$\left(\frac{5}{p}\right)$ via Gauss's Lemma $\Longrightarrow$ $\left(\frac{5}{p}\right) = \begin{cases} 1, & p \equiv \pm 1, \pm 9 \pmod{20} \\ -1, & p \equiv \pm 3, \pm 7 \pmod{20} \end{cases}$

$\{5, 10, 15, \ldots, 5\left(\frac{p-1}{2}\right)\}$

$5k < \frac{p}{2} \iff k < \frac{p}{10}$

$\frac{p-1}{2} - \left\lfloor \frac{p}{10} \right\rfloor$: $p \equiv 1, 3, 7, 9, 11, 13, 17, 19 \pmod{20}$

$p \equiv 1 \pmod{20} \Longrightarrow p = 20k+1 \Longrightarrow n = 10k - 2k = 8k$ even $+1$

$p \equiv 3 \pmod{20} \Longrightarrow p = 20k+3 \Longrightarrow n = 10k+1 - 2k = 8k+1$ odd -1

$p \equiv 7 \pmod{20} \Longrightarrow p = 20k+7 \Longrightarrow n = 10k+3 - 2k = 8k+3$ odd -1

$p \equiv 9 \pmod{20} \Longrightarrow p = 20k+9 \Longrightarrow n = 10k+4 - 2k = 8k+4$ even $+1$

$p \equiv 11 \pmod{20} \Longrightarrow p = 20k+11 \Longrightarrow n = 10k+5 - 2k-1 = 8k+4$ even $+1$

$p \equiv 13 \pmod{20} \Longrightarrow p = 20k+13 \Longrightarrow n = 10k+6 - 2k-1 = 8k+5$ odd -1

$p \equiv 17 \pmod{20} \Longrightarrow p = 20k+17 \Longrightarrow n = 10k+8 - 2k-1 = 8k+7$ odd -1

$p \equiv 19 \pmod{20} \Longrightarrow p = 20k+19 \Longrightarrow n = 10k+9 - 2k-1 = 8k+8$ even $+1$

The Law of Quadratic Reciprocity p, q odd primes

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

i.e., $$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if either } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod 4 \text{ \& } q \equiv 3 \pmod 4 \end{cases}$$

