Øvingsforelesning 3

TMA4140 Diskret Matematikk

17. og 19. september 2018

"O store store O" og generell repetisjon

Dagen i dag

- Repetisjon av algoritmer, **store O**, og tallteori/kryptografi begynnelse
- **K15.5**: 3 ulike måter å "regne ut" store O på
- Liste med "standardfunksjoner" sortert etter vekstrate
- **MS15.10**: Store O
- **MS11.3**: Store O
- **K18.3**: Modulær aritmetikk/kongruenser

Algoritmer I

Definisjon

En algoritme er en endelig følge av presise instruksjoner for å gjennomføre en beregning eller for å løse et problem.

- Merk: ikke en "ekte" definisjon!

Algoritmer I

Definisjon

En algoritme er en endelig følge av presise instruksjoner for å gjennomføre en beregning eller for å løse et problem.

- Merk: ikke en "ekte" definisjon!
- Gir forhåpentligvis den riktige ideen

Algoritmer I

Definisjon

En algoritme er en endelig følge av presise instruksjoner for å gjennomføre en beregning eller for å løse et problem.

- Merk: ikke en "ekte" definisjon!
- Gir forhåpentligvis den riktige ideen
- Grådige algoritmer: disse forsøker i hvert steg å gjøre det "optimale" eller "beste" valget

Algoritmer II

Oppgave 52: Use the greedy algorithm to make change using quarters, dimes, nickels, and pennies for

a) 87 cents

b) 49 cents

c) 99 cents

d) 33 cents

Store O

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $O(g(x))$ hvis det finnes konstanter C og k slik at

$$|f(x)| \leq C|g(x)|$$

når $x > k$.

Eksempler:

- $f(x) = x^2 + 2x + 1$ er $O(x^2)$

Store O

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $O(g(x))$ hvis det finnes konstanter C og k slik at

$$|f(x)| \leq C|g(x)|$$

når $x > k$.

Eksempler:

- $f(x) = x^2 + 2x + 1$ er $O(x^2)$
- $f(x) = 5x^2$ er $O(x^3)$

Store O

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $O(g(x))$ hvis det finnes konstanter C og k slik at

$$|f(x)| \leq C|g(x)|$$

når $x > k$.

Eksempler:

- $f(x) = x^2 + 2x + 1$ er $O(x^2)$
- $f(x) = 5x^2$ er $O(x^3)$
- x^n er $O(x^m)$ hvis $n \leq m$ men ikke omvendt!
- Konkret eksempel: x er $O(x^2)$

Store Omega

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $\Omega(g(x))$ hvis det finnes **positive** konstanter C og k slik at

$$|f(x)| \geq C|g(x)|$$

når $x > k$.

- **Eksempel:** $f(x) = x^2 + 2x + 1$ er $\Omega(x^2)$

Store Omega

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $\Omega(g(x))$ hvis det finnes **positive** konstanter C og k slik at

$$|f(x)| \geq C|g(x)|$$

når $x > k$.

- **Eksempel:** $f(x) = x^2 + 2x + 1$ er $\Omega(x^2)$
- Hvis $f(x)$ er $(\Omega(g(x))$, hva annet kan vi si om f og g?

Store Omega

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $\Omega(g(x))$ hvis det finnes **positive** konstanter C og k slik at

$$|f(x)| \geq C|g(x)|$$

når $x > k$.

- **Eksempel:** $f(x) = x^2 + 2x + 1$ er $\Omega(x^2)$
- Hvis $f(x)$ er $(\Omega(g(x))$, hva annet kan vi si om f og g?
- $g(x)$ er $O(f(x))$!

Store Theta

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $\Theta(g(x))$ hvis $f(x)$ er $O(g(x))$ og $f(x)$ er $\Omega(g(x))$. Vi sier at $f(x)$ er av orden $g(x)$ og at f og g er av samme orden.

- Hvis $f(x)$ er $\Theta(g(x))$, hva annet kan vi si om de?

Store Theta

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $\Theta(g(x))$ hvis $f(x)$ er $O(g(x))$ og $f(x)$ er $\Omega(g(x))$. Vi sier at $f(x)$ er av orden $g(x)$ og at f og g er av samme orden.

