信安数基第四次作业-冯东子-2022302181189

六、模47的原根有多个，求所有模47的原根.

解：共有$\varphi(\varphi(47))=\varphi(46)=22$个原根.

$46=2\times23$，即46有两个质因数2，23，

又$ord_{47}^{2}=23$，$ord_{47}^{-1}=2$，

故$ord_{47}^{-2}=46$，故-2是模47的一个原根，

当$(d,p-1)$时，d遍历模$p-1=46$的简化剩余系：

1，3，5，7，9，11，13，15，17，19，21，25，27，29，31，33，35，37，39，41，43，45.

$(-2)^1\equiv -2\equiv 45$，$(-2)^3=-8\equiv 39$，$(-2)^5=-32\equiv 15$，$(-2)^7=-128\equiv 13$

$(-2)^9\equiv 5$ $(-2)^{11}\equiv 20$，$(-2)^{13}\equiv 33$，$(-2)^{15}\equiv 38$ $(-2)^{17}\equiv 11$

$(-2)^{19}\equiv 44$ $(-2)^{21}\equiv 35$，$(-2)^{25}\equiv 43$，$(-2)^{27}\equiv 31$，$(-2)^{29}\equiv 30$

$(-2)^{31}\equiv 26$，$(-2)^{33}\equiv 10$，$(-2)^{35}\equiv 40$，$(-2)^{37}\equiv 19$ $(-2)^{39}\equiv 29$

$(-2)^{41}\equiv 22$，$(-2)^{43}\equiv 41$，$(-2)^{45}\equiv 23$

10. 设p，$\frac{p-1}{2}$个质数，设a是与p互素的正整数，如果$a^2\not\equiv 1$，$a^{\frac{p-1}{2}}\not\equiv 1 \pmod p$，则$a$是模$p$的原根.

证明：$\because a^2\not\equiv 1$且$a^{\frac{p-1}{2}}\not\equiv 1 \pmod p$，$(a,p)=1$

又$p-1$的因子有$1,2,\frac{p-1}{2},p-1$

$\therefore a^{p-1}\equiv 1 \pmod p$ 且 $\varphi(p)=p-1$

$\therefore a$为模p的原根

(7) $x^{22} \equiv 29 \pmod{41}$ $\varphi(41)=40$

$\because (22, 40)=2$, $\text{ind}\, 29 = 7$, $(7, 2)=1$. 故无解