Fermat: p prime, $a \in \mathbb{N}$ s.t. $p \nmid a$,

Then $a^{p-1} \equiv 1 \pmod{p}$.

converse NOT true!

And: p prime, $a \in \mathbb{N} \Rightarrow a^p \equiv a \pmod{p}$.

Wilson: $(n-1)! \equiv -1 \pmod{n}$ iff n is prime.

Theorem: p an odd prime

$x^2+1 \equiv 0 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{4}$.

pf. if $a^2+1 \equiv 0 \pmod{p} \Rightarrow a^2 \equiv -1 \pmod{p}$

$$\Rightarrow (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

$$\Rightarrow a^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

$$\Rightarrow 0 \equiv 1 \pmod{4}$$

if $p = 4k+3$, $\frac{p-1}{2} = 2k+1$, odd.

contradiction!!

if $p \equiv 1 \pmod 4$, compute:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-2)(p-1)$$

$$\begin{cases} p-1 \equiv -1 \pmod p \\ p-2 \equiv -2 \pmod p \\ \vdots \\ p-\left(\frac{p-1}{2}\right) \equiv -\frac{(p-1)}{2} \pmod p \\ \Rightarrow \frac{p+1}{2} \equiv -\frac{(p-1)}{2} \pmod p \end{cases}$$

Then $\underbrace{(p-1)!} \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 (-1)^{\frac{p-1}{2}} \pmod p$

$\equiv -1 \pmod p$

$p \equiv 1 \pmod 4 \Rightarrow p = 4k+1$

$\Rightarrow \frac{p-1}{2} = 2k$, even

and then

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p \Longrightarrow \left(\frac{p-1}{2}\right)! \text{ solves}$$

$$x^2 + 1 \equiv 0 \pmod p.$$

∎

6(c) $3^{100} \equiv ?\ (\mathrm{mod}\ 10)$

Fermat: $3^4 \equiv 1\ (\mathrm{mod}\ 5) \Rightarrow 3^{100} \equiv 1\ (\mathrm{mod}\ 5)$

parity: $3 \equiv 1\ (\mathrm{mod}\ 2) \Rightarrow 3^{100} \equiv 1\ (\mathrm{mod}\ 2)$

$\Rightarrow 3^{100} \equiv 1\ (\mathrm{mod}\ 10)$

2(a) $\gcd(a, 35) = 1 \Rightarrow a^{12} \equiv 1\ (\mathrm{mod}\ 35)$

$5, 7 \nmid a$

Fermat: $a^4 \equiv 1\ (\mathrm{mod}\ 5) \Rightarrow a^{12} \equiv 1\ (\mathrm{mod}\ 5)$

$\hookrightarrow a^6 \equiv 1\ (\mathrm{mod}\ 7) \Rightarrow a^{12} \equiv 1\ (\mathrm{mod}\ 7)$

$\Rightarrow a^{12} \equiv 1\ (\mathrm{mod}\ 35)$

2(b) $\gcd(a, 42) = 1 \Rightarrow 168 = 3 \cdot 7 \cdot 8 \mid a^6 - 1$

$2, 3, 7 \nmid a$

a odd, $a \geq 4$

Fermat: $a^2 \equiv 1\ (\mathrm{mod}\ 3) \Rightarrow a^6 \equiv 1\ (\mathrm{mod}\ 3)$

$\hookrightarrow a^6 \equiv 1\ (\mathrm{mod}\ 7) \Rightarrow a^6 \equiv 1\ (\mathrm{mod}\ 7)$

$a \equiv 1\ (\mathrm{mod}\ 2) \not\Rightarrow a^3 \equiv 1\ (\mathrm{mod}\ 8)$: ex: ~~$a = 3$~~ $a = 7$

However: $a \equiv 1\ (\mathrm{mod}\ 2) \Rightarrow a^2 \equiv 1\ (\mathrm{mod}\ 4)$

$$a = 4k \pm 1 \implies a^6 = (4k \pm 1)^6$$

$$= (4k)^6 \pm 6(4k)^5 + 15(4k)^4 \pm 20(4k)^3$$

$$+ 15(4k)^2 \pm 6(4k) + 1$$

$$\implies a^6 \equiv 1 \pmod 8$$

2(c) $\gcd(a, 133) = \gcd(b, 133) = 1 \implies 133 \mid a^{18} - b^{18}$

$133 = 7 \cdot 19$

Fermat: $a^{18} \equiv 1 \pmod{19}$

$b^{18} \equiv 1 \pmod{19}$

$a^6 \equiv 1 \pmod 7 \implies a^{18} \equiv 1 \pmod 7$

$b^6 \equiv 1 \pmod 7 \implies b^{18} \equiv 1 \pmod 7$

$a^{18} \equiv 1 \pmod{133}$

$b^{18} \equiv 1 \pmod{133}$

$\implies a^{18} - b^{18} \equiv 0 \pmod{133}$

$m = 8$, $a = 3$

$0, 1, 2, 3, 4, 5, 6, 7$

$1, 3, 5, 7$ relatively prime to 8

$3, 9, 15, 21$

$3, 1, 7, 5$

$3^4 \equiv 1 \pmod 8$

$m = 7$, $a \in \mathbb{N}$, $7 \nmid a$

$1, 2, 3, 4, 5, 6$

$a = 3$

$3, 6, 9, 12, 15, 18$

$\Rightarrow 3, 6, 2, 5, 1, 4$

Given $n \in \mathbb{N}$, <u>define</u> $\varphi(n) :=$ # integers $< n$ that are relatively prime to n.

<u>Ex</u>: $\varphi(8) = 4$, $\varphi(7) = 6$, $\varphi(p) = p-1$ for any prime p.

This is Euler's φ-function. (totient)

(ϕ-function)

Euler's Theorem

$m \in \mathbb{N}$, $a \in \mathbb{N}$ with $\gcd(a,m) = 1$

Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Pf. Take $\varphi(m)$ integers $q_1, \dots, q_{\varphi(m)}$ s.t.

$$1 \le q_1, \dots, q_{\varphi(m)} \le m-1 \quad \text{and} \quad \gcd(q_i, m) = 1 \ \forall i.$$

Then $aq_1, \dots, aq_{\varphi(m)}$ are congruent to $q_1, \dots, q_{\varphi(m)}$,

and we get

$$(aq_1)(aq_2)\cdots(aq_{\varphi(m)}) \equiv q_1 \cdot q_2 \cdot \dots \cdot q_{\varphi(m)} \pmod{m}$$

$$\Longrightarrow \quad a^{\varphi(m)} \equiv 1 \pmod{m}.$$

∎