

14/3-2025

2. Vad är sista tre siffror i $2003^{2002^{2001}}$?

- Först har vi $2003^{2002^{2001}} \equiv_{1000} 3^{2002^{2001}}$
- Låt $y = 3^{2002^{2001}}$. Enligt kinesiska restsatsen ska vi beräkna $y \bmod 8$ och $y \bmod 125$ eftersom $1000 = 8 \times 125$. Vi använder Eulers sats.

- Nu beräknar vi $y \bmod 8$.
• Eulers sats säger att $3^{\phi(8)} \equiv_8 1$ ($\text{SGD}(3,8)=1$)
• $\phi(8) = 8 \cdot (1 - \frac{1}{2}) = 4$. Så vi ska räkna ut värdet på $2002^{2001} \bmod 4$, dvs.

$$2002^{2001} \equiv_4 2^{2001} = 0$$

$$\Rightarrow 3^{2002^{2001}} \equiv_8 3^0 = 1$$

- Nästa: $y \bmod 125$.

Återigen Eulers sats. $3^{\phi(125)} \equiv_{125} 1$

$$(\text{SGD}(125,3)=1)$$

$\Rightarrow$ Vi behöver räkna på $2002^{2001} \bmod 100$ eftersom $\phi(125) = 125(1 - \frac{1}{5}) = 100$.

$$2002^{2001} \equiv_{100} 2^{2001}$$

(1)

Här kan vi antingen beräkna direkt eller använda kinesiska restsatsen: $100 = 25 \times 4$.

$$\begin{cases} 2^{2001} \equiv_4 0 \\ 2^{2001} \equiv_{25} 2 \end{cases}$$

$$2^{2001} = 2(2^{20})^{100} = 2(2^{\phi(25)})^{100} \equiv_{25} 2$$

(Låt $x = 2^{2001}$)

$$\Leftrightarrow x = 4k \text{ och } x = 25m + 2$$

$$\Leftrightarrow 4k = 25m + 2$$

Tag $\bmod 4$ på båda sidor för

$$0 \equiv_4 m + 2 \Leftrightarrow m \equiv_4 -2 \equiv_4 2$$

$$\Rightarrow x \equiv_{100} 25 \cdot 2 + 2 = 52$$

$$\Rightarrow 3^{2002^{2001}} \equiv_{125} 3^{52} = (3^5)^{10} \cdot 3^2$$

$$\equiv_{125} (-7)^{10} \cdot 9 = 7^{10} \cdot 9$$

$$= (7^4)^2 \cdot 7^2 \cdot 9 = (49^2)^2 \cdot 49 \cdot 9$$

$$\equiv_{125} 26^2 \cdot 49 \cdot 9 \equiv_{125} 51 \cdot 4 \cdot 9$$

$$\equiv_{125} 116$$

Alltså

$$3^{2002^{2001}} \equiv_{125} 116$$

- Lös nu $y \equiv_8 1$ & $y \equiv_{125} 116 \Leftrightarrow 8k + 1 = 125m + 116$
 $\Leftrightarrow 8k = 125m + 115 \Leftrightarrow 0 \equiv_8 5m + 3$
 $\Leftrightarrow 5m \equiv_8 -3 \equiv_8 5 \Leftrightarrow m \equiv_8 1$
 $\Rightarrow y = 125 \cdot 1 + 116 = 241$. sista siffrorna

3. Finn alla positiva heltal n sådana att $2^n - 1$ är en multipel av 3 och $\frac{2^n - 1}{3}$ är en delare till $4m^2 + 1$ för något heltal m .

Lösning. Vi vet $2^n - 1 \equiv_3 0 \Rightarrow n = 2k$ (jämn)

så ekvationen blir $\frac{4^k - 1}{3} \mid 4m^2 + 1$.

Lösningen till denna ekvation är $n = 2^r$ för $r \geq 1$.

dvs. $k = 2^m$ för $m \geq 0$.

