



华中科技大学计算机与科学技术学院 2024~2025 第一学
期

“ 离散数学（二） ” 期中考试试卷

考试方式 闭卷 考试日期 2024-10-16 考试时长 50 分钟

专业班级 学 号 姓 名

| 题号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 总分 | 总分人 | 核对人 |
|----|----|----|----|----|----|----|----|-----|-----|-----|
| 分值 | 20 | 10 | 10 | 20 | 10 | 10 | 20 | 100 | | |
| 得分 | | | | | | | | | | |

1. 分别计算 $3^{963} \bmod 35$ 以及 $17! \bmod 19$ 的值。(20 分)

参考答案:

因为 $\gcd(3,35)=1$, 且 $\varphi(35)=24$, 则 $3^{963} \bmod 35 = 3^3 \bmod 35 = 27$;

因为 19 为质数, 先计算 $18 \bmod 19$ 的逆元为 -1, 再在 $18! \bmod 19 = -1$
 $(\bmod 19)$ 两端同时乘上 $18 \bmod 19$ 的逆元, 即 -1, 可得 $17! \bmod 19 = 1 \bmod 19$

2. 求线性同余式 $35x \equiv 10 \bmod 50$ 的所有解。(10 分)

参考答案:

化简上述同余式得 $7x \equiv 2 \bmod 10$, 再求 $7 \bmod 10$ 的逆元为 3, 因此 $x \equiv 6 \bmod 10$, 即 $x = 6 + 10k$, 这里 k 是任意整数, 即 $x = 6, 16, 26, 36, \dots, -4, -14, -24, \dots$

3. 将整数 5 允许重复地有序拆分成三个非负整数的方案有几个? 要求写出具体求解过程。(10 分)

参考答案:

求 $x_1+x_2+x_3=5$, 其中 x_1, x_2 和 x_3 均为非负整数的解个数, 允许重复的组合, 即 $C(3+5-1, 2)=C(7, 2)=21$ 个方案。

4. 分别使用欧几里得算法反向处理, 以及扩展欧几里得算法把 $\gcd(100001, 1001)$ 表示成 100001 和 1001 的线性组合。 (20 分)

参考答案:

① 欧几里得反向处理:

$$\begin{aligned} 100001 &= 100 \times 999 + 902 \\ 1001 &= 902 \times 1 + 99 \\ 902 &= 99 \times 9 + 11 \\ 99 &= 11 \times 9 + 0 \end{aligned}$$

$$\begin{aligned} \therefore \gcd(100001, 1001) &= 11 = 902 - 99 \times 9 \\ &= 902 - 99(1001 - 902) \\ &= 902 \times 10 - 9 \times 1001 \\ &= (100001 - 1001 \times 99) \times 10 - 9 \times 1001 \\ &= 10 \times 100001 - 999 \times 1001 \end{aligned}$$

② 扩展欧几里得:

其中 $q_1=99, q_2=1, q_3=9, q_4=9$.

$$\begin{aligned} s_0 &= 1, s_1 = 0, \\ t_0 &= 0, t_1 = 1, \end{aligned}$$

根据 $s_j = s_{j-2} - q_{j-1} s_{j-1}$ 和 $t_j = t_{j-2} - q_{j-1} t_{j-1}$ 得

$$\begin{aligned} s_2 &= s_0 - q_1 s_1 = 1 & t_2 &= t_0 - q_1 t_1 = -99 \\ s_3 &= s_1 - q_2 s_2 = -1 & t_3 &= t_1 - q_2 t_2 = 100 \\ s_4 &= s_2 - q_3 s_3 = 10 & t_4 &= t_2 - q_3 t_3 = -999 \end{aligned}$$

因此 $\gcd(100001, 1001) = 10 \times 100001 - 999 \times 1001$

5. 美国邮政服务局(USPS)出售的汇票由 11 位数字 x_1, x_2, \dots, x_{11} 标识。

前十位数字标识汇票, x_{11} 是校验数位, 满足 $x_{11} = x_1 + x_2 + \dots + x_{10} \bmod 9$ 。

9. 针对以下以这十位数字开头的数, 查找 USPS 汇票的校验码。(1)

7555618873。(2) 3289744134。(10 分)

参考答案:

(1) $(7+5+5+5+6+1+8++8+7+3) \bmod 9=1$

(2) 0

6. 证明: 当 p 是质数且 e 是正整数时, 欧拉函数 $\varphi(p^e)=p^{e-1}(p-1)$, 这里欧拉函数 $\varphi(n)$ 表示小于或等于 n 的正整数中与 n 互质的数的个数。

(10 分)

参考答案:

与 p^e 不互质的数有 $p, 2p, 3p, 4p, \dots, p^e$, 这里最后一个数 p^e 可以表示成 $p^{e-1} * p$, 所以共有 p^{e-1} 个数与 p^e 不互质; 此外小于或等于 p^e 的正整数有 p^e 个,

因此 $\varphi(p^e)=p^e - p^{e-1}=p^{e-1}(p-1)$, 举例而言, $\varphi(8)=\varphi(2^3)=4*1=4$, 即 1,3,5,7 四个数。

7. RSA 密码系统, $N=55$, $k=13$, $t=54$ 。(1) k 作为私钥, 求明文 t 对应的密文。(2) k 作为公钥, 求密文 t 对应的明文。(20 分)

参考答案:

(1) $N = 55 = 5 * 11$. 因此 $(p-1)(q-1)=40$. $13 * e \equiv 1(\bmod 40)$, 那么 $e=37$. 要加密, $C = 54^{37}$

$\bmod 55$. 计算可得 $C = 54$.

(2) $N = 55 = 5 * 11$. 因此 $(p-1)(q-1)=40$. 13 模 $(p-1)(q-1)$ 的逆为 d . 即 $d * 13 \equiv 1(\bmod 40)$, 可得 $d=37$. 要解密, $M = 54^{37} \bmod 55$. 计算可得 $M = 54$.