1. 设m=737，$a=635$，利用广义欧几里得除法，求整数a',$1\le a'<m$，使得 $aa'\equiv 1 \pmod m$.

欲求$aa'=1(mod \quad m)$的a';
即$a'a+km=1$,求a',利用广义欧几里得除法可得到$sm+ta=(m,a)$
$737=1*635+102$
$635=6*102+23$
$102=4*23+10$
$23=2*10+3$
$10=3*3+1$
$3=3*1+0$
一共是$n+2=6$项,$n=4,(737,635)=1$

于是$q_0=1,q_1=6....q_n=3,q_{n+1}=1$
$s_{-2}=1,t_{-2}=0$
$s_{-1}=0,t_{-1}=1$
所以,$s_0=-q_0s_{-1}+s_{-2}=1,t_0=-q_0t_{-1}+t_{-2}=-1$
进而,$s_4=193,t_4=-224$
所以$193*737-224*635=1$,
$-224*a+193*737=1(mod\,737)$
$a'=-224$

2. 证明：如果p和q是不同的素数，则$p^{q-1}+q^{p-1}\equiv 1 \pmod{pq}$.

$$\text{由已知},(p,q)=1,\varphi(p)=p-1,\varphi(q)=q-1$$
$$\text{由欧拉定理},p^{\varphi(q)}\equiv 1(mod\,q),\text{即}\,p^{q-1}\equiv 1(mod\,q),\text{对}\,q\text{同理}$$
$$\text{因此},p^{q-1}+q^{p-1}\equiv 1(mod\,p)$$
$$p^{q-1}+q^{p-1}\equiv 1(mod\,q)$$
$$\text{而}\,[p,q]=\frac{pq}{(p,q)}=pq;\text{所以原式成立}$$

3. 证明：m是大于1的正整数，a是与m互素的整数，且$(a-1,m)=1$，那么$1+a+a^2+\cdots+a^{\varphi(m)-1}\equiv 0 \pmod m$.

$$(a,m)=1,\text{由欧拉定理},a^{\varphi(m)}\equiv 1(mod\,m)$$
$$\text{因而}\,a^{\varphi(m)}-1=(a-1)(1+a+a^2+...+a^{\varphi(m)-1})\equiv 0(mod\,m)$$
$$\text{所以}\,m|a^{\varphi(m)}-1 \qquad m|(a-1)(1+a+a^2+...+a^{\varphi(m)-1})$$
$$\text{注意到},(a-1,m)=1$$
$$\text{所以},\text{根据定理},m|(1+a+a^2+...+a^{\varphi(m)-1})$$
简要说明：
$$\text{由于}\,m|(a-1)(1+a+a^2+...+a^{\varphi(m)-1}),$$
$$(m,(a-1)(1+a+a^2+...+a^{\varphi(m)-1}))=m, \qquad (m,a-1)=1,\text{所以}$$
$$(m,(a-1)(1+a+a^2+...+a^{\varphi(m)-1}))=(m,(1+a+a^2+...+a^{\varphi(m)-1}))$$
$$\text{所以},m|(1+a+a^2+...+a^{\varphi(m)-1})$$
原式成立

4. 证明：设p为奇素数，$a_0, a_1, \ldots, a_{p\text{-}1}; b_0, b_1, \ldots, b_{p\text{-}1}$为模$p$的两组完全剩余系求证：$a_0b_0, a_1b_1, \ldots, a_{p\text{-}1}b_{p\text{-}1}$不是模$p$的完全剩余系.

反证法; 假设$a_0b_0, a_1b_1 \ldots a_{p-1}b_{p-1}$是模$p$的完全剩余系

因此, 其中只有一个数模p为0, 设该数为a_0b_0

由于p是奇素数, 除去a_0b_0后, $a_1b_1, \ldots., a_{p-1}b_{p-1}$就是模$p$的简化剩余系

那么$a_1b_1, \ldots., a_{p-1}b_{p-1}$和$1, 2..., p-1$是等价的, 由$Willson$定理

$$\Pi a_ib_i = (p-1)! \equiv -1(mod\, m)$$

由题干, $a_1 \ldots a_{p-1}$和$b_1 \ldots b_{p-1}$均是模p的简化剩余系

$$\Pi a_i \equiv -1(mod\, m)$$

$$\Pi b_i \equiv -1(mod\, m)$$

而根据假设$\Pi a_ib_i = (p-1)! \equiv -1(mod\, m)$

与题干信息矛盾, 假设错误， 不是模p的完全剩余系

5. 求一次同余方程$6x \equiv 3\ (\mathrm{mod}\, 9)$的所有解.

化简同余方程, $(6, 3, 9) = 3$

原方程等价为$2x \equiv 1(mod\, 3)$

步骤一：验证是否有解

$(2, 3) = 1|1$; 即原式的$(6, 9) = 3|3$; 因此原式有解

步骤二：求解简单特解

$(a, m) = (6, 9) = 3$, 方程左右除以3就是$2x \equiv 1(mod3)$

解得$x_0 = 2(mod3)$

步骤三：根据特解求得原解

$$x \equiv x_0 + t\frac{m}{(a, m)} = 2 + 3t(mod\, 9)$$

$$x \equiv 2, 5, 8(mod\, 9)$$