---

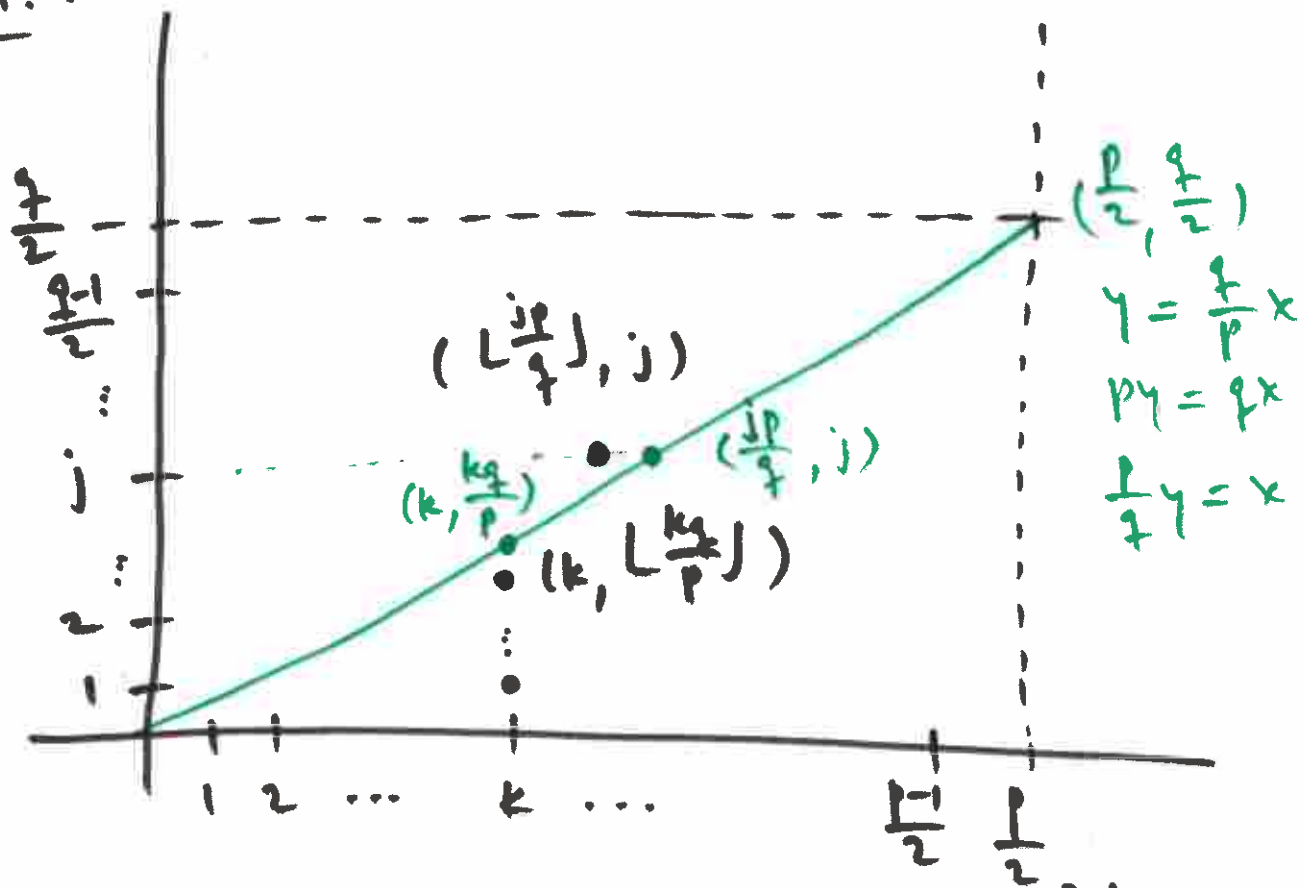
example: is $x^2 \equiv 15 \pmod{83}$ solvable? **No!**

$$\left(\frac{15}{83}\right) = \left(\frac{3}{83}\right)\left(\frac{5}{83}\right) = -\left(\frac{83}{3}\right)\left(\frac{83}{5}\right)$$

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

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

pf.:



total # lattice points is $\frac{(p-1)}{2} \times \frac{(q-1)}{2}$

lattice points below $y = \frac{q}{p}x$ is: $\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor$

lattice points above $y = \frac{q}{p}x$ is: $\sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor$

Thus, $\frac{p-1}{2} \times \frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor$.

Recall:

$(-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor} = (\frac{q}{p})$

&

$(-1)^{\sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor} = (\frac{p}{q})$

$\Downarrow$

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

$\left(\frac{5}{p}\right)$ via Quadratic Reciprocity:

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

$p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$ since p is prime

$p \equiv 1, 2, 3, 4 \pmod 5$

1, 4 are the quadratic residues; 2, 3 are nonresidues

$\left(\frac{p}{5}\right) = 1$ when $p \equiv 1 \pmod 4,\ p \equiv 1 \pmod 5 \implies p \equiv 1 \pmod{20}$

$p \equiv 1 \pmod 4,\ p \equiv 4 \pmod 5 \implies p \equiv 5 + 4 \equiv 9 \pmod{20}$

$p \equiv 3 \pmod 4,\ p \equiv 1 \pmod 5 \implies p \equiv 15 + 16 \equiv 11 \pmod{20}$

$p \equiv 3 \pmod 4,\ p \equiv 4 \pmod 5 \implies p \equiv 15 + 4 \equiv 19 \pmod{20}$

$5x \equiv 1 \pmod 4$, $4x \equiv 1 \pmod 5$

$x \equiv 1$ $x \equiv 4$

11(a) $\left(\frac{71}{73}\right) = \left(\frac{73}{71}\right) = \left(\frac{2}{71}\right) = 1 \Longrightarrow \exists\, x$ s.t. $x^2 \equiv 2 \pmod{71}$

