2006-2007 学年第二学期数论与代数结构考试题答案

1.（20） 设$a>2$是奇数．证明

（１）一定存在正整数$d \le a-1$，使得$a \mid 2^d-1$；

（２）设d_0是满足（１）的最小正整数．那么$a \mid 2^h-1(h \in N)$的充要条件是$d_0 \mid h$．

证明（ｉ）考虑以下a个数，$2^0, 2^1, 2^2, \cdots, 2^{a-1}$．

由$a \nmid 2^j (0 \le j < a)$及带余除法知，对每个$j, 0 \le j < a$，$2^j = q_j a + r_j, 0 < r_j < a$．

所以a个余数$r_0, r_1, \cdots, r_{a-1}$仅可能取$a-1$个值．因此其中必有两个相等，不妨设$0 \le i < k < a$且$r_i = r_k$，因而有 $a(q_k - q_i) = 2^k - 2^i = 2^i(2^{k-i}-1)$．

由$(a, 2)=1$，推出$a \mid 2^{k-i}-1$．取$d = k-i \le a-1$就满足要求．

（２）充分性是显然的，只要证必要性．同样由带余除法定理得

$$h = qd_0 + r, \quad 0 \le r < d_0 .$$

因而有

$$2^h - 1 = 2^{qd_0+r} - 2^r + 2^r - 1 = 2^r(2^{qd_0}-1) + (2^r - 1) .$$

由$a \mid 2^h-1$及$a \mid 2^{qd_0}-1$，易知$a \mid 2^r-1$．由此及d_0的最小性可以推出$r=0$，即$d_0 \mid h$．

2.（10 分）给定模m，及$0 \le a < m$，$0 \le x < \phi(m)$，试估计计算$a^x \pmod m$的复杂度。

解：给定模m，及$0 \le a < m$，$0 \le x < \phi(m)$，下面计算$a^x \pmod m$：

1 计算$x = (b_{l-1}, b_{l-1}, \cdots\cdots, b_0)_2$；

2 依次计算$a_1 = a^2 \bmod m$，$a_2 = (a_1)^2 = a^{2^2} \bmod m$，……，

$$a_{l-1} = (a_{l-2})^2 = a^{2^{l-1}} \bmod m ;$$

3 若 $b_0 = 0$， $a \leftarrow a^{b_0} \bmod m$；

对于 $i = 1,....l-1,\quad a \leftarrow a(a_i)^{b_i} \bmod m$.

所以利用模幂平方运算计算 $a^x (\bmod m)$ 需要 $O(\log_2^3 m)$ 次比特运算.

3. （20）给出一种由群 Z_p^*， Z_q^* 构造群 Z_{pq}^* 的方法， 其中 p, q 是素数，如果 p, q 是强素数，即存在 p', q' 使得 $p = 2p'+1,\quad q = 2q'+1$。试求出在群 Z_{pq}^* 中阶是 $2p'q'$ 的元素的个数。

解：这里我们给出一个一般的方法，设 $m = m_1 m_2$， $(m_1, m_2) = 1$. 当 $x_i^{(1)} (0 \le i \le m_1 - 1)$ 遍历模 m_1 的既约剩余系， $x_j^{(2)}$（ $0 \le j \le m_2 - 1$）遍历模 m_2 的既约剩余系时， $x_{ij} = m_2 x_i^{(1)} + m_1 x_j^{(2)}$ 遍历是模 m 的既约剩余系.

首先证明当 $x_i^{(1)} (0 \le i \le m_1 - 1)$， $x_j^{(2)}$（ $10 \le j \le m_2 - 1$）分别为模 m_1、 m_2 的完全剩余系时，

$$x_{ij} = m_2 x_i^{(1)} + m_1 x_j^{(2)}, 0 \le i < m_1, 0 \le j < m_2$$

构成模 m 的完全剩余系. 显然 x_{ij} 共有 $m = m_1 m_2$ 个数，因此只要证明它们两两对模 m 不同余. 若

$$m_2 x_{i_1}^{(1)} + m_1 x_{j_1}^{(2)} \equiv x_{i_1 j_1} \equiv x_{i_2 j_2} \equiv m_2 x_{i_2}^{(1)} + m_1 x_{j_2}^{(2)} (\bmod m_1 m_2) \quad ,$$

则

$$x_{i_1 j_1} \equiv x_{i_2 j_2} (\bmod m_1), \quad x_{i_1 j_1} \equiv x_{i_2 j_2} (\bmod m_2) .$$

从而

$$m_2 x_{i_1}^{(1)} \equiv m_2 x_{i_2}^{(1)} (\bmod m_1),$$

$$m_1 x_{j_1}^{(2)} \equiv m_1 x_{j_2}^{(2)} (\bmod m_2),$$

由 $(m_1, m_2) = 1$ 知，

$$x_{i_1}^{(1)} \equiv x_{i_2}^{(1)} (\bmod m_1), \quad x_{j_1}^{(2)} \equiv x_{j_2}^{(2)} (\bmod m_2) .$$

这就证明了 $m_1 m_2$ 个 x_{ij} 两两不同余，是模 m 的完全剩余系.