- Hvis $f(x)$ er $\Theta(g(x))$, hva annet kan vi si om de?
- $g(x)$ er $\Theta(f(x))$!

Store Theta

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $\Theta(g(x))$ hvis $f(x)$ er $O(g(x))$ og $f(x)$ er $\Omega(g(x))$. Vi sier at $f(x)$ er av orden $g(x)$ og at f og g er av samme orden.

- Hvis $f(x)$ er $\Theta(g(x))$, hva annet kan vi si om de?
- $g(x)$ er $\Theta(f(x))$!
- $x^2 + 2x + 1$ er $\Theta(x^2)$

Store Theta

Definisjon

La f og g være funksjoner fra heltallene eller de reelle tallene til mengden av reelle tall. Vi sier at $f(x)$ er $\Theta(g(x))$ hvis $f(x)$ er $O(g(x))$ og $f(x)$ er $\Omega(g(x))$. Vi sier at $f(x)$ er av orden $g(x)$ og at f og g er av samme orden.

- Hvis $f(x)$ er $\Theta(g(x))$, hva annet kan vi si om de?
- $g(x)$ er $\Theta(f(x))$!
- $x^2 + 2x + 1$ er $\Theta(x^2)$
- $1 + 2 + 3 + \cdots + n - 1 + n$ er $\Theta(n^2)$