• Notera att om $k = 2^m$, $m \geq 0$, har vi

$$\begin{aligned} \frac{4^k - 1}{3} &= \frac{4^{2^m} - 1}{3} = \frac{(4^{2^{m-1}} + 1)(4^{2^{m-1}} - 1)}{3} \quad \left\{ \begin{array}{l} \text{konjugat-} \\ \text{regeln} \end{array} \right\} \\ &= \dots = \frac{(4^{2^{m-1}} + 1)(4^{2^{m-2}} + 1) \dots (4 + 1)(4 - 1)}{3} \\ &= (4^{2^{m-1}} + 1)(4^{2^{m-2}} + 1) \dots (4 + 1) =: L \end{aligned}$$

Vi måste ha $4m^2 + 1 \equiv_2 0$.

För att använda kinesiska restsatsen att dela upp produktens delare vi visar att alla tal i L är relativt prima. Detta följer av observationen $4^{2^a} + 1 = 2^{2^{a+1}} + 1$ vilket är Fermats tal. Med induktion kan vi visa att

de är parvis relativt prima. Tillämpa kinesiska restsatsen ska vi lösa

$$\begin{cases} 4m^2 + 1 \equiv_{4^{2^{m-1}} + 1} 0 \\ 4m^2 + 1 \equiv_{4^{2^{m-2}} + 1} 0 \\ \vdots \\ 4m^2 + 1 \equiv_{4+1} 0 \end{cases}$$

Observera att $4^{2^a} + 1 = 4 - 4^{2^{a-1}} + 1 = 4(2^{2^{a-1}} + 1) + 1$ för $a \geq 0$. Därför är lösningen till

$$4m^2 + 1 \equiv_{4^{2^a} + 1} 0 \quad m \equiv 2^{2^a - 1} \pmod{4^{2^a} + 1}$$

så det finns ett m som uppfyller alla ekvationer ovan enligt kinesiska restsatsen

Dvs. vi har bevisat $k = 2^m$ för $m \geq 0$.

Nuskarvis visa att k måste vara 2^m .

Antag $k \neq 2^m$. Då $k = p \cdot 2^m$, $m \geq 0$, $p \neq 1$ är udda. Beräkna

$$\frac{4^{p \cdot 2^m} - 1}{3} = \frac{(4^{2^{m-1} \cdot p} + 1)(4^{2^{m-2} \cdot p} + 1) \dots (4^p + 1)(4 - 1)}{3}$$

1. Då har vi implikationen =

$$4m^2 + 1 \equiv 0 \pmod{4^{2^m} - 1}$$

$$\Rightarrow 4m^2 + 1 \equiv 0 \pmod{\frac{4^p - 1}{3}}$$

$$\cdot \frac{4^p - 1}{3} = \frac{(2^p - 1)(2^p + 1)}{3} \cdot \left\{ \begin{array}{l} \text{så implikationen blir} \\ p \text{ är udda} \Rightarrow 3 \mid 2^p + 1 \end{array} \right.$$

$$4m^2 + 1 \equiv 0 \pmod{\frac{4^p - 1}{3}} \Rightarrow 4m^2 + 1 \equiv 0 \pmod{2^p - 1}$$

Eftersom $p > 1$ har vi $2^p - 1 \equiv 3 \pmod{4}$. Antag att alla primdelare av $2^p - 1$ är på form 1 mod 4. Det medför att $2^p - 1 \equiv 1 \pmod{4}$. Så det finns minst en primtal delare av $2^p - 1$ som är på form

3 mod 4, Kalla den z .

$$(2m)^2 \equiv -1 \pmod{\frac{4^p - 1}{3}} \equiv -1 \pmod{z}$$

omöjligt (Eulers sats).

Så lösningen är $k = 2^m$ för $m \geq 0$.

$$\Rightarrow n = 2^r \text{ för } r \geq 1.$$