3. If $\gcd(a, 42) = 1$ then $168 \mid a^6 - 1$

$42 = 2 \cdot 3 \cdot 7$
$168 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7$

Because the gcd of a & 42 is 1 we know that a cannot divide any of 42's factors.

$42 = 2 \cdot 3 \cdot 7$ $\quad 2 \nmid a \quad 3 \nmid a \quad 7 \nmid a$

$168 \mid a^6 - 1$ can be re written as a congruence. And then gotten a simultaneous congruency for each of the factors of 168.

$168 \mid a^6 - 1$

$a^6 - 1 \equiv 0 \pmod{168}$

$a^6 \equiv 1 \pmod{168}$

$a^6 \equiv 1 \pmod 8$

- a must be odd as $2 \nmid a$
- All odd numbers can be represented as $4k+1$ or $4k-1$

$(4k+1)(4k+1) = 8(2k^2+k) + 1 \in 8n+1$

$(4k-1)(4k-1) = 8(2k^2-k) + 1 \in 8m+1$

thus any odd number squared is of form $8k+1$

therefore $a^2 \equiv 1 \pmod 8$

$(a^2)^3 \equiv a^6 \equiv 1^3 \equiv 1 \pmod 8$ ✓

$a^6 \overset{?}{\equiv} 1 \pmod 7$

$a^{7-1} \equiv 1 \pmod 7$

True by fermat's theorem as $7 \nmid a$. ✓

$a^6 \equiv 1 \pmod 3$

Because $3 \nmid a$, $a \not\equiv 0 \pmod 3$ and thus either

$a \equiv 1 \pmod 3$ or $a \equiv 2 \pmod 3$

$1^6 \overset{?}{\equiv} 1 \pmod 3$ $\qquad 2^6 \overset{?}{\equiv} 1 \pmod 3$

$1 \equiv 1 \pmod 3$ ✓ $\qquad 64 \equiv 1 \pmod 3$

$\qquad 1 \equiv 1 \pmod 3$ ✓

Because all 3 parts of the simultaneous congruence are guaranteed to hold, the original must also hold and so must ~~the~~ 168 divide $a^6 - 1$.

$133 = 7 \cdot 9$

4. $\gcd(a, 133) = \gcd(b, 133) = 1$ then $133 \mid a^{18} - b^{18}$

- because $133 = 7 \cdot 9$

$\gcd(a,7) = \gcd(b,7) = \gcd(a,9) = \gcd(b,9) = 1$ $\therefore$ $a \nmid 7$ $a \nmid 9$ $b \nmid 7$ $b \nmid 9$

- so we can apply Fermat's Little theorem giving

$a^8 \equiv b^8 \equiv 1 \pmod 9$ & $a^6 \equiv b^6 \equiv 1 \pmod 7$

the proposition can be rewritten as a simultaneous congruence.

$133 \mid a^{18} - b^{18}$

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

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

$a^{18} \overset{?}{\equiv} b^{18} \pmod 7$ $\qquad$ $a^{18} \overset{?}{\equiv} b^{18} \pmod 9$

$(a^6)^3 \overset{?}{=} (b^6)^3 \pmod 7$ $\qquad$ $(a^8)^2 \overset{?}{\equiv} (b^8)^2 \pmod 9$

substituting the congruencies from fermat's theorem...

$(1)^3 \equiv (1)^3 \pmod 7$ $\qquad$ $(1)^2 \equiv (1)^2 \pmod 7$

$1 \equiv 1 \pmod 7$ ✓ $\qquad$ $1 \equiv 1 \pmod 7$ ✓

as both parts of the simultaneous congruence hold ~~the original~~ so must the proposition #

6. $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13} \quad \forall\, a \in \mathbb{Z}$

The proposition can be rewritten as a simultaneous congruence

$a^{13} \equiv a \pmod 7$
$\therefore a^{14} \equiv a^2 \pmod 7$
$(a^2)^7 \equiv a^2 \pmod 7$
let $c = a^2$
$c^7 \equiv c \pmod 7$
true by corollary of FLT as 7 is prime ✓

$a^{13} \equiv a \pmod 3$
we can verify the congruence for all possible values of a. (exhaustion)
$a \bmod 3 \in \{0, 1, 2\}$

$a \equiv 0 \pmod 3$
$0^{13} \equiv 0 \pmod 3$
$0 \equiv 0 \pmod 3$ ✓

$a \equiv 1 \pmod 3$
$1^{13} \equiv 1 \pmod 3$
$1 \equiv 1 \pmod 3$ ✓

$a \equiv 2 \pmod 3$
$2^{13} \equiv 2 \pmod 3$
[illegible] $\equiv 2 \pmod 3$
[illegible] $\equiv 2 \pmod 3$ ✓

$a^{13} \equiv a \pmod{13}$
true by corollary of FLT as 13 is prime ✓

Because all 3 parts of the simultaneous congruence have been shown to hold for all a the proposition must also hold.

