No:
Date:

C5

T1. 证明：(1) $\prod_{1\le k\le p-1} k = \prod_{1\le k\le \frac{p-1}{2}} k(p-k) = (-1)^{\frac{p-1}{2}} \prod_{1\le k\le \frac{p-1}{2}} k^2 \mod p$

由 wilson 定理，$(p-1)! \equiv -1 \mod p$，故

$\prod_{1\le k\le p-1} k = (-1)^{\frac{p-1}{2}} \prod_{1\le k\le \frac{p-1}{2}} k^2 \quad , \equiv -1 \mod p$

若 $a_1, \cdots, a_{\frac{p-1}{2}}$ 为模 p 的全部二次剩余，则 $\prod_{1\le i\le \frac{p-1}{2}} a_i \equiv (-1)^{\frac{p+1}{2}} \mod p$

(二次剩余模 p 取遍 $1^2, 2^2, \cdots, (\frac{p-1}{2})^2$.)

(2) 设 $b_1, \cdots b_{\frac{p-1}{2}}$ 为模 p 的全部二次非剩余，由 $\prod_{1\le i\le \frac{p-1}{2}} a_i \prod_{1\le j\le \frac{p-1}{2}} b_j \equiv \prod_{1\le k\le p-1} k \pmod p$

得 $\prod_{1\le j\le \frac{p-1}{2}} b_j \equiv (-1)^{\frac{p+1}{2}} \div (-1) \equiv (-1)^{\frac{p-1}{2}} \mod p$.

T2. 解：(1) $\left(\frac{13}{47}\right) = (-1)^{\frac{47-1}{2}\cdot\frac{13-1}{2}} \left(\frac{47}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{-5}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{5}{13}\right)$

47、13均为素数，故

$= (-1)^{\frac{13-1}{2}} \cdot (-1)^{\frac{13-1}{2}\cdot\frac{5-1}{2}} \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right)$

$= 3^{\frac{5-1}{2}} \mod 5 \equiv -1 \mod 5$

故 $\left(\frac{13}{47}\right) = -1$

T3. 解：(1) $\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = (-1)^{p-1} \left(\frac{p}{3}\right)$，$p$ 为大于2的奇素数，

故 $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$，将 $p = 3, 5, 7, 11, \cdots$ 代入，可知 $p = 7, 13, 19 \cdots$ 即

$p = 6k+1$，$k \in N$ 时 $\left(\frac{p}{3}\right) = 1$，故 $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$ 当且仅当 $p \equiv 1 \mod 6$.

T4. 证明：充分性 ($\Leftarrow$)：设 $q = 2p+1$，由 $2^p \equiv 1 \mod (2p+1)$ 得

$2^{2p} \equiv 1 \mod (2p+1)$，即 $2^{q-1} \equiv 1 \mod q$，且 $(2, q) = 1$，故

$\varphi(q) = q-1$，$q = 2p+1$ 是素数.

必要性 ($\Rightarrow$)：若 $q = 2p+1$ 为素数，由 $p \equiv 3 \mod 4$ 可得 $q \equiv -1 \mod 8$

No:

Date:

令 $q=8k-1, k\in Z_+$，则 $\left(\frac{2}{q}\right)=(-1)^{\frac{q^2-1}{8}}=(-1)^{8k^2-2k}=1$，故 2 是模 q 的二次剩余，得 $2^{\frac{q-1}{2}}=2^p\equiv 1 \mod (2p+1)$.

综上，题设条件下 $2p+1$ 为素数 $\Leftrightarrow 2^p\equiv 1 \mod (2p+1)$

T6.(1) 解：227 是素数，题设转化为求解 $\left(\frac{7}{227}\right)$，7 也为素数，故

$\left(\frac{7}{227}\right)=(-1)^{\frac{7-1}{2}\cdot\frac{227-1}{2}}\left(\frac{227}{7}\right)=(-1)\cdot\left(\frac{3}{7}\right)$

$3^{\frac{7-1}{2}}=27\equiv -1 \mod 7$，故 $\left(\frac{7}{227}\right)=(-1)\times(-1)=1$，故

$x^2\equiv 7 \mod 227$ 有解.