HW3 参考答案

Ch2

30(1)

> $1^{p-1}+2^{p-1}+...+(p-1)^{p-1}\equiv -1(modp)$

- 由欧拉定理可得$a^{p-1}\equiv 1(modp)$对a = 1,...,p-1成立。故$1^{p-1}+2^{p-1}+...+(p-1)^{p-1}\equiv p-1\equiv -1(modp)$成立。

35

> 若n为偶完全数，n>6，证明$n\equiv 1(mod9)$

根据定理2.15， n=$2^{p-1}(2^p-1)$其中p和2^p-1都是素数。
由于n>6,则p>=3.

由于p是素数，分三种情况讨论。

1. p=3

   则n=28，满足条件。

2. p=3k+1,其中k为偶数

   则$n=2^{3k}(2^{3k+1}-1)=8^k(2*8^k-1)$

   则$n\equiv(-1)^k(2*(-1)^k-1)(mod9)$

   由于k是偶数，故满足条件。

3. p=3k+2,其中k为奇数

   则$n=2^{3k+1}(2^{3k+2}-1)=2*8^k(4*8^k-1)$

   则$n\equiv 2*(-1)^k(4*(-1)^k-1)\equiv 8+2(mod9)$

   故满足条件。

37

> 求2，4，7，8，11，13，14模15的阶是多少?

由于$\phi(15)=8$,故阶只可能为1，2，4，8.

易得阶依次为4，2，4，4，2，4，2.

38

(1)

k1	k2	k3	k4	k5	k6	k7
0	1	5	2	22	6	12
k8	k9	k10	k11	k12	k13	k14
3	10	23	25	7	18	13
k15	k16	k17	k18	k19	k20	k21
27	4	21	11	9	24	17
k22	k23	k24	k25	k26	k27	k28
26	20	8	16	19	15	14

(2)

由于29的最小原根为2。

故$ind_2 9 + ind_2 x \equiv ind_2 2 (mod 28)$

查表得$ind_2 9 = 10, ind_2 2 = 1$

故$ind_2 x \equiv -9 \equiv 19 (mod 28)$

查表得$x \equiv 26 (mod 29)$

(3)

由于29的最小原根为2。

故$9 * ind_2 x = ind_2 2 (mod 28)$

查表得

$9 * ind_2 x \equiv 1 (mod 28)$

$ind_2 x \equiv 25 (mod 28)$

$x \equiv 11 (mod 29)$

40

由书中表得2是37的最小原根。

则{2^0,2^1,...,$2^{\phi(37)-1}$}构成了模37的缩系，每个与37互素的a均与且仅与某个2^i模37同余。模37的原根都在上述集合中。

要使2^i也是37的原根，则i需要与36互素。

所以$i \in \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$

故37的原根集合为{2,32,17,13,15,18,35,5,20,24,22,19}