第2章习题

2.1 整除

解答题

1. 求以下整数对的最大公因子：(1) $(55, 85)$；(2) $(202, 282)$；(3) $(666, 1414)$；(4) $(20785, 44350)$.

解：(1) 5；(2) 2；(3) 2；(4) 5.

2. 求以下整数对的最小公倍数：(1) $(231, 732)$；(2) $(-871, 728)$.

解：(1) 56364；(2) 48776.

3. 求以下整数的标准分解式：(1) 36；(2) 69；(3) 200；(4) 289.

解：(1) $36 = 2^2 \times 3^2$；(2) $69 = 3 \times 23$；
(3) $200 = 2^3 \times 5^2$；(4) $289 = 17^2$.

4. 设a为正整数，问a^4-3a^2+9是素数还是合数？

解：

$$\begin{aligned}a^4-3a^2+9&=(a^2+3)^2-9a^2\\&=(a^2+3)^2-(3a)^2\\&=(a^2+3a+3)(a^2-3a+3)\\&=[(a+1)(a+2)+1][(a-1)(a-2)+1]\end{aligned}$$

$a=1$或2时，$(a-1)(a-2)+1=1$，此时$(a+1)(a+2)+1=7$或13，那么a^4-3a^2+9为素数；当$a>2$时，$(a+1)(a+2)+1>1$，$(a-1)(a-2)+1>1$，故此时a^4-3a^2+9一定为合数.

证明题

1. 证明若$2|n,5|n,7|n$，那么$70|n$.

证明：$[2,5,7]|n$，即$70|n$

2. 证明任意三个连续的正整数的乘积都被6整除.

证明：连续的三个正整数中至少有一个为偶数，连续的三个正整数中一定存在一个3的倍数.

3. 证明每个奇数的平方都具有$8k+1$的形式.

证明：设奇数为$2n+1$. 有$(2n+1)^2=4n^2+4n+1=4n(n+1)+1$，$n$和$n+1$中

一定有一个偶数，所以$8|4n(n+1)$.

4. 证明若$m-p|mn+pq$，则$m-p|mq+np$.

证明：因为$m-p|(m-p)(n-q)$且$m-p|mn+pq$，所以$m-p|(mn+pq)-(m-p)(n-q) \Rightarrow m-p|mq+np$

5. 证明若a是整数，则a^3-a 能被3整除.

证明：$a^3-a=(a-1)a(a+1)$，连续三个整数中必有一个3的倍数.

6. 证明对于任意给定的正整数k，必有k个连续的正整数都是合数.

证明：定理2.1.6

$(k+1)!+2, (k+1)!+3, \ldots, (k+1)!+(k+1)$.

7. 证明若整数a, b满足$(a,b)=1$，那么$(a+b, a-b)=1$或2.

证明：设$d=(a+b, a-b)$. 有$d|a+b, d|a-b \Rightarrow d|2a, d|2b \Rightarrow d|(2a, 2b) \Rightarrow d|2(a,b) \Rightarrow d|2 \Rightarrow d=1$或2

8. 证明若整数a, b满足$(a,b)=1$，那么$(a+b, a^2+b^2)=1$或2.

证明：设$d=(a+b,a^2+b^2)$. 有$d|a+b,d|a^2+b^2\Rightarrow d|2ab\Rightarrow d|2$或$d|a$或$d|b$. 如果$d|a$，那么由于$d|a+b$，所以$d|b$，故$d|(a,b)\Rightarrow d|1\Rightarrow d=1$. 如果$d|2$，那么$d=1$或2.

9. 证明若k为正整数，那么$3k+2$与$5k+3$互素.

证明：$5(3k+2)+(-3)(5k+3)=1$.

10. 证明$12|n^4+2n^3+11n^2+10n$.

证明：

$$\begin{aligned} n^4+2n^3+11n^2+10n &= n^4+2n^3-n^2-2n+12n^2+12n \\ &= n^2(n^2-1)+2n(n^2-1)+12n(n+1) \\ &= (n^2+2n)(n^2-1)+12n(n+1) \\ &= (n-1)n(n+1)(n+2)+12n(n+1) \end{aligned}$$

连续四个整数中一定有两个偶数，也一定至少有一个3的倍数，故$12|(n-1)n(n+1)(n+2)$.

