Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Oppgave 3 La universalmengden være $\mathbb{Z}_{55} = \{0, 1, \ldots, 54\}$. Hvilke av følgende utsagn er sanne?

1. $\forall a \exists b (a \cdot b \equiv 1 \pmod{55})$
2. $\exists b \forall a (a^b \equiv a \pmod{55})$
3. Antall element i $\mathbb{Z}_{55}$ som har en invers i $\mathbb{Z}_{55}$ er 40.
4. Kongruensen $x^2 \equiv 1 \pmod{55}$ har nøyaktig 2 løsninger modulo 55.

Alt 1): Dette er galt. Denne var grei.

Alt 2): Dette er riktig. Denne var grei siden $b = 1$ ga resultatet.

Alt 3): Dette er riktig. Dette fulgte fra Bezout's teorem og prinsippet om inklusjon/eksklusjon: Vi trenger ikke å se på 0 da denne åpenbart ikke har en invers. Antallet elementer tall mellom 1 og 54 relativt primiske til 55 er $54 - m_5 - m_{11} + m_{5\cdot 11}$, hvor m_5 er antallet tall som er multiplum av 5 mellom 1 og 55, m_{11} er antallet tall som er multiplum av 11 mellom 1 og 55, og $m_{5\cdot 11}$ er antallet tall som er multiplum av 5 og 11 mellom 1 og 55.

m_5 er 10 siden $5 \cdot 10$ er høyeste multiplum av 5 og vi ikke inkluderer 0. m_{11} er 4 siden høyeste multiplum av 11 er 44 og vi ikke inkluderer 0, og $m_{5\cdot 11}$ er 0 siden vi ikke inkluderer 0. Antall element i $\mathbb{Z}_{55}$ som har en invers i $\mathbb{Z}_{55}$ er $54 - 10 - 4 + 0 = 40$.

Alt 4): Kongruensen $x^2 \equiv 1 \pmod{55}$ har nøyaktig 2 løsninger modulo 55.

Løsning 1: Dette er galt.

Her ønsker vi å bruke det Kinesiske restteoremet slik vi gjør det i RSA. Ved Fermats lille holder $y^4 \equiv 1 \mod 5$ og $y^{10} \equiv 1 \mod 11$ for y som tilfredsstiller $\gcd(y,5) = \gcd(y,11) = 1$ slik at $y^{(2\cdot 10)} \equiv 1 \mod 55$.

Så vi leter etter en y relativt primiskt til både 5 og 11 som vi så opphøyer i 10 modulo 55 s.a. $(y^{10})^2 \equiv 1 \mod 55$. $x \not\equiv \pm 1 \mod 55$ blir da y^{10}, eventuelt en mindre potens hvis denne mindre potensen kvadrerer til 1 modulo 55.

Hvis man prøver $y = 2$ finner man ved rask regning at $2^{10} \equiv 34 \mod 55$ samt at $34^2 \equiv 1 \mod 55$, og dette er da tilstrekkelig.

Løsning 2: Vi kan også bruke KRT på en annen måte. Vi prøver å finne $x \equiv -1 \mod 5$ og $x \equiv 1 \mod 11$. Ved KRT får vi $x = -1 \cdot 11 \cdot 1 + 5^2 \cdot 2^2 \equiv 34 \mod 55$ og man kan sjekke at $34^2 \equiv 1 \mod 55$.