2005-2006 学年第二学期数论与代数结构考试题

1．(20） 设 p,q 是两个不同的素数。证明

$$(2^p-1, 2^q-1)=1.$$

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。

3.（20）设 $n=p_1p_2p_3$， 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。

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。

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 $G/H\cong G'/H'$.