11. 设$3|a^2+b^2$，证明$3|a$且$3|b$.

证明：任意一个整数可以表示为$3k,3k+1,3k+2$中的一种形式. 只有当a,b都是$3k$的形式时，a^2+b^2才能被3整除.

12. 设n,k是正整数，证明n^k 与n^{k+4}的个位数字相同.

证明：即要证$10|n^{k+4}-n^k$. 已知$n^{k+4}-n^k=n^k(n^4-1)=n^k(n^2+1)(n^2-1)$. 显然$2|n^k(n^2+1)(n^2-1)$. 任意一个整数都可以表示为$5k,5k\pm1,5k\pm2$中的一种形式. 当$n=5k\pm2$ 时，$5|n^2+1$；当$n=5k\pm1$ 时，$5|n^2-1$；当$n=5k$时，$5|n^k$. 综上，$10|n^k(n^2+1)(n^2-1)$.

13. 证明对于任何整数n,m，等式$n^2+(n+1)^2=m^2+2$不可能成立.

证明：等式整理为$2n(n+1)=m^2+1$. 等式左边被4整除，那么m只能取奇数，但此时m^2+1只能表示为$4k^2+4k+2$ 的形式，不能被4整除.

14. 证明n的标准分解式中次数都是偶数，当且仅当n是完全平方数.

证明：略.

15. 证明若a,b是正整数，且满足$a^3|b^2$，那么$a|b$.

证明：设p为a的素因子，而且设$p^r|a$且$p^{r+1}\nmid a$. 那么有$p^{3r}|a^3\Rightarrow p^{3r}|b^2$. 设$p^s|b$且$p^{s+1}\nmid b$，那么有$3r\leq 2s\Rightarrow r\leq\frac{2}{3}s<s$，所以有$p^r|b$. 以上对于$a$的所有素因子都成立，所以有$a|b$.

16. 证明$\sqrt[3]{5}$为无理数.

证明：假设$\sqrt[3]{5}=\frac{a}{b}$，a,b为整数且$(a,b)=1$. 那么有$a^3=5b^3$，所以$5|a^3\Rightarrow$

$5|a \Rightarrow 5^3|a^3 \Rightarrow 5^3|5b^3 \Rightarrow 5^2|b^3 \Rightarrow 5|b \Rightarrow 5|(a,b)$，矛盾.

17*. 证明在$1, 2, 3, \ldots, 2n$中任取$n+1$个数，其中至少有一个能被另一个整除.

证明： 整数都可以表示为$a \cdot 2^k$的形式，其中a为奇数. 我们可以根据a的值，对整数进行分类. 同一类中的整数，有相同的奇数因子，不同的是k的值. $1, \cdots, 2n$中有n个奇数，那么可以分为n类. 任取$n+1$ 个数时，根据鸽笼原理，至少有2个数会在同一类，k值大的数会被k 值小的数整除.

18*. 证明对于任意给定的n个整数，必可以从中找出若干个数作和，使得这个和能被n整除.

证明： 设n个数为$a_1, a_2, \ldots, a_n$. 设$S_1 = a_1$, $S_2 = a_1 + a_2, \ldots, S_n = a_1 + a_2 + \cdots + a_n$. 若某个$S_i$能够被$n$整除，那么得证；已知$0, 1, \ldots, n-1$是一个模$n$的完全剩余系，若所有和式都不能被$n$ 整除，那么这些和式都不会以0为代表元的剩余类中. 也就是说n个数要“放到”$n-1$个剩余类中，根据鸽笼原理，至少有两个和式S_i, S_j会在同一剩余类中，此时$S_i - S_j \equiv 0 \pmod{n}$，即$S_i - S_j$能被$n$整除.

19*. 证明$1 + \frac{1}{2} + \cdots + \frac{1}{n}$ $(n \geq 2)$不是整数.

