4,只需检查小于 11 的素数是否能整除 111. 小于 11 的素数有 2,3,5,7. 它们都不能整除 111,故 111 是素数.

(2) $\sqrt{2\,299}<48$,小于 48 的素数有 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47. 逐个检查的结果是 11 能整除 2 299,故 2 299 是合数.

当数 a 比较大时,不一定能记住所有不超过 $\sqrt{a}$ 的素数,此时可以用厄拉多塞筛法产生所有不超过 $\sqrt{a}$ 的素数. 首先,不超过 10 的素数有 2,3,5,7. 用它们逐个除 11 到 48 之间的数,删去可以被它们整除的数,得到 11,13,17,19,23,29,31,37,41,43,47,加上原有的 2,3,5,7,就是所有不超过 48 的素数.

4. (1) 6 除自身外的正因子有 1,2,3,而 $1+2+3=6$,故 6 是完全数.

28 除自身外的正因子有 1,2,4,7,14,它们的和恰好等于 28,故 28 是完全数.

(2) 由于 2^p-1 是素数,$2^{p-1}(2^p-1)$ 除自身外的正因子有

$$1,2,2^2,\cdots,2^{p-1},(2^p-1),2(2^p-1),2^2(2^p-1),\cdots,2^{p-2}(2^p-1).$$

它们的和为

$$(1+2+2^2+\cdots+2^{p-2})2^p+2^{p-1}=(2^{p-1}-1)2^p+2^{p-1}=2^{p-1}(2^p-1).$$

得证 $2^{p-1}(2^p-1)$ 是完全数.

题型二：求最大公因数和最小公倍数

1. 求 280 与 180 的最大公因数和最小公倍数.
2. 验证 35 与 72 互素，并求 x,y 使得 $35x+72y=1$.
3. 证明：对任意的正整数 a 和 b，$ab=\gcd(a,b)\cdot\operatorname{lcm}(a,b)$.
4. 求欧拉函数 $\phi(15)$.

解答与分析

1. 方法一　利用整数的素因子分解. 因为

$$280=2^3\times5\times7,\ 180=2^2\times3^2\times5,$$

所以有

$\gcd(280,180)=2^2\times5=20$,

$\operatorname{lcm}(280,180)=2^3\times3^2\times5\times7=2\,520$.

方法二　用辗转相除法和公式 $ab=\gcd(a,b)\cdot\operatorname{lcm}(a,b)$（见本题型第 3 题）.

做辗转相除：

$280=180+100$,

$180=100+80$,

$100=80+20$,

$80=4\times20$.

于是

$\gcd(280,180)=20$,

$\operatorname{lcm}(280,180)=\dfrac{280\times180}{20}=2\,520$.

2. 为了证明 35 和 72 互素，只需计算出 $\gcd(35,72)=1$. 这有多种方法，例如，35 只含素因子 5 和 7，而 72 只含素因子 2 和 3，两者没有共同的素因子，故互素. 但考虑到第二个要求，应该用辗转相除法.

$$72=2\times35+2,$$
$$35=17\times2+1,$$

得 $\gcd(35,72)=1$，故 35 和 72 互素.

又由上述两式得，

$$\begin{aligned}1&=35-17\times2\\&=35-17\times(72-2\times35)\\&=35\times35-17\times72,\end{aligned}$$

即 $x=35,y=-17$.

3. 首先不难验证：对任意的正整数 x 和 y，$\min(x,y)+\max(x,y)=x+y$.

设

$$a=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k},\ b=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k},$$

其中 $p_1,p_2,\cdots,p_k$ 是互不相同的素数，$r_1,r_2,\cdots,r_k,s_1,s_2,\cdots,s_k$ 是非负整数. 则

$$\gcd(a,b)=p_1^{\min(r_1,s_1)}p_2^{\min(r_2,s_2)}\cdots p_k^{\min(r_k,s_k)},$$
$$\operatorname{lcm}(a,b)=p_1^{\max(r_1,s_1)}p_2^{\max(r_2,s_2)}\cdots p_k^{\max(r_k,s_k)}.$$

于是

$$\begin{aligned}\gcd(a,b)\cdot\operatorname{lcm}(a,b)&=p_1^{\min(r_1,s_1)+\max(r_1,s_1)}p_2^{\min(r_2,s_2)+\max(r_2,s_2)}\cdots p_k^{\min(r_k,s_k)+\max(r_k,s_k)}\\&=p_1^{r_1+s_1}p_2^{r_2+s_2}\cdots p_k^{r_k+s_k}\\&=ab.\end{aligned}$$

4. $1,2,\cdots,15$ 中与 15 互素的数是 $1,2,4,7,8,11,13,14$，故 $\phi(15)=8$.

题型三：同余的概念及性质

1. 判断下列命题的真假.

(1) $527 \equiv 465 \pmod{15}$.

(2) $215 \equiv -175 \pmod{13}$.

2. 计算：

(1) $2\,100 \bmod 11$.

(2) $2^{340} \bmod 31$.

3. 求使下列同余关系成立的所有正整数 x.

(1) $20 \equiv 2 \pmod{x}$.

(2) $30 \equiv x \pmod{8}$.

(3) $x \equiv 3 \pmod{5}$.

4. 证明同余关系是等价关系，即同余关系具有

(1) 自反性：$a \equiv a \pmod{m}$.

(2) 对称性：$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

(3) 传递性：$a \equiv b \pmod{m}$ 且 $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

解答与分析

1. (1) 假. (2) 真.

2. (1) 方法一　用带余除法. 由 $2\,100 = 190 \times 11 + 10$，得 $2\,100 \bmod 11 = 10$.