$x = 12, 59$

(c) $\left(\frac{461}{773}\right) = \left(\frac{773}{461}\right) = \left(\frac{312}{461}\right) = \left(\frac{2^3 \cdot 39}{461}\right) = \left(\frac{2^3 \cdot 3 \cdot 13}{461}\right)$

$= \left(\frac{2 \cdot 3 \cdot 13}{461}\right) = \left(\frac{2}{461}\right)\left(\frac{3}{461}\right)\left(\frac{13}{461}\right)$

$= (-1)\left(\frac{461}{3}\right)\left(\frac{461}{13}\right) = (-1)\left(\frac{-1}{3}\right)\left(\frac{6}{13}\right)$

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

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

(b) $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1$ iff

$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$ or $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$.

$\left(\frac{2}{p}\right) = 1$ iff $p \equiv \pm 1 \pmod 8$

$\left(\frac{3}{p}\right) = 1$ iff $p \equiv \pm 1 \pmod{12}$

$p \equiv 1 \pmod 8$, $p \equiv 1 \pmod{12}$

$p \equiv 1 \pmod 3$, $p \equiv 1 \pmod 4$

$p \equiv 1 \pmod{24}$

$p \equiv -1 \pmod 8$, ~~$p \equiv 1 \pmod{12}$~~

~~$p \equiv 1 \pmod 3$, $p \equiv 1 \pmod 4$~~

$\Rightarrow p \equiv \pm 1 \pmod{24}$

$\left(\frac{2}{p}\right) = -1$ iff $p \equiv \pm 3 \pmod 8$

$\left(\frac{3}{p}\right) = -1$ iff $p \equiv \pm 5 \pmod{12}$

$p \equiv 3 \pmod 8$ & ~~$p \equiv 5 \pmod{12}$~~

~~$p \equiv 5 \pmod 3$~~ & ~~$p \equiv 5 \pmod 4$~~

$p \equiv 3 \pmod 8$ & $p \equiv -5 \pmod 3$

$3x \equiv 1 \pmod 3$ $\quad 7x \equiv 1 \pmod 8$

$x \equiv 2$ $\quad x \equiv 7$

$p \equiv -80 + 27 = -53 \equiv \underline{19}$

or

$p = 80 - 27 = +13 \equiv \underline{5}$

Theorem $x^2 \equiv a \pmod{p^n}$ is solvable iff $\left(\frac{a}{p}\right) = 1$.
$n \geq 1$

pf. Suppose that $x^2 \equiv a \pmod{p}$ has a solution. Then
$x^2 \equiv a \pmod{p^n}$ is also solvable.

via induction: base case — then $x^2 \equiv a + bp^n$

IH: suppose that $x^2 \equiv a \pmod{p^n}$ has a solution x
for some $n \geq 1$. Then define y by $2xy \equiv -b \pmod{p}$

and compute:

$$(x + yp^n)^2 = x^2 + 2xyp^n + p^{2n}$$

$$= a + bp^n + 2xyp^n + p^{2n} \equiv a \pmod{p^{n+1}}.$$

$$bp^n + 2xyp^n \equiv 0 \pmod{p^{n+1}}$$

$\blacksquare$

Theorem $x^2 \equiv a \pmod 2$ is always solvable.

$x^2 \equiv a \pmod 4$ is solvable iff $a \equiv 1 \pmod 4$.

$x^2 \equiv a \pmod{2^n}$, $n \geq 3$, is solvable iff $a \equiv 1 \pmod 8$.

pf of 3rd part: base case: $n = 3$

$x^2 \equiv a \pmod 8$ is solvable iff $a \equiv 1 \pmod 8$. ∎

IH: suppose that $x^2 \equiv a \pmod{2^n}$ solvable

Then $x^2 = a + b \cdot 2^n$, define y by

$xy \equiv -b \pmod 2$ and compute

$$(x + y \cdot 2^{n-1})^2 = x^2 + 2^n \cdot xy + y^2 \cdot 2^{2n-2}$$

$$= a + b \cdot 2^n + 2^n \cdot xy + y^2 \cdot 2^{2n-2}$$

$$\equiv a \pmod{2^{n+1}}.$$

∎