证明： 假设$1 + \frac{1}{2} + \cdots \frac{1}{n} = Q$，$Q$为整数. 令$2^\alpha \leq n$且$2^{\alpha+1} > n$，$R = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$，其中$p_i$为奇素数，满足$p_i^{\beta_i} \leq n$且$p_i^{\beta_i+1} > n$. 在等式两边乘上$2^{\alpha-1}R$，可以得到$A + \frac{1}{2} = 2^{\alpha-1}RQ$，其中$A$ 为整数. 矛盾.

20**. 证明若m,n,a为正整数且$a>1$，则有$(a^m-1,a^n-1)=a^{(m,n)}-1$.

证明：对于整数u,v，有带余除法$u=vq+r,\ 0\le r<v$. 那么有

$$\begin{aligned}
a^u-1&=a^{vq+r}-1\\
&=a^{vq}a^r-a^r+a^r-1\\
&=(a^{vq}-1)a^r+(a^r-1)\\
&=(a^v-1)(a^{v(q-1)+r}+\cdots+a^{v+r}+a^r)+(a^r-1)
\end{aligned}$$

这就说明$u\equiv r\pmod v$时，有$a^u-1\equiv a^r-1\pmod{a^v-1}$. 令$r_0=m,\ r_1=n,\ R_0=a^m-1=a^{r_0}-1,\ R_1=a^n-1=a^{r_1}-1$. 下面开始执行欧几里得算法：

$$\begin{array}{cc}
r_0=r_1q_1+r_2,\quad 0\le r_2<r_1 & R_0=R_1Q_1+R_2,\quad R_2=a^{r_2}-1\\
r_1=r_2q_2+r_3,\quad 0\le r_3<r_2 & R_1=R_2Q_2+R_3,\quad R_3=a^{r_3}-1\\
\vdots & \vdots\\
r_{k-2}=r_{k-1}q_{k-2}+r_k,\quad 0\le r_k<r_{k-1} & R_{k-2}=R_{k-1}Q_{k-1}+R_k,\quad R_k=a^{r_k}-1\\
r_{k-1}=r_kq_k+r_{k+1},\quad r_{k+1}=0 & R_{k-1}=R_kQ_k+R_{k+1},\quad R_{k+1}=a^{r_{k+1}}-1=0
\end{array}$$

所以有$(m,n)=r_k$，$(a^m-1,a^n-1)=R_k=a^{r_k}-1=a^{(m,n)}-1$.

编程练习

1. 编写程序求1000000内的所有素数.

2. 编写程序计算整数a,b的最大公因子.

3. 编写程序求正整数n的素因子分解.

2.2 同余

解答题

1. 求7^{2046}写成十进制数时的个位数字.

解：即计算$7^{2046} \pmod{10}$.

$\varphi(10)=4$，$2046=4\times 511+2$，$7^{2046}\equiv 7^2\equiv 9 \pmod{10}$.

2. 求2^{1000}的十进制表示中的末尾两位数字.

解：即计算$2^{1000} \pmod{100}=76$

3. 求$1^5+2^5+3^5+\cdots+99^5$被4除的余数.

解：

$$\begin{aligned}
&1^5+2^5+\cdots+99^5\\
\equiv\ &0^5+1^5+2^5+\cdots+99^5\\
\equiv\ &(0^5+1^5+2^5+3^5)+(4^5+5^5+6^5+7^5)+\cdots+(96^5+97^5+98^5+99^5)\\
\equiv\ &(0^5+1^5+0\cdot 2^3+(-1)^5)+(0^5+1^5+0\cdot 2^3+(-1)^5)+\cdots+(0^5+1^5+0\cdot 2^3+(-1)^5)\\
\equiv\ &0 \pmod 4
\end{aligned}$$

4. 计算555^{555}被7除的余数.

解：$555^{555}\equiv 2^{555}\equiv 1 \pmod 7$.

注：可以算$555 \pmod 6$，也可以算$555 \pmod 3$.

5. 求模11的一个完全剩余系$\{r_1, r_2, \ldots, r_{11}\}$，满足$r_i \equiv 1 \pmod 3$, $1 \leq i \leq 11$.