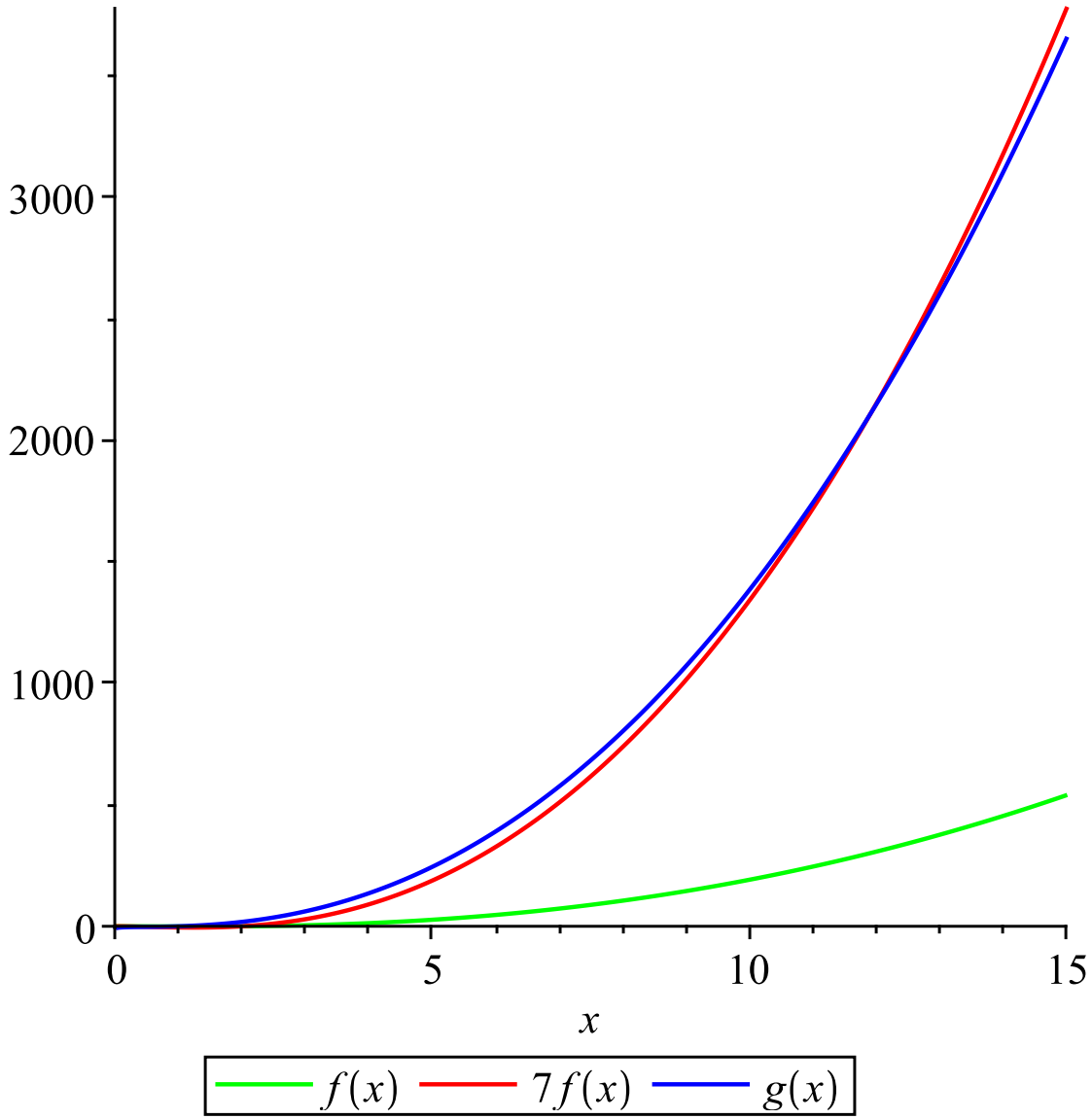
K15.5

La $f, g : \mathbb{R}^+ \to \mathbb{R}$ være definert ved

$$f(x) = (x^2 - 2x)\log(x+1)$$
$$g(x) = (3x^2 + 1)\log(x^2)$$

Vis at $f(x)$ er $\Theta(g(x))$.

K15.5



Grensemetoden

La $f, g : \mathbb{R}/\mathbb{R}^+/\mathbb{Z}/\mathbb{Z}^+ \to \mathbb{R}$ være funksjoner.

1. $\lim_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| = 0 \implies f(x)$ er $O(g(x))$, og $g(x)$ er *ikke* $O(f(x))$.

2. $\lim_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| = \infty \implies g(x)$ er $O(f(x))$, og $f(x)$ er *ikke* $O(g(x))$.

3. $\lim_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| = L$, der $0 < L < \infty \implies f(x)$ er $\Theta(g(x))$.

Teoremer

Teorem (2)

Hvis f_1 *er* $O(g_1)$, f_2 *er* $O(g_2)$ *og* g_1 *er* $O(g_2)$, *så er* $f_1 + f_2$ $O(g_2)$.

Teorem (3)

Hvis f_1 *er* $O(g_1)$ *og* f_2 *er* $O(g_2)$, *så er* $f_1 f_2$ $O(g_1 g_2)$.

Teorem (4)

$a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$ *er* $\Theta(x^k)$, *og*
$\log_b(a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k)$ *er* $\Theta(\log(x))$.

Liste av funksjoner

- **Viktige funksjoner**: $1, \log n, n, n \log n, n^2, n^3, \cdots, 2^n, n!$
  (Også: side 271.)

Liste av funksjoner

- **Viktige funksjoner**: $1, \log n, n, n \log n, n^2, n^3, \cdots, 2^n, n!$
  (Også: side 271.)
- **Merk:** Disse er sortert etter vekstrate/orden.

Liste av funksjoner

- **Viktige funksjoner**: $1, \log n, n, n \log n, n^2, n^3, \cdots, 2^n, n!$
  (Også: side 271.)
- **Merk:** Disse er sortert etter vekstrate/orden.
- Hvis du ikke kan kalkulus/analyse, tilbring litt tid med Wolfram Alpha eller noe annet som kan grafe funksjoner

Liste av funksjoner

- **Viktige funksjoner**: $1, \log n, n, n \log n, n^2, n^3, \cdots, 2^n, n!$
  (Også: side 271.)
- **Merk:** Disse er sortert etter vekstrate/orden.
- Hvis du ikke kan kalkulus/analyse, tilbring litt tid med Wolfram Alpha eller noe annet som kan grafe funksjoner
- Viktig å ha en intuitiv følelse for disse

Liste av funksjoner

- **Viktige funksjoner**: $1, \log n, n, n \log n, n^2, n^3, \cdots, 2^n, n!$
  (Også: side 271.)
- **Merk:** Disse er sortert etter vekstrate/orden.
- Hvis du ikke kan kalkulus/analyse, tilbring litt tid med Wolfram Alpha eller noe annet som kan grafe funksjoner
- Viktig å ha en intuitiv følelse for disse

MS15.10

La f betegne en funksjon fra $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ inn i $\mathbb{R}$. Hvilke av følgende utsagn er sanne?