方法二　利用同余的性质化简计算. 因为

$$2\,100 \equiv 21 \times 10 \times 10 \equiv (-1) \times (-1) \times (-1) \equiv -1 \equiv 10 \pmod{11},$$

故 $2\,100 \bmod 11 = 10$.

显然，当数不大时，可以用带余除法直接计算余数. 而当数很大或由较复杂的形式表示时，则需要设法用同余的性质化简计算.

(2) 因为 $2^{340} \equiv 2^{5\times 68} \equiv 32^{68} \equiv 1^{68} \equiv 1 \pmod{31}$，故 $2^{340} \bmod 31 = 1$.

3. (1) $x \mid (20-2)$，即 $x \mid 18$，故 $x = 1, 2, 3, 6, 9, 18$.

(2) $8 \mid (30 - x)$，得 $x = 30 - 8k$，其中 k 为小于等于 3 的整数.

(3) $5 \mid (x - 3)$，得 $x = 3 + 5k$，其中 k 为非负整数.

4. (1) 显然.

(2) 由 $a \equiv b \pmod{m}$，有 $m \mid (a-b)$，自然也有 $m \mid (b-a)$，故 $b \equiv a \pmod{m}$.

(3) 根据定义，由 $a \equiv b \pmod{m}$，有 $m \mid (a-b)$，即 $a = b + k_1 m$. 同理，由 $b \equiv c \pmod{m}$，有 $b = c + k_2 m$. 于是，$a = c + k_2 m + k_1 m = c + (k_1 + k_2)m$，故 $a \equiv c \pmod{m}$.

题型四：解一次同余方程和求模 m 逆

1. 下列一次同余方程是否有解？若有解，试给出它的全部解.
   (1) $10x \equiv 6 \pmod 4$.
   (2) $15x \equiv 6 \pmod{10}$.
2. 对下列每一组数 a 和 m，是否有 a 的模 m 逆？若有，试给出.
   (1) $a = 8, m = 3$.

   (2) $a = 20, m = 8$.

解答与分析

1. (1) $\gcd(10,4) = 2, 2 \mid 6$，根据定理 4.1.9，方程有解. 取模 4 等价类的代表元 $-1,0,1,2$，代入方程验证，得

$$10 \times (-1) \equiv 10 \times 1 \equiv 2 \equiv 6 \pmod 4,$$
$$10 \times 0 \equiv 10 \times 2 \equiv 0 \pmod 4,$$

故

$$x \equiv -1, 1 \pmod 4,$$

即

$$x = 4k \pm 1, k \in \mathbb{Z}.$$

   (2) $\gcd(15,10) = 5, 5 \nmid 6$，故方程无解.

2. (1) 8 与 3 互素，根据定理 4.1.10，8 的模 3 逆存在.

方法一　直接观察. 不难看出 $2 \times 8 \equiv 1 \pmod 3$，故 $8^{-1} \equiv 2 \pmod 3$.

方法二　检查模 3 等价类的代表元 $0,1,2$. 检查结果如下：

$$0 \times 8 \equiv 0 \pmod 3,$$
$$1 \times 8 \equiv 2 \pmod 3,$$
$$2 \times 8 \equiv 1 \pmod 3.$$

故

$$8^{-1} \equiv 2 \pmod 3.$$

方法三　用辗转相除法. 计算如下：

$$\begin{aligned} 8 &= 2 \times 3 + 2, \\ 3 &= 2 + 1, \\ 1 &= 3 - 2 \\ &= 3 - (8 - 2 \times 3) \\ &= 3 \times 3 - 8, \end{aligned}$$

得

$$(-1) \times 8 \equiv 1 \pmod 3,$$
$$8^{-1} \equiv -1 \equiv 2 \pmod 3.$$

   (2) $\gcd(20,8) = 4$，20 与 8 不互素，故 20 的模 8 逆不存在.

题型五：欧拉定理和费马小定理的应用

1. 利用费马小定理证明 10 不是素数.
2. 利用费马小定理计算 $5^{923} \bmod 11$.

解答与分析

1. $3^{10-1} \equiv 27^3 \equiv (-3)^3 \equiv -27 \equiv 3 \not\equiv 1 \pmod{10}$，根据费马小定理，得证 10 不是素数.
2. $5^{923} \equiv 5^{10\times 92+3} \equiv (5^{10})^{92} \times 5^3 \equiv 5^3 \equiv 4 \pmod{11}$，得 $5^{923} \bmod 11 = 4$.

作业

1. 填空题(6 小题,每小题 5 分,共 30 分).

   (1) 下列各式中成立的是________.

   A. $-5 \mid 25$　B. $8 \mid 2$　C. $-18 \bmod 4 = -2$　D. $3 \equiv 28 \pmod 5$　E. $8^{-1} \equiv 2 \pmod 4$

   (2) 42 的所有因子为________.

   (3) 450 的素因子分解为________.

   (4) 5 的模 6 逆等于________.

   (5) 欧拉函数 $\phi(20) =$________.

   (6) $\mathbb{Z}_4$ 上的乘法表为________.

2. 计算题(6 小题,每小题 10 分,共 60 分).

   (1) 求 84 与 198 的最大公因数和最小公倍数.

   (2) 验证 21 与 275 互素,并求 x 和 y 使得 $21x + 275y = 1$.

   (3) 求使同余式 $15 \equiv -13 \pmod m$ 成立的所有正整数 m.

   (4) 一次同余方程 $8x \equiv 14 \pmod 6$ 是否有解?若有解,试给出它的全部解.

   (5) 求 $35^{-1} \pmod 8$.

   (6) 计算:

   (a) $12^{1\,000} \bmod 7$.

   (b) $3^{1\,002} \bmod 10$.

3. 证明题(10 分).

   已知 $a \equiv b \pmod m$,求证 $\gcd(a, m) = \gcd(b, m)$.