解：1,4,7,10,13,16,19,22,25,28,31

6. 计算以下整数的欧拉函数：(1) 24；(2) 64；(3) 187；(4) 360.

解：

(1) 8；(2) 32；(3) 160；(4) 96.

7. 利用**费马小定理**求解以下题目：

(1) 求a $(0 \leq a < 73)$，使得$a \equiv 9^{794} \pmod{73}$；

(2) 解方程$x^{86} \equiv 6 \pmod{29}$；

(3) 解方程$x^{39} \equiv 3 \pmod{13}$.

解：

(1) $9^{73} \equiv 9 \pmod{73}$，结果为$a = 8$

(2) $x^{29} \equiv x \pmod{29}$，结果为$x \equiv 8, 21 \pmod{29}$

(3) $x^{13} \equiv x \pmod{13}$，无解.

8. 求$229^{-1} \pmod{281}$. **解**：27

9**. 写出所有$\varphi(m)$不能被4整除的m. (不要用列举法，用表达式来表示m)

解：设$m = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，那么$\varphi(m) = 2^{\alpha-1}p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_k^{\alpha_k-1}(p_k-1)$. 观察以下情况：

(1) 当$\alpha \geq 3$时，$\varphi(m)$一定能被4整除，因此α只能取0,1,2；

(2) 已知p_i为奇素数，那么p_i-1为偶数；当m包括两种及以上的素因子时，$\varphi(m)$能被4整除，因此m最多只能有一种素因子；

(3) 当$\alpha = 2$且m有素因子时，$\varphi(m)$能被4整除，因此$\alpha = 2$时m不能有素因子；

(4) 奇素数可以分为两类：$p_i \equiv 1,3 \pmod 4$，当$p_i \equiv 1 \pmod 4$时，p_i-1被4整除，因此若m有素因子，该素因子只能是$p_i \equiv 3 \pmod 4$形式的.

综上，$m = 4$或$2^{\alpha}p^{\beta}$，其中$\alpha = 0$或$1, p \equiv 3 \pmod 4$.

10. 求解下列一次同余方程：

(1) $27x \equiv 12 \pmod{15}$

(2) $24x \equiv 6 \pmod{81}$

(3) $91x \equiv 26 \pmod{169}$

(4) $71x \equiv 32 \pmod{3441}$

解：

(1) $x \equiv 1, 6, 11 \pmod{15}$

(2) $x \equiv 7, 34, 61 \pmod{81}$

(3) $x \equiv 4 + 13t \pmod{169}, t = 0, 1, \ldots, 12$

(4) $x \equiv 1309 \pmod{3441}$

11. 如果在一个密码系统中，明文x被加密成密文y，加密过程可表示

为$y\equiv 7x+3 \pmod{26}$，那么由密文y得到明文的解密过程可由什么公式表示？

解：

$x\equiv 7^{-1}(y-3)\equiv 15(y-3)\equiv 15y+7 \pmod{26}$

12. 求解线性同余方程组.

(1) $\begin{cases} x\equiv 9 \pmod{12} \\ x\equiv 6 \pmod{25} \end{cases}$ (2) $\begin{cases} x\equiv 5 \pmod{7} \\ x\equiv 12 \pmod{15} \\ x\equiv 18 \pmod{22} \end{cases}$ (3) $\begin{cases} x\equiv 2 \pmod{9} \\ 3x\equiv 4 \pmod{5} \\ 4x\equiv 3 \pmod{7} \end{cases}$

解：

(1) $x\equiv 81 \pmod{300}$

(2) $x\equiv 1272 \pmod{2310}$

(3) $x\equiv 83 \pmod{315}$

13. 有总数不满50人的一对士兵. 一至三报数，最后一人报“一”；一至五报数，最后一人报“二”；一至七报数，最后一人也报“二”. 问：这队士兵有多少人？

解： 设士兵有x人($x<50$)，解方程组

$$\begin{cases} x\equiv 1 \pmod{3} \\ x\equiv 2 \pmod{5} \\ x\equiv 2 \pmod{7} \end{cases}$$

解得$x=37$.

