No: C3

Date:

T1. 设素数 $p \nmid a$, $k \geq 1$. 证明: $n^2 \equiv an \bmod p^k \Leftrightarrow n \equiv 0 \bmod p^k$ 或 $n \equiv a \bmod p^k$.

证明: $\Rightarrow$ 必要性: $n^2 \equiv an \bmod p^k \Leftrightarrow p^k \mid n^2 - an = n(n-a)$

则可能的所有情形有 ① $p^k \mid n$, 即 $n \equiv 0 \bmod p^k$; ② $p^k \mid n-a$, 即 $n \equiv a \bmod p^k$; ③ $\exists i, j \in \mathbb{Z}$, $1 \leq i, j < p^k$, 使得 $p^i \mid n$, $p^j \mid n-a$, 其中 $i+j \geq k$.

下面证明③情形不存在:

设 $p^m = \min\{p^i, p^j\}$, 则 $p^m \mid n$, $p^m \mid n-a$, 由此得 $p^m \mid a$, 与 $p \nmid a$ 矛盾! 故③情形不可能成立。

由 $n^2 \equiv an \bmod p^k$ 可得 $n \equiv 0 \bmod p^k$ 或 $n \equiv a \bmod p^k$

$\Leftarrow$ 充分性: $n \equiv 0 \bmod p^k \Rightarrow p^k \mid n \Rightarrow p^k \mid n(n-a) \Leftrightarrow n^2 \equiv an \bmod p^k$

$n \equiv a \bmod p^k \Rightarrow p^k \mid n-a \Rightarrow p^k \mid n(n-a) \Leftrightarrow n^2 \equiv an \bmod p^k$

综上所述, $n^2 \equiv an \bmod p^k$ 成立的充要条件为 $n \equiv 0 \bmod p^k$ 或 $n \equiv a \bmod p^k$.

T2. 解：(1) $10 = 2\times 5$，$2^{400} \equiv 0 \bmod 2$，又 $(2,5)=1$，$\varphi(5)=4$

由 Euler 定理得 $2^4 \equiv 1 \bmod 5$，故 $2^{400} = (2^4)^{100} \equiv 1 \bmod 5$

即已知 $\begin{cases} 2^{400} \equiv 0 \bmod 2 \\ 2^{400} \equiv 1 \bmod 5 \end{cases}$，在模5剩余类中满足是偶数且 $\bmod 5 = 1$

的（且个位数）有且仅有 6（或利用中国剩余定理求解）.

故 $2^{400} \equiv 6 \bmod 10$.

（也可利用 $\varphi(\overset{5}{\text{而}}) = 4$ 求出 $2^n \bmod 10$ 的周期性变化，其中 $T=4$）

(3) 因为 $(9,10)=1$，$\varphi(10)=4$，由 Euler 定理，$9^4 \equiv 1 \bmod 10$，故

$9^8 \equiv 1 \bmod 10$，$9^9 \equiv 9 \bmod 10$，$\overset{\varphi(100)=40}{\vee}$ 故有

$9^{99} \equiv 9^9 \equiv -11 \equiv 89 \bmod 100$，末两位为 89；

$9^{999} \equiv 9^{89} \equiv 9^9 \equiv 89 \bmod 100$，末两位为 89.

T5. 证明：当 $m>2$ 时，$0^2, 1^2, 2^2, \cdots, (m-1)^2$ 一定不是模 m 的完全剩余系。

证明：$m>2$ 时，$m-1>1$，$(m-1)^2 = m^2-2m+1 = m(m-2)+1$

$m \mid m(m-2)$，故 $(m-1)^2 \equiv 1 \bmod m$，不满足任意两个数模 m 不同余。

故 $0^2, 1^2, 2^2, \cdots, (m-1)^2$ 一定不是模 m 的完全剩余系。

T6. 证明：$(m,n)=1$，由 Euler 定理得 $m^{\varphi(n)} \equiv 1 \bmod n$，

$n^{\varphi(m)} \equiv 1 \bmod m$。由于 $n^{\varphi(m)} \equiv 0 \bmod n$，故 $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod n$

