# Tallteori

Astrid Mysterud

August 2023

# Introduksjon

## Hva er tallteori?

Læren om heltallene, ofte de naturlige tallene.

## Notasjon og mengder

| | |
|---|---|
| $\in$ | Er element i |
| $\subset$ | Er delmengde (subset) av |
| $\Longrightarrow$ | Implikasjon |
| $\Longleftrightarrow$ | Ekvivalens |
| $\setminus$ | Differanse (for mengder) |
| $\cap$ | Snitt |
| $\cup$ | Union |
| $\forall$ | For alle/hver |
| $\exists$ | Det eksisterer |
| $\emptyset$ | Den tomme mengden |
| $\mathbb{N} = \{1, 2, 3, \ldots\}$ | De naturlige tallene |
| $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ | Heltallene |
| $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ | De rasjonale tallene |
| $\mathbb{R}$ | De reelle tallene. Inkluderer både rasjonale og irrasjonale tall. Eksempler: $-\pi$, $-\frac{1}{5}$, 0, 1, $\sqrt{2}$ |
| $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$ | De komplekse tallene |

Mengde ("set" på engelsk): Samling av ulike objekter. Objektene i en mengde kalles elementer.

**Eksempler.** La $A = \{1, 2, 4, 8, 16\}$, $B = \{0, 1, 2, 3, 5, 8\}$ og $C = \{2, 4, 16\}$.

$8 \in A$, 8 er element i $A$

$C \subset A$, siden alle elementer i $C$ er i $A$

$A \setminus C = \{1, 8\}$, $\setminus$ trekker fra elementene felles for $A$ og $C$

$A \cap B = \{1, 2, 8\}$, elementene som er i $A$ og $B$

$A \cup B = \{0, 1, 2, 3, 4, 5, 8, 16\}$, elementene som er i $A$ eller $B$

# Primtall og aritmetikkens fundamentalteorem

Et primtall er et naturlig tall større enn 1, som bare er delelig med seg selv og 1.

Et sammensatt tall er et naturlig tall større enn 1, som ikke er et primtall.

**Aritmetikkens fundamentalteorem**

Ethvert naturlig tall større enn 1 kan skrives som et entydig produkt av primtall.

## Telle divisorer

La $n \in \mathbb{N}$ ha primtallsfaktoriseringen $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$, altså er $p_i$ primtall. En divisor $d$ av $n$ er et heltall på formen $d = p_1^{a_1} \cdot p_2^{a_2} \cdots p_m^{a_m}$ hvor $0 \leq a_i \leq k_i$. Ved bruk av litt kombinatorikk kan vi telle antall divisorer $n$ har. For hver eksponent $a_i$ har vi $k_i + 1$ mulige eksponenter å velge mellom, altså 0, 1, 2, ..., $k_i$. Antall divisorer blir da $\prod_{i=1}^{m}(k_i + 1) = (k_1 + 1)(k_2 + 1) \cdots (k_m + 1)$.

**Eksempel.** $24 = 2^3 \cdot 3$ har $4 \cdot 2 = 8$ divisorer, nemlig 1, 2, 3, 4, 6, 8, 12, 24.

**Oppgave (Abelkonkurransen 21/22).** Hvor mange positive heltall som deler 10! er ikke kvadrattall?

# Delelighet

**Definisjon.** La $a, b \in \mathbb{Z}$. Vi sier at $b$ deler $a$, skrives $b \mid a$, dersom det eksisterer et heltall $n$ slik at $a = n \cdot b$.

**Oppgaver.** Hvis du skjønner greia er det unødvendig å gjøre alle, men anbefaler uansett å gjøre iii og vi. Tenk over hvordan man beviser noe utifra en definisjon.