14. 利用转化成联立方程组的方法解$91x \equiv 419 \pmod{440}$.

解:

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{8} \\ x \equiv 4 \pmod{11} \end{cases}$$

解得$x \equiv 169 \pmod{440}$

15. 一个数被$3, 5, 7, 11$除所得的余数均为2，且为13的倍数. 求出符合上述条件的最小正整数.

解：该数为x

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 2 \pmod{7} \\ x \equiv 2 \pmod{11} \\ x \equiv 0 \pmod{13} \end{cases}$$

解得$x = 1157$

16. 已知有相邻的4个整数，它们依次可被$2^2, 3^2, 5^2, 7^2$整除. 求出符合上述条件的最小的一组正整数.

解：设这4个数里最小的为x

$$\begin{cases} x \equiv 0 \pmod{4} \\ x+1 \equiv 0 \pmod{9} \\ x+2 \equiv 0 \pmod{25} \\ x+3 \equiv 0 \pmod{49} \end{cases}$$

解得四个数为29348,29349,29350,29351.

17. 已知Hill密码中的明文分组长度是2，密钥**K**是一个2阶可逆方阵. 假设明文3, 14, 2, 19对应的密文是1, 14, 11, 21，试求密钥**K**.

解：

$$\begin{pmatrix} 3 & 14 \\ 2 & 19 \end{pmatrix} \cdot \mathbf{K} \equiv \begin{pmatrix} 1 & 14 \\ 11 & 21 \end{pmatrix} \pmod{26}$$

从而有

$$\begin{aligned} \mathbf{K} &\equiv \begin{pmatrix} 3 & 14 \\ 2 & 19 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 14 \\ 11 & 21 \end{pmatrix} \\ &\equiv \frac{1}{29} \begin{pmatrix} 19 & -14 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 14 \\ 11 & 21 \end{pmatrix} \\ &\equiv \begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix} \pmod{26} \end{aligned}$$

18. 求解同余方程$3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod{5}$.

解：原方程可化简为$3x^2 + 4x + 2x^3 + x + x^2 + x^3 + 2x^2 + x \equiv 3x^3 + x^2 + x$

$\pmod 5$，直接验证可得解为$x \equiv 0, 1, 2 \pmod 5$.

证明题

1. 证明正整数n能被3整除的充要条件是将n的十进制表示中的各位数字相加所得之和能被3整除.

证明：

$10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 3$

2. 设$f(x)$是整系数多项式，且$f(1), f(2), \ldots, f(m)$都不能被m整除，证明$f(x) = 0$没有整数解.

证明：对于任意整数x，$x \pmod m$只存在以下情况$x \equiv i \pmod m$，$i = 1, 2, \ldots, m$. 因为f是整系数多项式，所以有$f(x) \equiv f(i) \pmod m$，$i = 1, 2, \ldots, m$. 由于$f(i)$都不能被m整除，因此$f(x) \pmod m \neq 0$. 故没有整数解.

3. 证明当$m > 2$时，$0^2, 1^2, \ldots, (m-1)^2$一定不是模$m$的完全剩余系.

证明：$1^2 \equiv (m-1)^2 \pmod m$

4. 设有m个整数，它们都不属于模m的0剩余类，证明其中必有两个数属于同一剩余类.

证明：鸽笼原理，m个整数“放到”$m-1$个剩余类中.

5. 证明$2, 2^2, 2^3, \ldots, 2^{18}$ 是模27的一个缩系.

证明：假设存在$0 < j < i \leq 18$使得$2^i \equiv 2^j \pmod{27}$，即$2^{i-j} \equiv 1 \pmod{27}$. 已知$2^{18} \equiv 1 \pmod{27}$，$1 \leq i-j \leq 17$，18的因子有$1, 2, 3, 6, 9, 18$，我们只需检验$i-j = 6, 9$的情况. 经检验，$2^6$和$2^9$模27都不等于1，因此不存在$1 \leq i-j \leq 17$满足$2^{i-j} \equiv 1 \pmod{27}$，故假设不成立.

