No.

Date. / /

习题1：∵ $x^2 \equiv (23-x)^2 \pmod{23}$ ∴ 计算1至11

$1^2 \equiv 1 \pmod{23}$，$2^2 \equiv 4 \pmod{23}$，$3^2 \equiv 9 \pmod{23}$，$4^2 \equiv 16 \pmod{23}$

$5^2 \equiv 2 \pmod{23}$，$6^2 \equiv 13 \pmod{23}$，$7^2 \equiv 3 \pmod{23}$，$8^2 \equiv 18 \pmod{23}$

$9^2 \equiv 12 \pmod{23}$，$10^2 \equiv 8 \pmod{23}$，$11^2 \equiv 6 \pmod{23}$

∴ 二次剩余：1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18

非二次剩余：5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22

习题2：(1) $x^2 \equiv 2 \pmod{31}$

∵ 31是素数且 $(\frac{2}{31}) \equiv (-1)^{\frac{31^2-1}{8}} = (-1)^{120} = 1$

∴ 有2个解

(2) $x^2 \equiv 3 \pmod{31}$

$(\frac{3}{31}) = (-1)^{\frac{(3-1)(31-1)}{4}} (\frac{31}{3}) = (-1)^{\frac{2\times30}{4}} (\frac{1}{3}) = -1$

∴ 无解

(3) $x^2 \equiv 19 \pmod{30}$，$30 = 2\times3\times5$

$(\frac{19}{2}) = (\frac{1}{2}) = 1$，$(\frac{19}{3}) = (\frac{1}{3}) = 1$，$(\frac{19}{5}) = (\frac{4}{5}) = 1$

但 $x^2 \equiv 1 \pmod{2}$ 只有1个解，$1\times2\times2 = 4$

∴ 共4个解

习题3：$7\times1 \equiv 7 \pmod{19}$，$7\times2 \equiv 14 \pmod{19}$，$7\times3 \equiv 2 \pmod{19}$，$7\times4 \equiv 9 \pmod{19}$

$7\times5 \equiv 16 \pmod{19}$，$7\times6 \equiv 4 \pmod{19}$，$7\times7 \equiv 11 \pmod{19}$，$7\times8 \equiv 18 \pmod{19}$

$7\times9 \equiv 6 \pmod{19}$

大于 $\frac{19}{2} = 9$ 的有4个

∴ $(\frac{7}{19}) = (-1)^4 = 1$

No.

Date. / /

习题4：$\because \left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{(p-1)^2(p+1)}{16}}$

① $\left(\frac{-1}{p}\right)=1$ 且 $\left(\frac{2}{p}\right)=1$，则 $p\equiv 1\pmod 8$

② $\left(\frac{-1}{p}\right)=-1$ 且 $\left(\frac{2}{p}\right)=-1$，则 $p\equiv 3\pmod 8$

③ $\left(\frac{-1}{p}\right)=1$ 且 $\left(\frac{2}{p}\right)=-1$，则 $p\equiv 5\pmod 8$

④ $\left(\frac{-1}{p}\right)=-1$ 且 $\left(\frac{2}{p}\right)=1$，则 $p\equiv 7\pmod 8$

$\therefore$ 二次剩余：$p\equiv 1\pmod 8$ 或 $p\equiv 3\pmod 8$

非二次剩余：$p\equiv 5\pmod 8$ 或 $p\equiv 7\pmod 8$

习题5：

① $\left(\frac{17}{79}\right)=\left(\frac{11}{17}\right)\times\left(\frac{17}{79}\right)$

$\left(\frac{17}{79}\right)=\left(\frac{8}{79}\right)=\left(\frac{2}{79}\right)^3=(-1)^{3\times\frac{79^2-1}{8}}=1$

$\left(\frac{11}{17}\right)=\left(\frac{6}{11}\right)=\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)=(-1)^{\frac{11^2-1}{8}}(-1)^{\frac{(3-1)(11-1)}{4}}\left(\frac{11}{3}\right)=\left(\frac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=-1$

$\therefore\left(\frac{17}{79}\right)=1\times(-1)=-1$

② $\left(\frac{610}{987}\right)$，$610=2\times5\times61$，$987=3\times7\times47$

$\therefore$ 原式 $=\left(\frac{2}{3}\right)\left(\frac{2}{7}\right)\left(\frac{2}{47}\right)\left(\frac{5}{3}\right)\left(\frac{5}{7}\right)\left(\frac{5}{47}\right)\left(\frac{61}{3}\right)\left(\frac{61}{7}\right)\left(\frac{61}{47}\right)$

$=\left(\frac{2}{3}\right)\left(\frac{2}{7}\right)\left(\frac{2}{47}\right)\left(\frac{2}{3}\right)\left(\frac{5}{7}\right)\left(\frac{5}{47}\right)\left(\frac{1}{3}\right)\left(\frac{5}{7}\right)\left(\frac{2}{47}\right)\left(\frac{7}{47}\right)$

$=-1$

习题6：$p=2^n+1$ 为素数 $\therefore\varphi(p)=p-1=2^n$，3模p的阶r整除 $\varphi(p)=2^n$

$\therefore r=2^k$，$0\le k\le n$

若 $k<n$，由费马小定理 $3^{p-1}=3^{2^n}\equiv 1\pmod p$，则 $(3^{2^{k-1}})^2\equiv 1\pmod p$

即 $(3^{2^{k-1}}-1)(3^{2^{k-1}}+1)\equiv 0\pmod p$

对于 $p=2^n+1>3$，若 $3^{2^{k-1}}\equiv 1\pmod p$ 与 $r=2^k$ 是3模p的阶矛盾；若 $3^{2^{k-1}}\equiv -1\pmod p$，两边平方得 $3^{2^k}\equiv 1\pmod p$，当 $k<n$ 可推出矛盾

$\therefore r=2^n=p-1$

$\therefore$ 3为p的一个原根