La $a$, $b$, $c$, $d \in \mathbb{Z}$. Vis at

(i) $1 \mid a$

(ii) $a \mid 1 \implies a = \pm 1$

(iii) $a \mid b$ og $b \mid c \implies a \mid c$

(iv) $ab \mid c \implies a \mid c$ og $b \mid c$

(v) $a \mid b$ og $c \mid d \implies ac \mid bd$

(vi) $a \mid b$ og $a \mid c \implies a \mid xb + yc \ \forall\, x, y \in \mathbb{Z}$

# Største felles divisor (GCD)

**Definisjon.** Den største felles divisor (GCD, "greatest common divisor") for $x, y \in \mathbb{N}$ er den største $d \in \mathbb{N}$ slik at $d \mid x$ og $d \mid y$. Da skriver vi $\gcd(x, y) = d$.

Dersom $\gcd(x, y) = 1$ sier vi at $x$ og $y$ er *relativt primske* ("coprime").

Følgende gjelder for gcd.

- $\gcd(1, x) = 1$
- $\gcd(x, 0) = x$
- $\gcd(x, y) = \gcd(x, y + mx)$, $m \in \mathbb{Z}$

## Euklids algoritme

Euklids algoritme bruker nederste punkt ovenfor for å finne største felles faktor for to tall.

**Eksempel.**

$$\begin{aligned}\gcd(45, 260) &= \gcd(45, 35 + 5 \cdot 45) = \gcd(35, 45) \\ &= \gcd(35, 10 + 1 \cdot 35) = \gcd(10, 35) \\ &= \gcd(10, 5 + 3 \cdot 10) = \gcd(5, 10) \\ &= \gcd(5, 0 + 2 \cdot 5) = \gcd(0, 5) = 5\end{aligned}$$

**Oppgave.** Finn $\gcd(84, 132)$.

# Minste felles multilpum (LCM)

**Definisjon.** Det minste felles multiplum (LCM, "lowest common multiple") for $x, y \in \mathbb{N}$ er den minste $n \in \mathbb{N}$ slik at $x \mid n$ og $y \mid n$. Da skriver vi $\operatorname{lcm}(x, y) = n$.

## Nyttig sammenheng mellom GCD og LCM

**Teorem.** $\gcd(x, y) \cdot \operatorname{lcm}(x, y) = x \cdot y$.

# Modulo-regning

Vi sier at to heltall $a$ og $b$ er kongruente modulo $n$, dersom $n$ deler differansen deres. Det vil si at $a$ og $b$ er kongruente modulo $n$, dersom det eksisterer et heltall $k$ slik at $a - b = kn$, altså $n \mid (a - b)$.

Dersom $a$ og $b$ er kongruente modulo $n$ skriver vi $a \equiv b \pmod{n}$.

**Eksempel.** $18 \equiv 4 \mod 7$, siden $18 - 4 = 14 = 2 \cdot 7$.
$27 \equiv 0 \mod 3$, siden $27 - 0 = 27 = 9 \cdot 3$.

## Kongruensklasser

$a$ og $b$ er kongruente dersom de har samme rest når de deles på $n$. Vi samler kongruente tall i det vi kaller kongruensklasser. For eksempel vil tall som har 3 i rest når de deles på 4 være i kongruensklassen $\overline{3}$ (kan også skrives $[3]_4$). Vi kaller mengden kongruensklasser modulo $n$ for $\mathbb{Z}_n$, altså $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. I motsetning til $\mathbb{Z}$, som har uendelig antall elementer, har $\mathbb{Z}_n$ kun $n$ elementer. Enkelte operasjoner blir dermed mer oversiktlige i $\mathbb{Z}_n$ enn i $\mathbb{Z}$.

