1. 设$m,n\in \mathrm{N}^+,(n,\varphi(m))=1$,求证：当$a$遍历模$m$的简化剩余系时，$a^n$也遍历模$m$的简化剩余系.

反证法.

假设模m的简化剩余系中,两个不同的元素为a_1,a_2,且有$a_1^n\equiv a_2^n(mod\quad m)$

而模m的简化剩余系$(Z/mZ)*$是一个交换乘法群,a_1,a_2的逆元a_1^{-1}、a_2^{-1}也在$(Z/mZ)*$中(或者

通过$ax\equiv b(modm)$有解的条件$(a,m)|b$来证明

因此,$(a_1^{-1})^n\equiv(a_2^{-1})^n\quad(mod\quad m)$

而：$a_1^n*(a_1^{-1})^n\equiv 1(mod\quad m)$,且　$(a_1^{-1})^n\equiv(a_2^{-1})^n\quad(mod\quad m)$

所以,$a_1^n*(a_2^{-1})^n\equiv(a_1a_2^{-1})^n\equiv 1(mod\quad m)$

所以对于数$a_1a_2^{-1}$有其指数$ord_m(a_1a_2^{-1})|n$,而$a_1a_2^{-1}$显然与m互素,根据欧拉定理有$(a_1a_2^{-1})^{\varphi(m)}\equiv 1(mod\quad m)$

因此$ord_m(a_1a_2^{-1})|\varphi(m)$

根据题设,$(n,\varphi(m))=1$,而$ord_m(a_1a_2^{-1})$又是两者的公因数,则$ord_m(a_1a_2^{-1})$只能为1

因此$(a_1a_2^{-1})\equiv 1(mod\quad m)$,对于$a_1$,其逆元解应该是唯一存在的,因此$a_1^{-1}\equiv a_2^{-1},a_1\equiv a_2$,这是与假设矛盾的.

因此,证明完备.

2. 求解同余方程$x^8\equiv 38\ (\mathrm{mod}\,11)$.

注意到11是一个素数,有$(38,11)=1$,于是查原根表,模11有一个原根$g=2$

将方程指标化,得到$8ind(x)\equiv ind(38)(mod\quad \varphi(m)=10)$

而$38\equiv 5(mod\quad 11)$,因此$ind(38)=ind(5)=r$,有$2^r\equiv 5(mod\quad 11)$,所以$r=4$

$8ind(x)\equiv 4(mod\quad 10)$

解得$ind(x)\equiv 3(mod\quad 5)\equiv 3,8(mod\quad 10)$

所以,$ind(x)\equiv 3,8(mod\quad 10)$

$x\equiv 2^{ind(x)}\equiv 2^3,2^8(mod\quad 11)$

也就是$x\equiv 8,3(mod\quad 11)$

3. 构造模23的指数表.

(1)指数表

$\varphi(23)=22$,因此模23的指数只可能是22的因数：$1,2,11,22$

对$0-22$依次代入这些因数次方即可

(2)指标表,23的原根$g=5$

十位\个位	0	1	2	3	4	5	6	7	8	9
0		22	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

4. 设p为奇素数，a，b为模p的两个原根，求证：$ord_p(ab)<\varphi(p)$.

欲求证$ord_p(ab) < \varphi(p)$，而本有$ord_p(ab)|\varphi(p)$，即证明(ab)不是模p的原根

反证法.

假设(ab)是模p的原根，$ord_p(ab) = \varphi(p)$，于是$C = \{(ab)^0, (ab), \ldots (ab)^{\varphi(p)-1}\}$构成了模$p$的简化剩余系

由$Wilson$定理，对于一个素数p，有$(p-1)! \equiv -1(mod \quad p)$，注意到：

C中的每个元素$c_i \equiv k(mod \quad p), k \in (0, p-1)$，不重不漏，因此有：

$$\prod_{i=0}^{\varphi(p)-1} c_i \equiv \prod_{i=1}^{p-1} i \equiv (p-1)!(mod \quad p)$$

由$Wilson$定理，$\prod_{i=0}^{\varphi(p)-1} c_i \equiv -1(mod \quad p)$

$\because a, b$是模p的原根，$\prod_{0 \le k \le \varphi(p)-1} a^k \equiv \prod_{0 \le k \le \varphi(p)-1} b^k \equiv -1(mod \quad p)$

而$\prod c_i$即$\prod (ab)^k \equiv (-1)(-1) = 1(mod \quad p)$

与假设推出的结论矛盾，故原命题成立

5. 设$(a,2)=1, l \ge 3$，证明$a^{2^{l-2}} \equiv 1 \pmod{2^l}$.

证明(数学归纳法)：

由$(a, 2) = 1$可知，a必为奇数，$a \equiv 1(mod \quad 2)$，设$a = 2k+1 \quad k \in Z$

当$l = 3$时，$a^{2^{l-2}} = a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$，$k$和$k+1$中必有一数是偶数$2n$

因此，原式 $= 4k(k+1) + 1 \equiv 1(mod \quad 8 = 2^l = 2^3)$，成立

当$l > 3$时，假设$l = n \ge 3$时，命题成立，也就是有：

$a^{2^{n-2}} \equiv 1(mod \quad 2^n)$

可以设$a^{2^{n-2}} = k \cdot 2^n + 1, k \in Z$

那么，当$l = n+1$时，$a^{2^{l-2}} = a^{2^{n-1}} = a^{2^{n-2}+2^{n-2}} = a^{2^{n-2}} \cdot a^{2^{n-2}} = (k \cdot 2^n + 1)^2 = k^2 2^{2n} + 2k \cdot 2^n + 1$

欲证：$a^{2^{(n+1)-2}} \equiv 2^{n+1}(mod \quad 2^{n+1})$

可以发现，$2^n | 2^{n+1}$，因此$a^{2^{(n+1)-2}} = k^2 2^{2n} + 2k \cdot 2^n + 1 \equiv 1(mod 2^{n+1})$

归纳证明成立.

6. 求解同余方程$6 \cdot 8^x \equiv 9 \pmod{13}$.

注意到13是一个素数，查原根表得到，13的一个原根$g = 2$

将原方程指标化为：$ind_g 6 + x \cdot ind_g 8 \equiv ind_g 9(mod \quad \varphi(13) = 12)$

计算指标表

$ind_g 6 = 5$

$ind_g 8 = 3$

$ind_g 9 = 8$

因此原式可以写成：$5 + 3x \equiv 8(mod \quad 12)$

$3x \equiv 3(mod \quad 12)$

解得$x \equiv 1(mod \quad 4)$

因此$x \equiv 1, 5, 9(mod \quad 13)$