Speciell uppgift tycker jag!

$\boxed{2157}$

(a) Vi låter p vara 3.

$$x^{3-1} \equiv 1 \pmod 3$$

$$x^2 \equiv 1 \pmod 3$$

Detta innebär att $x^2 - 1$ är delbart med 3.

(Testa med $x = 7$: $7^2 - 1 = 48$, $48 = 16 \cdot 3$ ok!)

Allmänt innebär

$$x^{p-1} \equiv 1 \pmod p$$

att $x^{p-1} - 1$ är delbart med p. ~~Ferm~~

Fermats lilla sats kan alltså formuleras

"Om p är ett primtal, och x ett heltal som inte har p som faktor, är $x^{p-1} - 1$ delbart med p".

(b) Vi låter $p = 7$. Då är $x^{7-1} - 1 = x^6 - 1$ delbart med 7.

Svar: $x^6 - 1$ (x heltal som inte har 7 som faktor)

(c) Vi sätter $x = 2$. Satsen kan då skrivas:

p primtal $\Rightarrow$ $2^{p-1} - 1$ delbart med p.

Omvändningen blir

$2^{p-1} - 1$ delbart med p $\Rightarrow$ p primtal, dvs

"Om $2^{p-1} - 1$ är delbart med p är p ett primtal".

Ingen aning!