Alt 1) $f(n) = 3n \log\left(\frac{n^2+n+1}{n+5}\right) \implies f(n)$ er $O(n\sqrt{n})$

Alt 2) $f(n) = n^2 \sin(n\pi) + n \implies f(n)$ er $O(n^3 \sin(n\pi))$

Alt 3) $f(n) = 7n^3 - n \log(n^2 + 1) \implies f(n)$ er $\Theta(n^3 + n^2)$

Alt 4) $f(n) = \frac{e^n}{n^2+1} \implies f(n)$ er $O(n^3 + n^2)$

MS15.10

La f betegne en funksjon fra $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ inn i $\mathbb{R}$. Hvilke av følgende utsagn er sanne?

Alt 1) $f(n) = 3n \log\left(\frac{n^2+n+1}{n+5}\right) \implies f(n)$ er $O(n\sqrt{n})$

Alt 2) $f(n) = n^2 \sin(n\pi) + n \implies f(n)$ er $O(n^3 \sin(n\pi))$

Alt 3) $f(n) = 7n^3 - n \log(n^2 + 1) \implies f(n)$ er $\Theta(n^3 + n^2)$

Alt 4) $f(n) = \frac{e^n}{n^2+1} \implies f(n)$ er $O(n^3 + n^2)$

MS15.10

La f betegne en funksjon fra $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ inn i $\mathbb{R}$. Hvilke av følgende utsagn er sanne?

Alt 1) $f(n) = 3n \log\left(\frac{n^2+n+1}{n+5}\right) \implies f(n)$ er $O(n\sqrt{n})$

Alt 2) $f(n) = n^2 \sin(n\pi) + n \implies f(n)$ er $O(n^3 \sin(n\pi))$

Alt 3) $f(n) = 7n^3 - n \log(n^2 + 1) \implies f(n)$ er $\Theta(n^3 + n^2)$

Alt 4) $f(n) = \frac{e^n}{n^2+1} \implies f(n)$ er $O(n^3 + n^2)$

MS15.10

La f betegne en funksjon fra $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ inn i $\mathbb{R}$. Hvilke av følgende utsagn er sanne?

Alt 1) $f(n) = 3n \log\left(\frac{n^2+n+1}{n+5}\right) \implies f(n)$ er $O(n\sqrt{n})$

Alt 2) $f(n) = n^2 \sin(n\pi) + n \implies f(n)$ er $O(n^3 \sin(n\pi))$

Alt 3) $f(n) = 7n^3 - n \log(n^2 + 1) \implies f(n)$ er $\Theta(n^3 + n^2)$

Alt 4) $f(n) = \frac{e^n}{n^2+1} \implies f(n)$ er $O(n^3 + n^2)$

MS11.3

La $f : \mathbb{R} \to \mathbb{R}$ være definert ved $f(x) = 3x^3 \sin^2 x + x^2$. Hvilke av følgende er riktig?

Alt 1) $f(x)$ er $O(x^2)$

Alt 2) $f(x)$ er $O(x^3|\sin x|)$

Alt 3) $f(x)$ er $O(x^3 - 2x^2)$

Alt 4) $f(x)$ er $\Theta(3x^3 - x^2)$

MS11.3

La $f : \mathbb{R} \to \mathbb{R}$ være definert ved $f(x) = 3x^3 \sin^2 x + x^2$. Hvilke av følgende er riktig?

Alt 1) $f(x)$ er $O(x^2)$

Alt 2) $f(x)$ er $O(x^3|\sin x|)$

Alt 3) $f(x)$ er $O(x^3 - 2x^2)$

Alt 4) $f(x)$ er $\Theta(3x^3 - x^2)$

MS11.3

La $f : \mathbb{R} \to \mathbb{R}$ være definert ved $f(x) = 3x^3 \sin^2 x + x^2$. Hvilke av følgende er riktig?

Alt 1) $f(x)$ er $O(x^2)$

Alt 2) $f(x)$ er $O(x^3|\sin x|)$

Alt 3) $f(x)$ er $O(x^3 - 2x^2)$

Alt 4) $f(x)$ er $\Theta(3x^3 - x^2)$

MS11.3

La $f : \mathbb{R} \to \mathbb{R}$ være definert ved $f(x) = 3x^3 \sin^2 x + x^2$. Hvilke av følgende er riktig?