同理 $m^{\varphi(n)} \equiv 0 \bmod m$，$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod m$，所以得出

$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod mn$。证毕。

T8. 证明：(1) $(p-1)! = [2\cdot(p-2)]\cdot[4\cdot(p-4)]\cdot\cdots\cdot[(p-1)\cdot(p-(p-1))]$

$$\equiv (-1)^{\frac{p-1}{2}} \cdot 2^2 \cdot 4^2 \cdot \cdots \cdot (p-1)^2 \bmod p$$

又由 Wilson 定理得 $(p-1)! \equiv -1 \bmod p$，所以

$2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \bmod p \equiv (-1)^{\frac{p+1}{2}} \bmod p$，证毕

No:

Date:

T5. (不确定，尝试) 证明：(1) 设 $S_1=\{-r_s,\cdots,-r_2,-r_1,r_1,r_2,\cdots,r_s\}$，$S_2=\{r_1,r_2,\cdots,r_s,(m-r_s),(m-r_{s-1}),\cdots,(m-r_2),(m-r_1)\}$. 要证明 S_1、S_2 是 m 的简化剩余系，需证 ① S_1、S_2 包含所有小于 m 且与 m 互素的整数；② S_1、S_2 中元素两两模 m 不同余，而 S_1、S_2 在模 m 运算下等价，只需证 S_2 即

① : 设 a 是小于 m 与 m 互素的整数，若 $0<a<\frac{m}{2}$，则为 $r_1,\cdots r_s$，必在 S_2 中；若 $\frac{m}{2}<a<m$，则 $0<m-a<\frac{m}{2}$，由于 $(a,m)=1$，得 $(m-a,m)=1$，所以 $m-a\in S_2$，所以 S_2 包含所有小于 m 与 m 互素的数.

② : 对于 $1\le i,j\le s, i\ne j$. 易知 r_i 与 r_j 模 m 不同余，$m-r_i$ 与 $m-r_j$ 模 m 等价于 $-r_i$、$-r_j$ 模 m 也不同余. 考虑 r_i 与 $m-r_j$，假设 $r_i\equiv m-r_j \bmod m$，则 $m\mid r_i-(m-r_j)=r_i+r_j-m$，即 $m\mid r_i+r_j$. 又 $0<r_{i,j}<\frac{m}{2}$ 故 $0<r_i+r_j<m$，$m\mid r_i+r_j$ 不成立，矛盾！故 r_i 与 $m-r_j$ 模 m 不同余.

综上 ①② 得 S_1、S_2 为 m 的简化剩余系。

(2) 由以上证明，当 $m\ge 3$ 时，对 $\forall r_i\in S_1$，必有对应 $m-r_i\in S_1$，S_1 元素个数为偶数，即 $2\mid\varphi(m)$.

Date:

五.证明：(1) $q \mid a^p+1 \Rightarrow a^p \equiv -1 \bmod q \Rightarrow a^{2p} \equiv 1 \bmod q$

故 a 模 q 的阶（离散的知识？）d 是 $2p$ 的因子. 显然, $d \neq 1$, $d \neq q$.

若 $d=2$, 则 $a^2 \equiv 1 \bmod q$, 又 $a^p \equiv -1 \bmod q$, 故有 $a \equiv -1 \bmod q$.

即 $q \mid a+1$; 若 $d=2p$, ~~则 $a^{2p} \equiv 1 \bmod q$~~ 由同余运算以及 q 的剩余系构成的群阶为 $q-1$, $d \mid q-1$, 即 $2p \mid q-1$, 得 $q \equiv 1 \bmod 2p$.

综上, q 为 $a+1$ 的因子或 $q \equiv 1 \bmod 2p$.

(2)（没想很明白，太难了qwq）