7a. $3^{100} \bmod 10 = ?$

$10 \nmid 3 \quad 10 = 2 \cdot 5$

$3 \equiv 1 \pmod 2$
$3^{100} \equiv 1^{100} \equiv \underline{1} \pmod 2$

$3^4 \equiv 1 \pmod 5$
$(3^4)^{25} \equiv 1^{25} \equiv \underline{1} \pmod 5$

$3^{100} \equiv 1 \pmod{10}$

Because there is a simultaneous solution @ 1

7b. $a^5 \equiv a \pmod{10}$
Prop can be rewritten as simultaneous congruence

$a^5 \equiv a \pmod 5$
true by corollary of FLT as 5 is prime ✓

$+$

$a^5 \equiv a \pmod 2$
proof by exhaustion
$0^5 \equiv 0 \pmod 2$
$0 \equiv 0 \pmod 2$ ✓
$1^5 \equiv 1 \pmod 2$
$1 \equiv 1 \pmod 2$ ✓

supports prop.

Because the representative simultaneous congruency holds for all $a \in \mathbb{Z}$ we confirm the proposition.

6. $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ $\forall\ a \in \mathbb{Z}$

The proposition can be rewritten as a simultaneous congruence

$a^{13} \equiv a \pmod 7$

$\therefore a^{14} \equiv a^2 \pmod 7$

$(a^2)^7 \equiv a^2 \pmod 7$

let $c = a^2$ in

$c^7 \equiv c \pmod 7$

true by corollary of FLT as 7 is prime ✓

$a^{13} \equiv a \pmod 3$

we can verify the congruence for all possible values of a. (exhaustion)

$a \bmod 3 \in \{0,1,2\}$

$a \equiv 0 \pmod 3$

$0^{13} \equiv 0 \pmod 3$

$0 \equiv 0 \pmod 3$ ✓

$a \equiv 1 \pmod 3$

$1^{13} \equiv 1 \pmod 3$

$1 \equiv 1 \pmod 3$ ✓

$a \equiv 2 \pmod 3$

$2^{13} \equiv 2 \pmod 3$

$8192 \equiv 2 \pmod 3$

$20 \equiv 2 \equiv 2 \pmod 3$ ✓

$a^{13} \equiv a \pmod{13}$

true by corollary of FLT as 13 is prime ✓

Because all 3 parts of the simultaneous congruence have been proven to hold for all a the proposition must also hold.

7a. $3^{100} \bmod 10 = ?$ $10 + 3$ $10 = 2 \cdot 5$

$3 \equiv 1 \pmod 2$

$3^{100} \equiv 1^{100} \equiv 1 \pmod 2$

$3^4 \equiv 1 \pmod 5$

$(3^4)^{25} \equiv 1^{25} \equiv 1 \pmod 5$

$3^{100} \equiv 1 \pmod{10}$

Because there is a simultaneous solution @ 1

7b. $a^5 \equiv a \pmod{10}$

Prop can be rewritten as simultaneous congruence

$a^5 \equiv a \pmod 5$ + $a^5 \equiv a \pmod 2$

true by corollary of FLT as 5 is prime ✓

proof by exhaustion

$0^5 \equiv 0 \pmod 2$

$0 \equiv 0 \pmod 2$ ✓

$1^5 \equiv 1 \pmod 2$

$1 \equiv 1 \pmod 2$ ✓

Because the representative simultaneous congruency holds for all $a \in \mathbb{Z}$ we [illegible] confirm the proposition. supports prop.

4. p is prime $a, b \in \mathbb{Z}$ $p \nmid a, b$

a. if $a^p \equiv b^p \pmod{p}$ then $a \equiv b \pmod{p}$

a corollary of FLT states that $a^p \equiv a \pmod{p}$ when p is prime and $a \in \mathbb{Z}$.
using this we can simplify

$a^p \equiv a \pmod{p}$ $b^p \equiv b \pmod{p}$

$a^p \equiv b^p \pmod{p}$

$a \equiv b \pmod{p}$ ⁂

b. if $a^p \equiv b^p \pmod{p}$ then $a^p \equiv b^p \pmod{p^2}$ uh...

9. see attached sagemath code

4. p is prime $a, b \in \mathbb{Z}$ $p \nmid a, b$

a. if $a^p \equiv b^p \pmod{p}$ then $a \equiv b \pmod{p}$

a corollary of FLT states that $a^p \equiv a \pmod{p}$ when p is prime and $\forall a \in \mathbb{Z}$.
using this we can simplify

$$a^p \equiv a \pmod{p} \qquad b^p \equiv b \pmod{p}$$

$$a^p \equiv b^p \pmod{p}$$

$$a \equiv b \pmod{p}$$

b. if $a^p \equiv b^p \pmod{p}$ then $a^p \equiv b^p \pmod{p^2}$

ehh...