Alt 1) $f(x)$ er $O(x^2)$

Alt 2) $f(x)$ er $O(x^3|\sin x|)$

Alt 3) $f(x)$ er $O(x^3 - 2x^2)$

Alt 4) $f(x)$ er $\Theta(3x^3 - x^2)$

Tallteori I

Definisjon

Hvis a og b er heltall med $a \neq 0$, sier vi at a deler b hvis det finnes et heltall c slik at $b = ac$, eller, ekvivalent, at $\frac{a}{b}$ er et heltall. Når a deler b sier vi at a er en faktor eller divisor av b, og at b er et multiplum av a.

Merk: Notasjonen $a|b$ uttrykker at a deler b.

- $57 = 19 \cdot 3$
- $19 \mid 57$
- $101 = 4 \cdot 24 + 5$
- $24 \nmid 101$

Tallteori I

Definisjon

Hvis a og b er heltall med $a \neq 0$, sier vi at a deler b hvis det finnes et heltall c slik at $b = ac$, eller, ekvivalent, at $\frac{a}{b}$ er et heltall. Når a deler b sier vi at a er en faktor eller divisor av b, og at b er et multiplum av a.

Merk: Notasjonen $a|b$ uttrykker at a deler b.

- $57 = 19 \cdot 3$
- $19 \mid 57$
- $101 = 4 \cdot 24 + 5$
- $24 \nmid 101$

Tallteori I

Definisjon

Hvis a og b er heltall med $a \neq 0$, sier vi at a deler b hvis det finnes et heltall c slik at $b = ac$, eller, ekvivalent, at $\frac{a}{b}$ er et heltall. Når a deler b sier vi at a er en faktor eller divisor av b, og at b er et multiplum av a.

Merk: Notasjonen $a|b$ uttrykker at a deler b.

- $57 = 19 \cdot 3$
- $19 \mid 57$
- $101 = 4 \cdot 24 + 5$
- $24 \nmid 101$

Tallteori I

Definisjon

Hvis a og b er heltall med $a \neq 0$, sier vi at a deler b hvis det finnes et heltall c slik at $b = ac$, eller, ekvivalent, at $\frac{a}{b}$ er et heltall. Når a deler b sier vi at a er en faktor eller divisor av b, og at b er et multiplum av a.

Merk: Notasjonen $a|b$ uttrykker at a deler b.

- $57 = 19 \cdot 3$
- $19 \mid 57$
- $101 = 4 \cdot 24 + 5$
- $24 \nmid 101$

Tallteori II

Theorem (Divisjonsalgoritmen)

La a være et heltall og d et positivt heltall. Da finnes det unike heltall q og r, med $0 \leq r < d$, slik at $a = dq + r$

Merk: Dette er ikke en algoritme!

Tallteori II

Theorem (Divisjonsalgoritmen)

La a være et heltall og d et positivt heltall. Da finnes det unike heltall q og r, med $0 \leq r < d$, slik at $a = dq + r$

Merk: Dette er ikke en algoritme!

Eksempler:

- $101 = 11 \cdot 9 + 2$
- $78 = 3 \cdot 25 + 3$
- $-11 = 3 \cdot (-4) + 1$

Theorem (Divisjonsalgoritmen)

La a være et heltall og d et positivt heltall. Da finnes det unike heltall q og r, med $0 \leq r < d$, slik at $a = dq + r$

Merk: Dette er ikke en algoritme!

Eksempler:

- $101 = 11 \cdot 9 + 2$
- $78 = 3 \cdot 25 + 3$
- $-11 = 3 \cdot (-4) + 1$

Tallteori II

Theorem (Divisjonsalgoritmen)

La a være et heltall og d et positivt heltall. Da finnes det unike heltall q og r, med $0 \leq r < d$, slik at $a = dq + r$

Merk: Dette er ikke en algoritme!

Eksempler:

- $101 = 11 \cdot 9 + 2$
- $78 = 3 \cdot 25 + 3$
- $-11 = 3 \cdot (-4) + 1$

Tallteori III

Theorem (Divisjonsalgoritmen)

La a være et heltall og d et positivt heltall. Da finnes det unike heltall q og r, med $0 \leq r < d$, slik at $a = dq + r$

Definisjon

I likningen ovenfor kaller vi d for divisoren, q for kvotienten og r for resten.

