第2章习题

注：请大家自学鸽笼原理(也称抽屉原理)，有些题目会涉及

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) $(20785, 44350)$.

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

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

4. 设a为正整数，问$a^4 - 3a^2 + 9$是素数还是合数？

证明题

1. 证明若$2|n, 5|n, 7|n$，那么$70|n$.

2. 证明任意三个连续的正整数的乘积都被6整除.

3. 证明每个奇数的平方都具有$8k + 1$的形式.

4. 证明若$m - p|mn + pq$，则$m - p|mq + np$.

5. 证明若a是整数，则$a^3 - a$能被3整除.

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.

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

9. 证明若k为正整数，那么$3k + 2$与$5k + 3$互素.

10. 证明$12 | n^4 + 2n^3 + 11n^2 + 10n$.

11. 设$3 | a^2 + b^2$，证明$3 | a$且$3 | b$.

12. 设n, k是正整数，证明n^k与n^{k+4}的个位数字相同.

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.

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.

15. 证明若a, b是正整数，且满足$a^3 | b^2$，那么$a | b$.

16. 证明$\sqrt[3]{5}$为无理数.

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.

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.

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

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

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.

2. 求2^{1000}的十进制表示中的末尾两位数字.

3. 求$1^5+2^5+3^5+\cdots+99^5$被4除的余数.

4. 计算555^{555}被7除的余数.

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

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

7. 利用**费马大定理**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$x^{39} \equiv 3 \pmod{13}$.

8. 求$229^{-1} \pmod{281}$.

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)

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

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？

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) $\begin{cases} x \equiv 2 \pmod{9} \\ 3x \equiv 4 \pmod{5} \\ 4x \equiv 3 \pmod{7} \end{cases}$

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？

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

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.

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.

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**.

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

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.

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.

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.

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

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

6. 证明：如果p是奇素数，那么

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

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

8. 证明$m > 3$时，$\varphi(m)$总是偶数.

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

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

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$d_0|h$.

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

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.