Euler's criterion

more professionally: quadratic residue

THM p odd prime, $\gcd(r,p)=1$.

$$r^{\frac{p-1}{2}} \equiv \begin{cases} +1 & \text{if } r \pmod p \text{ is a square} \\ -1 & \text{if } r \pmod p \text{ is not a square} \end{cases}$$

$\left(r^{\frac{p-1}{2}}\right)^2 = r^{p-1} \equiv 1 \pmod p$

EG Is 5 a square mod 19? Mod 37?

mod 19 $\quad 5^{\frac{19-1}{2}} = 5^9 \equiv ? \pmod{19}$

binary exponentiation: $5^2 \equiv 6$, $5^4 \equiv 6^2 \equiv -2$, $5^8 \equiv (-2)^2 = 4$

$5^9 = 5^8 \cdot 5 \equiv 4 \cdot 5 \equiv 1 \pmod{19}$

$\overset{\text{Euler}}{\Longrightarrow}$ 5 (mod 19) is a square

extra: $9^2 \equiv 5 \pmod{19}$

mod 37 $\quad 5^{\frac{37-1}{2}} = 5^{18} \equiv ? \pmod{37}$

$5^2 \equiv -12$, $5^4 \equiv -4$, $5^8 \equiv 16$, $5^{16} \equiv -3$

$5^{18} = 5^{16} \cdot 5^2 \equiv -3 \cdot (-12) \equiv -1$

$\overset{\text{Euler}}{\Longrightarrow}$ 5 (mod 37) is not a square

Pf like Wilson

$(p-1)! =$ product of all invertible residues mod p

$\equiv -1 \pmod p$

Wilson: pair up x with x^{-1} $\qquad x \cdot x^{-1} \equiv 1$

now: pair up x with $r \cdot x^{-1}$

paired with $r \cdot (r \cdot x^{-1})^{-1} \equiv x$

$x \cdot (rx^{-1}) \equiv r$

except if $x \equiv r \cdot x^{-1}$

$x^2 \equiv r$

if r is not a square mod p $\qquad$ no solution / no exception

$$\underset{\text{Wilson}}{-1} \equiv (p-1)! \equiv \underbrace{\_\_\_\_ \; x \cdot (r \cdot x^{-1}) \; \_\_\_\_}_{\frac{p-1}{2} \text{ pairs}} \equiv r^{(p-1)/2} \pmod p$$

if r is a square mod p $\qquad$ two solutions: $\pm b$

$$-1 \equiv (p-1)! \equiv \underbrace{+b \cdot (-b)}_{-b^2 \equiv -r} \underbrace{\_\_\_\_ \; x \cdot (r \cdot x^{-1}) \; \_\_\_\_}_{\frac{p-1}{2} - 1 \text{ pairs}} \equiv -r \cdot r^{(p-1)/2 - 1}$$

$$\equiv -r^{(p-1)/2} \pmod p$$

$\square$

COR $-1 \pmod p$ (odd) is a square $\iff (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p \iff (-1)^{\frac{p-1}{2}} = 1$

$\iff \frac{p-1}{2}$ even $\iff \frac{p-1}{2} = 2m \iff p-1 = 4m$

$\iff p-1 \equiv 0 \pmod 4$

$\iff p \equiv 1 \pmod 4$

EG $p = 13 \qquad 13 \equiv 1 \pmod 4$

$5^2 \equiv -1 \pmod{13}$