6. 证明：如果p是奇素数，那么

$$1^2 3^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

证明：

$$\begin{aligned}
1^2 3^2 \cdots (p-4)^2 (p-2)^2 &\equiv 1(1-p+p)3(3-p+p)\cdots(p-4)(p-4-p)(p-2)(p-2-p) \\
&\equiv 1 \cdot (-2) \cdot 3 \cdot (-4) \cdots (p-4) \cdot (-1)(p-3) \cdot (p-2) \cdot (-1)(p-1) \\
&\equiv (-1)^{\frac{p-1}{2}} (p-1)! \\
&\equiv (-1)^{\frac{p+1}{2}} \pmod{p}
\end{aligned}$$

7. 证明：若a是整数，且$(a, 3) = 1$，那么$a^7 \equiv a \pmod{63}$.

证明：根据费马小定理，有$a^7 \equiv a \pmod 7$，根据欧拉定理有$a^6 \equiv 1 \pmod 9 \Rightarrow a^7 \equiv a \pmod 9$. 综上，$a^7 \equiv a \pmod{63}$.

8. 证明$m > 3$时，$\varphi(m)$总是偶数.

证明：设$m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. m有奇素因子，$\varphi(m)$一定是偶数. 若m没有素因子，那么在$m > 3$的情况下，α一定大于1，那么$\varphi(m)$一定是偶数.

9. 若p为素数，n为正整数，证明$p \nmid n$当且仅当$\varphi(pn) = (p-1)\varphi(n)$.

证明：

"$\Rightarrow$"：$p \nmid n \Rightarrow (p, n) = 1 \Rightarrow \varphi(pn) = \varphi(p)\varphi(n) = (p-1)\varphi(n)$

"$\Leftarrow$"：假设$p|n$. 设$n = p^k m$, $(p, m) = 1$，那么等式右边有$\varphi(pn) = \varphi(p^{k+1}m) = \varphi(p^{k+1})\varphi(m) = (p-1)p^k\varphi(m)$；另一边有$(p-1)\varphi(n) = (p-1)\varphi(p^k m) = (p-1)^2 p^{k-1}\varphi(m)$，两侧不相等，假设不成立.

10. 若p为素数，且$0 < k < p$，证明$(p-k)!(k-1)! \equiv (-1)^k \pmod p$.

证明：

$$\begin{aligned}
(p-k)!(k-1)! &\equiv (p-k)!(-p+k-1)(-p+k-2)\cdots(-p+2)(-p+1) \\
&\equiv (p-k)!(-1)^{k-1}(p-(k-1))(p-(k-2))\cdots(p-2)(p-1) \\
&\equiv (-1)^{k-1}(p-1)! \\
&\equiv (-1)^k \pmod p
\end{aligned}$$

11. 设$a > 2$是奇数，证明

(1) 一定存在正整数$d \leq a-1$，使得$a|2^d-1$；

(2) 若d_0是满足(1)的最小正整数，那么$a|2^h-1$的充要条件是$d_0|h$.

证明：

(1) $(a,2)=1$，所以有$2^{\varphi(a)} \equiv 1 \pmod a$，显然$\varphi(a) \leq a-1$，故一定存在.

(2) 定理4.1.1的证明过程.

12. 证明同余方程$2x^3-x^2+3x+11 \equiv 0 \pmod 5$有3个解.

证明：定理3.7.7

$2x^3-x^2+3x+11 \equiv 0 \pmod 5 \Rightarrow x^3-3x^2+4x+3 \equiv 0 \pmod 5$

$x^5-x = (x^3-3x^2+4x+3)(x^2+3x+5)-15(2x+1)$，余式的系数都可被5整除.

编程练习

1. 编写计算正整数欧拉函数的程序.

2. 编程判断两个正整数m,n是否互素，如果互素，求出$m^{-1} \pmod n$和$n^{-1} \pmod m$.

3. 编程判断同余方程$ax \equiv b \pmod m$是否有解，如果有解，求出所有的解.

4. 编程实现中国剩余定理.