Forelesning 26 – mandag den 17. november

Del I

Richard Williamson

19. november 2014

Fire typer oppgaver

Vis uten å regne ut at $72 \cdot (32!) + 3$ er delelig med 37

Vis uten å regne ut at $3 \cdot \left(5^{128}\right) + 1$ er delelig med 19

Vis uten å regne ut at $72 \cdot (32!) + 3$ er delelig med 37

$\boxed{\text{Oversett først til modulær aritmetikk.}}$

Får: $72 \cdot (32!) + 3 \equiv 0 \pmod{37}$.

$\boxed{\text{Vi ser et fakultet: Wilsons teorem.}}$

Wilsons teorem

$\boxed{\text{La } p \text{ være et primtall. Da er } (p-1)! \equiv -1 \pmod{p}.}$

Har: 37 er et primtall.

Derfor må benytte: $36! \equiv -1 \pmod{37}$.

Tips: Til og med om du ikke kan gå videre, skriv ned at du skjønner at denne kongruensen bør benyttes.

Hvordan kan $36! \equiv -1 \pmod{37}$ benyttes?

Imidlertid: Har 32!, ikke 36!.

$\boxed{\text{Finn en forhold mellom } 32! \text{ og } 36!.}$

Har:

$$\begin{aligned} 36! &= 32! \cdot 33 \cdot 34 \cdot 35 \cdot 36 \\ &\equiv 32! \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \pmod{37}. \end{aligned}$$

Tips

Når vi har et heltall som er litt mindre enn heltallet vi jobber modulo med, er det ofte en god idé å erstatte det med et negativt heltall det er kongruent til.

Her ersattet vi: 36 med -1, 35 med -2, 34 med -3, iog 33 med -4.

Sjekk alltid: om du kan benytte dette trikset for å gjøre en utregning enklere. Ikke alltid mulig/nyttig!

Nå benytter vi Wilsons teorem, som vi har hensikt til å gjøre

Dermed: $36! \equiv 32! \cdot 24 \pmod{37}$.

Derfor: $24 \cdot (32!) \equiv 36! \pmod{37}$.

$\boxed{\text{Benytt: } 36! \equiv -1 \pmod{37}.}$

Får: $24 \cdot (32!) \equiv -1 \pmod{37}$.

Hvordan benytter vi $24 \cdot (32!) \equiv -1 \pmod{37}$?

$\boxed{\text{Sammenlign med målet, nemlig } 72 \cdot (32!) + 3 \equiv 0 \pmod{37}.}$

Ser: $72 = 24 \cdot 3$.

Derfor: Gang begge sidene av $24 \cdot (32!) \equiv -1 \pmod{37}$ med 3.

Får: $3 \cdot 24 \cdot (32!) \equiv 3 \cdot (-1) = -3 \pmod{37}$.

Dermed: $72 \cdot (32!) \equiv -3 \pmod{37}$.

Nå har vi vist at $72 \cdot (32!) \equiv -3 \pmod{37}$

$\boxed{\text{Sammenlign igjen med målet, nemlig } 72 \cdot (32!) + 3 \equiv 0 \pmod{37}.}$

Ser: Kan legge 3 til begge sidene.

Får: $72 \cdot (32!) + 3 \equiv 0 \pmod{37}$.

Vi har rukket målet!

Vis uten å regne ut at $3 \cdot \left(5^{128}\right) + 1$ er delelig med 19

Oversett først til modulær aritmetikk.

Får: $3 \cdot \left(5^{128}\right) + 1 \equiv 0 \pmod{19}$.

Vi ser en stor potens og at vi jobber modulo et primtall: Fermats

lille teorem.

Fermats lille teorem

La p være et primtall. La x være et heltall slik at det ikke er sant at $x \equiv 0 \pmod{p}$. Da er $x^{p-1} \equiv 1 \pmod{p}$.

Har: 19 er et primtall.

Derfor må benytte: $5^{18} \equiv 1 \pmod{19}$.

Hvordan kan $36! \equiv -1 \pmod{37}$ benyttes?

$\boxed{\text{Del 128 med 18.}}$

Får: $128 = 7 \cdot 18 + 2$.

Derfor: $5^{128} = 5^{7 \cdot 18} \cdot 5^2 = \left(5^{18}\right)^7 \cdot 5^2$.

$\boxed{\text{Benytt: } 5^{18} \equiv 1 \pmod{19}.}$

Får: $\left(5^{18}\right)^7 \cdot 5^2 \equiv 1^7 \cdot 5^2 = 25 \equiv 6 \pmod{19}$.

Dermed: $5^{128} = \left(5^{18}\right)^7 \cdot 5^2 \equiv 6 \pmod{19}$.

Hvordan benytter vi $5^{128} \equiv 6 \pmod{19}$?

$\boxed{\text{Sammenlign med målet, nemlig } 3 \cdot \left(5^{128}\right) + 1 \equiv 0 \pmod{19}}$

Deretter: Gang begge sidene av $5^{128} \equiv 6 \pmod{19}$ med 3.

Får: $3 \cdot 5^{128} \equiv 3 \cdot 6 = 18 \pmod{19}$.

$\boxed{\text{Sammenlign igjen med målet, nemlig } 3 \cdot \left(5^{128}\right) + 1 \equiv 0 \pmod{19}}$

Deretter: Legg 1 til begge sidene av $3 \cdot 5^{128} \equiv 18 \pmod{19}$.

Får: $3 \cdot 5^{128} + 1 \equiv 18 + 1 = 19 \equiv 0 \pmod{19}$.

Vi har rukket målet!