2005-2006 学年第二学期数论与代数结构考试题答案

1. （20 分） 设 m,n 是正整数．证明

$$(2^m-1,\ 2^n-1)=2^{(m,n)}-1.$$

证明：不妨设 $m\ge n$．由带余除法得

$$m=q_1n+r_1,\qquad 0\le r_1<n.$$

我们有

$$2^m-1=2^{q_1n+r_1}-2^{r_1}+2^{r_1}-1=2^{r_1}(2^{q_1n}-1)+2^{r_1}-1.$$

由此及 $2^n-1\mid 2^{q_1n}-1$ 得

$$(2^m-1,\ 2^n-1)=(2^{r_1}-1,\ 2^n-1).$$

注意到 $r_1=0$，则 $(m,n)=n$，结论成立．若 $r_1>0$，则继续对 $(2^{r_1}-1,\ 2^n-1)$ 作同样的讨论，由辗转相除法知，结论成立．

2．(20) 若 a,b 为不全为零的整数，设计一个效率尽可能高的算法求这两个数的最大公因数 (a,b)，并估计其复杂度。

解：应用带余除法得到的下面 k 个等式：

$a=q_0b+r_0$，　　$0<r_0<|b|$，

$b=q_1r_0+r_1$，　　$0<r_1<r_0$，

$r_0=q_2r_1+r_2$，　　$0<r_2<r_1$，

… … … …　　… … … …

$r_{k-5}=q_{k-3}r_{k-4}+r_{k-3}$，　　$0<r_{k-3}<r_{k-4}$，

$r_{k-4}=q_{k-2}r_{k-3}+r_{k-2}$，　　$0<r_{k-2}<r_{k-3}$ ，

$r_{k-3}=q_{k-1}r_{k-2}$．

容易看出：$r_{k-2}=(a,b)$，并且满足 $k\le\log_2 a$，每一步的复杂度为 $(\log_2 a)^2$ ，

所以该算法求两个数的最大公因数复杂度为 $(\log_2 a)^3$。

3.（20）设 $n = p_1 p_2 p_3$， 其中 $p_i, i = 1,2,3$ 是互不相等素数，令

$$J^{+1} = \left\{ x \mid x \in Z_n^*, \left(\frac{x}{n}\right) = 1 \right\}; \qquad J^{-1} = \left\{ x \mid x \in Z_n^*, \left(\frac{x}{n}\right) = -1 \right\},$$

这里 $\left(\frac{x}{n}\right)$ 表示 Jacobi 符号， Z_n^* 表示模 n 的既约剩余系。

(i) 证明: $|J^{+1}| = |J^{-1}|$, 这里 $|J^{+1}|, |J^{-1}|$ 表示集合 J^{+1}, J^{-1} 元素的个数；

(ii) 计算在 $x \in J^{+1}$ 的条件下， x 是模 n 的二次剩余的概率；

（i）解： $\left(\frac{x}{n}\right) = 1$；当且仅当 $\left(\frac{x}{p_1}\right), \left(\frac{x}{p_2}\right), \left(\frac{x}{p_3}\right)$ 都取正号或者其中两个取负号另外一个取正号； $\left(\frac{x}{n}\right) = -1$；当且仅当 $\left(\frac{x}{p_1}\right), \left(\frac{x}{p_2}\right), \left(\frac{x}{p_3}\right)$ 都取负号或者其中两个取正号另外一个取负号，又因为 $\left(\frac{x}{p_1}\right), \left(\frac{x}{p_2}\right), \left(\frac{x}{p_3}\right)$ 取正负号的概率是相等的，所以 $|J^{+1}| = |J^{-1}|$。

（ii）解：$x \in J^{+1}$ 并且 x 是模 n 的二次剩余当且仅当 $\left(\frac{x}{p_1}\right), \left(\frac{x}{p_2}\right), \left(\frac{x}{p_3}\right)$ 都取正号，所以 $x \in J^{+1}$ 的条件下， x 是模 n 的二次剩余的概率是 $\frac{1}{4}$。

4.（20）设 p 是一个素数，证明：Z_p^* 是一个乘法循环群，对于任意的 $q \mid p-1$ 求一个元素 $x \in Z_p^*$ 并且 x 的阶是 q。

证明 ：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 $\delta_p(i) \mid \delta, \quad i = 1, 2, \cdots, p-1.$ 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. 所

以可得Z_p^*是一个乘法循环群。容易看出$g^{(p-1)/q}$的阶就是q。

5.（20）设f是G到G'的满同态，H'是G'的不变子群，

$$H = f^{-1}(H') = \{a \mid a \in G,\ f(a) \in H'\},$$

证明：　H是G的不变子群，且$G/H \cong G'/H'$。

证明：　由同态基本定理，$G' \sim G'/H'$，ϕ是自然同态，又因为$f: G \sim G'$，故$\varphi: G \sim G' \sim G'/H'$是$G$到$G'/H'$的满同态．若能证明$\ker\varphi = H$，则由同态基本定理就可推出所要结论．

$\forall a \in G$，　$\varphi(a) = (\phi \circ f)(a) = \phi(f(a)) = f(a)H'$，　设　$a \in f^{-1}(H')$，　则$f(a) \in H' \Rightarrow f(a)H' = H' \Rightarrow \varphi(a) = H'$，即$a \in \ker\varphi$，亦即

$f^{-1}(H') \subseteq \ker\varphi$．

反之，设$a \in \ker\varphi$，则

$$\varphi(a) = f(a)H' = H' \Rightarrow f(a) \in H' \Rightarrow a \in f^{-1}(H'),$$

即$f^{-1}(H') \supseteq \ker\varphi$，从而$\ker\varphi = H$为$G$的不变子群．由同态基本定理得证$G/H \cong G'/H'$．