- $101 = 11 \cdot 9 + 2$ har kvotient 9 og rest 2 hvis vi lar 11 være divisoren.
- $-11 = 3 \cdot (-4) + 1$
- **Merk:** Per definisjon kan vi ikke ha negative divisorer og rest.
- Derfor **ikke**: $-11 = 3 \cdot (-3) - 2$ med "rest -2".

Tallteori III

Theorem (Divisjonsalgoritmen)

La a være et heltall og d et positivt heltall. Da finnes det unike heltall q og r, med $0 \leq r < d$, slik at $a = dq + r$

Definisjon

I likningen ovenfor kaller vi d for divisoren, q for kvotienten og r for resten.

- $101 = 11 \cdot 9 + 2$ har kvotient 9 og rest 2 hvis vi lar 11 være divisoren.
- $-11 = 3 \cdot (-4) + 1$
- **Merk:** Per definisjon kan vi ikke ha negative divisorer og rest.
- Derfor **ikke**: $-11 = 3 \cdot (-3) - 2$ med "rest -2".

Tallteori III

Theorem (Divisjonsalgoritmen)

La a være et heltall og d et positivt heltall. Da finnes det unike heltall q og r, med $0 \leq r < d$, slik at $a = dq + r$

Definisjon

I likningen ovenfor kaller vi d for divisoren, q for kvotienten og r for resten.

- $101 = 11 \cdot 9 + 2$ har kvotient 9 og rest 2 hvis vi lar 11 være divisoren.
- $-11 = 3 \cdot (-4) + 1$
- **Merk:** Per definisjon kan vi ikke ha negative divisorer og rest.
- Derfor **ikke**: $-11 = 3 \cdot (-3) - 2$ med "rest -2".

Tallteori III

Theorem (Divisjonsalgoritmen)

La a være et heltall og d et positivt heltall. Da finnes det unike heltall q og r, med $0 \leq r < d$, slik at $a = dq + r$

Definisjon

I likningen ovenfor kaller vi d for divisoren, q for kvotienten og r for resten.

- $101 = 11 \cdot 9 + 2$ har kvotient 9 og rest 2 hvis vi lar 11 være divisoren.
- $-11 = 3 \cdot (-4) + 1$
- **Merk:** Per definisjon kan vi ikke ha negative divisorer og rest.
- Derfor **ikke**: $-11 = 3 \cdot (-3) - 2$ med "rest -2".

Modulær aritmetikk I

Definisjon

Hvis a og b er heltall og m er et positivt heltall, da er a kongruent til b modulo m hvis m deler $a - b$, altså $m \mid a - b$. Vi bruker notasjonen

$$a \equiv b \mod m$$

for å indikere at a er kongruent til b modulo m.
Vi kaller $a \equiv b \mod m$ for en kongruens og m er dens modulus.

Eksempler:

- $17 \equiv 5 \mod 6$
- $24 \not\equiv 14 \mod 6$
- $101 \equiv 2 \mod 9$
- Også: $101 \equiv 11 \mod 9$ siden $101 - 10 \cdot 9 = 11$

Modulær aritmetikk I

Definisjon

Hvis a og b er heltall og m er et positivt heltall, da er a kongruent til b modulo m hvis m deler $a - b$, altså $m \mid a - b$. Vi bruker notasjonen

$$a \equiv b \mod m$$

for å indikere at a er kongruent til b modulo m.
Vi kaller $a \equiv b \mod m$ for en kongruens og m er dens modulus.

Eksempler:

- $17 \equiv 5 \mod 6$
- $24 \not\equiv 14 \mod 6$
- $101 \equiv 2 \mod 9$
- Også: $101 \equiv 11 \mod 9$ siden $101 - 10 \cdot 9 = 11$

Modulær aritmetikk I

Definisjon

Hvis a og b er heltall og m er et positivt heltall, da er a kongruent til b modulo m hvis m deler $a - b$, altså $m \mid a - b$. Vi bruker notasjonen

$$a \equiv b \mod m$$

for å indikere at a er kongruent til b modulo m.
Vi kaller $a \equiv b \mod m$ for en kongruens og m er dens modulus.