Her er det masse annet spennende man kan lese om, blant annet algebraiske strukturer som ringer og kropper, primitive røtter, Eulers totientfunksjon og mye mer. Wikipedia kan heldigvis masse om dette:)

## Addisjon

- $a + b = c \implies a \pmod{n} + b \pmod{n} \equiv c \pmod{n}$
- $a \equiv b \implies a + c \equiv b + c \pmod{n}$
- $a \equiv b \pmod{n}$ og $c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$

## Multiplikasjon

- $a \cdot b = c \implies a \pmod{n} \cdot b \pmod{n} \equiv c \pmod{n}$
- $a \equiv b \pmod{n} \implies ka \equiv kb \pmod{n}$
- $a \equiv b \pmod{n}$ og $c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$
- $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$ for $k \in \mathbb{N}$

## Oppgaver

1. Hva blir resten når $57 + 231 + 1 + 89 + 1149 + 25$ deles på 3?

2. Anta at klokka er 14:00, hva er klokka om 1000 timer?

3. Hva blir resten når $7 \cdot 328 \cdot 53 \cdot 71$ deles på 6?

4. Hva blir resten når $44 \cdot 739 \cdot 77 \cdot 5 \cdot 65$ deles på 7?

5. Hva er det siste sifferet i $67^{67}$?

6. Hva blir resten når $1! + 2! + 3! + \cdots + 60!$ deles på $6!$ ?

7. La $n \in \mathbb{N}$. Finn største mulige verdi av $\gcd(5n + 6,\ 8n + 7)$.

8. La $a$, $x \in \mathbb{N}$ større enn 2. Gitt at $a^x \equiv a - 2 \pmod{a - 1}$. Hva er verdien av $a$?

9. Hvilket heltall $n \geq 5$ løser følgende kongruenssystem?

$$n^3 - 3n + 7 \equiv 0 \pmod{n - 5}$$
$$2n^2 - n + 2 \equiv 0 \pmod{n + 6}$$

10. **Abelfinalen 21/22 P1a.** Bestem alle positive heltall $n$ som er slik at $2022 + 3^n$ er et kvadrattall.

11. **Abelfinalen 22/23 P3a.** Finn alle ikkenegative heltall $n$, $a$ og $b$ slik at $2^a + 5^b + 1 = n!$.

12. Vis at det finnes uendelig mange tall som ikke kan skrives som sum av to kvadrattall.

13. **MA1301 eksamen.** Vis at $\gcd(7t + 2,\ 4t + 1) = 1$ for alle $t$.

14. La $p$ være et primtall. Vis at dersom et produkt i $\mathbb{Z}_p$ er 0, må en av faktorene være 0. Altså for $x$, $y \in \mathbb{Z}$ som er slik at $x \not\equiv 0 \pmod{p}$ og $y \not\equiv 0 \pmod{p}$, så er $xy \not\equiv 0 \pmod{p}$.

# Teoremer

## Det kinesiske restteoremet

Gitt parvise relativt primske positive heltall $n_1, \ldots, n_k$ og heltall $a_1, \ldots, a_k$, har kongruenssystemet

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

en løsning, og løsningen er unik modulo $N = n_1 n_2 \cdots n_k$.

**Oppgave.** Løs kongruenssystemet

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

## Fermats lille teorem

Hvis $a$ er et heltall, $p$ er et primtall og $p \nmid a$, så er

$$a^{p-1} \equiv 1 \pmod{p}$$

**Oppgave.** Regn ut $3^{31} \pmod 7$ og $29^{25} \pmod{11}$.

## Wilsons teorem

Et positivt heltall $n$ er et primtall hvis og bare hvis

$$(n-1)! \equiv -1 \pmod{n}$$

**Oppgave (Abelfinalen 21/22 P1b).** Finn alle primtall $p$ og positive heltall $n$ som er slik at

$$n\, 5^{n-n/p} = p!\,(p^2+1) + n$$

**Fasit for oppgave 1-11.** 1) 1, 2) 06:00, 3) 4, 4) 0, 5) 3, 6) 153, 7) 13, 8) 3, 9) 14, 10) $n = 1$, 11) $a = 2$, $b = 0$, $n = 3$

**Kilder**


- wikipedia.com
- brilliant.com
- matematikksenteret.no/konkurranser/abelkonkurransen
- artofproblemsolving.com/wiki