MA1301 Tallteori
Midtsemesterprøve
Løsningsforslag

Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Løsningsforslag — Øving

$\boxed{1}$ Én av følgende diofantiske ligninger kan løses. Hvilken?

1. $26x + 39y = 13$
2. $16x + 6y = 3$
3. $35x + 10y = 3$
4. $38x + 4y = 19$

Løsning:
For at den diofantiske ligningen $ax + by = c$ skal ha en løsning, må $\gcd(a, b) \mid c$. Svaret er dermed $26x + 39y = 13$, siden $\gcd(26, 39) = 13$, og $13 \mid 13$.

$\boxed{2}$ Hvilket av følgende tall er delelig med 33?

1. $101^{76} - 130^{33}$
2. $101^{77} - 130^{33}$
3. $101^{78} - 130^{33}$
4. $101^{79} - 130^{33}$

Løsning:
Vi ser at $101 \equiv 2 \pmod{33}$ og $130 \equiv -2 \pmod{33}$. Vi regner så ut at $2^5 \equiv -1 \pmod{33}$, som betyr at $2^{10} \equiv 1 \equiv (-2)^5 \pmod{33}$. Med dette regner vi ut at

$$\begin{aligned} 101^{78} - 130^{33} &\equiv 2^{78} - (-2)^{33} \pmod{33} \\ &\equiv 2^5 2^3 (2^{10})^7 - (-2)^3((-2)^5)^6 \pmod{33} \\ &\equiv -2^3 - (-2)^3 \equiv -8 + 8 \equiv 0 \pmod{33} \end{aligned}$$

Altså er $101^{78} - 130^{33}$ delelig på 33. Vi kan også sjekke på samme måte at ingen av de andre er delelig på 33.

$\boxed{3}$ Hvilken av følgende lineære kongruenser har nøyaktig 3 løsninger som er parvis inkongruente modulo 33?

1. $11x \equiv 22 \pmod{33}$

2. $12x \equiv 21 \pmod{33}$

3. $11x \equiv 3 \pmod{33}$

4. $12x \equiv 22 \pmod{33}$

Løsning:
Den lineære kongruensen $ax \equiv b \pmod{n}$ er løsbar hvis og bare hvis $\gcd(a, n) \mid b$. I det tilfellet er antallet parvis inkongruente løsninger modulo n lik $\gcd(a, n)$. Følgelig er det eneste alternativet som har 3 parvis inkongruente løsninger $12x \equiv 21 \pmod{33}$, siden $\gcd(12, 33) = 3$.

$\boxed{4}$ Hvilket av følgende tall er siste siffer i $2^{10^{100}}$?

1. 2

2. 4

3. 6

4. 8

Løsning:
For å finne siste siffer må vi regne ut $2^{10^{100}}$ modulo 10. Vi begynner med å regne ut at $2^{10} \equiv 6 \pmod{10}$, og at $6^2 \equiv 6 \pmod{10}$. Ved induksjon ser vi at det siste betyr at $6^n \equiv 6 \pmod{10}$ for alle $n \geq 1$. Dermed kan vi regne ut at

$$2^{10^{100}} \equiv 2^{\overbrace{10 \cdot 10 \cdots 10}^{\text{100 ganger}}} \equiv (2^{10})^{10^{99}} \equiv 6^{10^{99}} \equiv 6 \pmod{10}$$

Altså er svaret at det siste sifferet i $2^{10^{100}}$ er 6.

$\boxed{5}$ Hva får vi til rest når vi deler $(-42) \cdot 69!$ på 71?

1. 27
2. 29
3. 42
4. 69

løsning:
Siden 71 er et primtall sier Wilsons teorem at $70! \equiv (-1) \pmod{71}$. Siden $70 \equiv -1 \pmod{71}$ betyr dette at $69! \equiv 1 \pmod{71}$. Dermed får vi at

$$(-42) \cdot 69! \equiv -42 \cdot 1 \equiv 29 \pmod{71}$$

Altså er svaret 29.