1. $2^{\frac{29-1}{2}} \equiv 2^{14} \pmod{29}$

$\equiv (2^7)^2 \cdot 2^2 \pmod{29}$

$\equiv 144 \pmod{29}$

$\equiv -1 \pmod{29}$

∴ 2是29的二次非剩余

2. 根据欧拉判别条件

$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

∵ p是奇素数

设 $p = 4n+1$

$(-1)^{\frac{p-1}{2}} = (-1)^{2n} = 1$

设 $p = 4n+3$

$(-1)^{\frac{p-1}{2}} = (-1)^{2n+1} = -1$

∴ 当 $p = 4n+1$ 时 $(\frac{-1}{p}) = 1$

即 $p \equiv 1 \pmod 4$ 时，-1是模p的充要条件.

3. $x^2 \equiv 191 \pmod{397}$

$(\frac{191}{397}) = (\frac{397}{191})(-1)^{198 \cdot 95}$

$= (\frac{15}{191})$

$= (-1)^{7 \cdot 95} \cdot (\frac{191}{15})$

$$= (-1)\left(\frac{11}{15}\right)$$

$$= (-1)\cdot(-1)^{5\cdot 7}\left(\frac{15}{11}\right)$$

$$= \left(\frac{4}{11}\right)$$

$$= \left(\frac{2^2}{11}\right) = 1 \quad \therefore \text{有解.}$$

4. $x^2 \equiv 2 \pmod{73}$

$$\left(\frac{2}{73}\right) = (-1)^{\frac{73^2-1}{8}} = 1$$

$\therefore$ 此方程有解

$x^2 - 2 \equiv 0 \pmod{73}$

$a = 8$

$y^2 \equiv a \pmod{73}$

$y^2 \equiv 81 \pmod{73}$

$y \equiv 9 \pmod{73}$ 或 $y \equiv -9 \pmod{73}$

$y = \sqrt{x}$

若 $2x \equiv 82 \pmod{73}$

$x \equiv 41 \pmod{73}$

若 $\sqrt{x} \equiv 64 \pmod{73}$

$x \equiv 32 \pmod{73}$

$\therefore$ 解为 $x \equiv 32, 41 \pmod{73}$

5. (1) $\left(\frac{17}{37}\right) = (-1)^{8\cdot 18}\cdot\left(\frac{37}{17}\right)$

$= \left(\frac{3}{17}\right)$

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

$= \left(\frac{2}{3}\right)$

$= -1$

(2) $\left(\frac{151}{373}\right) = (-1)^{75\cdot 186}\left(\frac{373}{151}\right)$

$= \left(\frac{71}{151}\right)$

$= (-1)^{35\cdot 75}\left(\frac{151}{71}\right)$

$= (-1)\left(\frac{9}{71}\right)$

$= (-1)\left(\frac{3^2}{71}\right)$

$= -1$

(3) $\left(\frac{191}{397}\right) = (-1)^{95\cdot 188}\left(\frac{397}{191}\right)$

$= \left(\frac{15}{191}\right)$

$= (-1)^{7\cdot 95}\cdot\left(\frac{191}{15}\right)$

$= (-1)\left(\frac{11}{15}\right)$

$= (-1)(-1)^{5\cdot 7}\left(\frac{15}{11}\right)$

$= \left(\frac{4}{11}\right)$

$= \left(\frac{2^2}{11}\right)$

$= 1$

6. (1) $\left(\frac{51}{71}\right) = (-1)^{25\cdot 35}\left(\frac{71}{51}\right)$

$= (-1)\left(\frac{20}{51}\right)$

$= (-1)\left(\frac{20}{3}\right)\left(\frac{20}{17}\right)$

$= (-1)\left(\frac{2}{3}\right)\left(\frac{3}{17}\right)$

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

$= (-1)^9 \cdot \left(\frac{2}{3}\right)\left(\frac{2}{3}\right)$

$= -1$

(2) $\left(\frac{313}{401}\right) = (-1)^{100\cdot 156}\left(\frac{401}{313}\right)$

$= \left(\frac{88}{313}\right)$

$= \left(\frac{2^2}{313}\right)\left(\frac{2}{313}\right)\left(\frac{11}{313}\right)$

$= (-1)^{\frac{313^2-1}{8}} \cdot (-1)^{5\cdot 156}\left(\frac{313}{11}\right)$

$= \left(\frac{5}{11}\right)$

$= (-1)^{2\cdot 5}\left(\frac{11}{5}\right)$

$= \left(\frac{1}{5}\right) = 1$

证明：

1. p是奇素数，且$(p,12)=1$

模12的缩系为 5，7，11，13

$(\frac{3}{5})=(-1)^{1\cdot 2}\cdot(\frac{5}{3})=-1$ $\quad 5\equiv 5 \pmod{12}$

$(\frac{3}{7})=(-1)^{1\cdot 3}\cdot(\frac{7}{3})=-1$ $\quad 7\equiv -5 \pmod{12}$

$(\frac{3}{11})=(-1)^{1\cdot 5}(\frac{11}{3})=1$ $\quad 11\equiv -1 \pmod{12}$

$(\frac{3}{13})=(-1)^{1\cdot 6}(\frac{13}{3})=1$ $\quad 13\equiv 1 \pmod{12}$

通过归纳法，可得

$x^2\equiv 3 \pmod p$ 有解条件为 $p\equiv \pm 1 \pmod{12}$

2. $\because b\mid p$

$\therefore$ 原式 $=(\frac{b}{p})+(\frac{2}{p})(\frac{b}{p})+\cdots+(\frac{p-1}{p})(\frac{b}{p})$

且p是奇素数，可得 $1\cdots p-1$ 是p的缩系

由定理5.1.2得，

模p的缩系中二次剩余与非二次剩余

两个数都为 $\frac{p-1}{2}$

即可知

原式 $= (-1)^{\frac{p-1}{2}}\left(\frac{b}{p}\right) + (1)^{\frac{p-1}{2}}\left(\frac{b}{p}\right)$

$= (-1+1)\left(\frac{b}{p}\right)$

$= 0$ 证毕.

3. ∵ p是奇素数

∴ $(3, p) = 1$

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

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

$= \left(\frac{p}{3}\right)$

模6加1余数为 5, 7

$\left(\frac{-3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ $\quad 5 \equiv -1 \pmod 6$

$\left(\frac{-3}{7}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$ $\quad 7 \equiv 1 \pmod 6$

通过归纳得知.

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 6 \\ -1 & p \equiv -1 \pmod 6 \end{cases}$$