Eksempler:

- $17 \equiv 5 \mod 6$
- $24 \not\equiv 14 \mod 6$
- $101 \equiv 2 \mod 9$
- Også: $101 \equiv 11 \mod 9$ siden $101 - 10 \cdot 9 = 11$

Modulær aritmetikk I

Definisjon

Hvis a og b er heltall og m er et positivt heltall, da er a kongruent til b modulo m hvis m deler $a - b$, altså $m \mid a - b$. Vi bruker notasjonen

$$a \equiv b \mod m$$

for å indikere at a er kongruent til b modulo m.
Vi kaller $a \equiv b \mod m$ for en kongruens og m er dens modulus.

Eksempler:

- $17 \equiv 5 \mod 6$
- $24 \not\equiv 14 \mod 6$
- $101 \equiv 2 \mod 9$
- Også: $101 \equiv 11 \mod 9$ siden $101 - 10 \cdot 9 = 11$

Modulær aritmetikk I

Definisjon

Hvis a og b er heltall og m er et positivt heltall, da er a kongruent til b modulo m hvis m deler $a - b$, altså $m \mid a - b$. Vi bruker notasjonen

$$a \equiv b \mod m$$

for å indikere at a er kongruent til b modulo m.
Vi kaller $a \equiv b \mod m$ for en kongruens og m er dens modulus.

Eksempler:

- $17 \equiv 5 \mod 6$
- $24 \not\equiv 14 \mod 6$
- $101 \equiv 2 \mod 9$
- Også: $101 \equiv 11 \mod 9$ siden $101 - 10 \cdot 9 = 11$

Modulær aritmetikk II

Theorem

La m være et positivt heltall. Hvis $a \equiv b \mod m$ og $c \equiv d \mod m$, så har vi

$$a + c \equiv b + d \mod m$$

og

$$ac \equiv bd \mod m.$$

Eksempler:

- $100^{100} \equiv 1^{100} \equiv 1 \mod 99$
- $101 \equiv 2 \mod 9$
- $396 \equiv 0 \mod 9$
- $427 \equiv 9 \mod 11$

Modulær aritmetikk II

Theorem

La m være et positivt heltall. Hvis $a \equiv b \mod m$ og $c \equiv d \mod m$, så har vi

$$a + c \equiv b + d \mod m$$

og

$$ac \equiv bd \mod m.$$

Eksempler:

- $100^{100} \equiv 1^{100} \equiv 1 \mod 99$
- $101 \equiv 2 \mod 9$
- $396 \equiv 0 \mod 9$
- $427 \equiv 9 \mod 11$

Modulær aritmetikk II

Theorem

La m være et positivt heltall. Hvis $a \equiv b \mod m$ og $c \equiv d \mod m$, så har vi

$$a + c \equiv b + d \mod m$$

og

$$ac \equiv bd \mod m.$$

Eksempler:

- $100^{100} \equiv 1^{100} \equiv 1 \mod 99$
- $101 \equiv 2 \mod 9$
- $396 \equiv 0 \mod 9$
- $427 \equiv 9 \mod 11$

Modulær aritmetikk II

Theorem

La m være et positivt heltall. Hvis $a \equiv b \mod m$ og $c \equiv d \mod m$, så har vi

$$a + c \equiv b + d \mod m$$

og

$$ac \equiv bd \mod m.$$

Eksempler:

- $100^{100} \equiv 1^{100} \equiv 1 \mod 99$
- $101 \equiv 2 \mod 9$
- $396 \equiv 0 \mod 9$
- $427 \equiv 9 \mod 11$

K18, Oppgave 3

a Finn $1 \leq x < 59$ slik at

$$x \equiv 58^{5745} \mod 59.$$

Forklar din fremgangsmåte.

b Finn $1 \leq x < 30$ slik at

$$x \equiv 32^{30} \mod 30.$$

Forklar din fremgangsmåte.

K18, Oppgave 3

a Finn $1 \leq x < 59$ slik at

$$x \equiv 58^{5745} \mod 59.$$

Forklar din fremgangsmåte.

b Finn $1 \leq x < 30$ slik at

$$x \equiv 32^{30} \mod 30.$$

Forklar din fremgangsmåte.