下面证明 $x_i^{(1)}$， $x_j^{(2)}$ 分别遍历 m_1， m_2 的既约剩余系时， x_{ij} 是模 m 的既约

剩余系．由以上证明知 x_{ij} 两两不同余。只要证明 $(x_{ij}, m)=1$ 当且仅当 $(x^{(1)}, m_1)=(x^{(2)}, m_2)=1$．由于

$$(m_1, m_2)=1,\ (x^{(1)}, m_1)=(x^{(2)}, m_2)=1,$$

所以 $(x_{ij}, m)=1$ 当且仅当

$$(m_2x^{(1)}+m_1x^{(2)}, m_1)=1,\ (m_2x^{(1)}+m_1x^{(2)}, m_2)=1$$

当且仅当 $(x^{(1)}, m_1)=(x^{(2)}, m_2)=1$．结论得证．

上面给出一种由群 Z_p^*，Z_q^* 构造群 Z_{pq}^* 的方法，在群 Z_{pq}^* 中阶是 $2p'q'$ 的元素的个数是 $(p'-1)(q'-1)$。

4.（20）设 p 是奇素数，证明：模 p 必有原根。

证明 由指数的性质知，一定存在整数 g 使得

$$\delta_p(g)=[\delta_p(1), \delta_p(2), \cdots, \delta_p(p-1)]=\delta .$$

下证 $\delta=p-1$．显然 $\delta \mid p-1$，从而 $\delta \le p-1$．由于 $\delta_p(i) \mid \delta,\ \ i=1, 2, \cdots, p-1.$ 因而同余方程

$$x^{\delta} \equiv 1 (\mathrm{mod}\ p)$$

有解 $x=1, 2, \cdots, p-1 (\mathrm{mod}\ p)$．又因为同余方程解的个数 $n \le \min\{\delta, p\}$，所以 $p-1 \le \delta$．故可得到 $\delta=p-1$，这就说明了 g 是模 p 的原根．

5.（20） 若 ϕ 是群 G 到群 G' 的同态满射，证明 $G/Ker\phi \cong G'$。

证明： 作一个映射：$\varphi: aK \mapsto a'=\phi(a)$，$(a \in G)$，则这是一个 G/K 到 G 的同构映射．

1) $aK=bK \Rightarrow ab^{-1} \in K \Rightarrow b^{-1}a \in K \Rightarrow b'^{-1}a'=e' \Rightarrow a'=b'$，说明 φ 映射下 G/K 的元素有唯一确定的象．

2) 给定 G' 的一个任意元 a'，在 G 里至少有一个元 a 满足 $\phi(a)=a'$，由 φ 的定义，对给定的 G' 的一个任意元 a'，aK 为其在 G/K 的原象．所以 φ 是 G/K 到 G 的满射．

3) $aK \neq bK \Rightarrow b^{-1}a \notin K \Rightarrow b'^{-1}a' \neq e' \Rightarrow a' \neq b'$，所以$\varphi$是$G/K$到$G$的单射.

4) 在φ之下，

$$\varphi(aK \circ bK) = \varphi(abK) = (ab)' = \phi(ab) = \varphi(aK) \cdot \varphi(bK),$$

所以φ是G/K到G的同态映射．因而 $G/Ker\phi \cong G$.

6.（10）证明：p是奇素数，$p-1$的所有不同的素因数是$q_1, q_{2,} \cdots q_s$，那么g为模p原根的充要条件是 $g^{(p-1)/q_j} \neq 1(\mathrm{mod}\, p), \quad j = 1,2,\cdots s$。

证明：必要性由原根的定义显然成立。下面证明充分性，假设g不是模p原根，则存在$d \mid p-1$使得$g^d = 1(\mathrm{mod}\, p)$成立，且$d \neq p-1$，所以存在$q_i \mid \frac{p-1}{d}$也就是$d \mid \frac{p-1}{q_i}$，由此可得$g^{(p-1)/q_i} \neq 1(\mathrm{mod}\, p)$, 此与题设矛盾，故原命题成立。