

**Z:** De hele tallene, dvs.  $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ .

$a|b$  (a går opp i b): Hvis  $a$  og  $b$  er hele tall med  $a \neq 0$ , sier vi at  $a$  går opp i  $b$  (a **divides**  $b$ ) hvis det finnes et helt tall  $c$  slik at  $b = ac$ . Notasjon:  $a|b$  leses som "a går opp i b", mens  $a \nmid b$  leses som "a går ikke opp i b".

**Synonymer til "går opp i":** Når  $a|b$ , sier vi at

- $a$  er en **faktor** i  $b$ ,
- $b$  er et **multiplum av**  $a$ ,
- $b$  er **delelig med**  $a$ .

**Teorem:** La  $a$ ,  $b$  og  $c$  være hele tall. Da har vi følgende:

1. Hvis  $a|b$  og  $a|c$ , så vil  $a|(b+c)$ .
2. Hvis  $a|b$ , så vil  $a|bc$  for alle hele tall  $c$ .
3. Hvis  $a|b$  og  $b|c$ , så vil  $a|c$ .
4. Hvis  $a|1$ , så er  $a = \pm 1$ .
5. Hvis  $a|b$  og  $b|a$ , så er  $a = \pm b$ .
6. Ethvert helt tall  $b \neq 0$  går opp i 0.
7. Hvis  $b|g$  og  $b|h$ , så vil  $b|(mg+nh)$  for alle hele tall  $m$  og  $n$ .

1

**Største felles divisor:** La  $a$  og  $b$  være hele tall, ikke begge lik 0. Det største hele tallet  $d$  slik at  $d|a$  og  $d|b$ , kalles for den største felles divisor (**greatest common divisor**) til  $a$  og  $b$ . Notasjon:  $\gcd(a, b)$ .

**Relativt primiske:** De hele tallene  $a$  og  $b$  er relativt primiske (**relatively prime**) hvis deres største felles divisor er 1.

**Parvis relativt primiske:** De hele tallene  $a_1, a_2, \dots, a_n$  er parvis relativt primiske (**pairwise relatively prime**) hvis  $\gcd(a_i, a_j) = 1$  for alle  $i$  og  $j$  slik at  $1 \leq i < j \leq n$ .

**Teorem:** La  $m$  og  $n$  være to positive hele tall.

1. Hvis  $k = mn$ , så vil  $k_p = m_p + n_p$  for alle primtall  $p$ .
2. Hvis  $m|n$ , så vil  $m_p \leq n_p$  for alle primtall  $p$ .
3. Hvis  $k = \gcd(a, b)$ , så er  $k_p = \min(a_p, b_p)$  for alle primtall  $p$ .

3

**Primtall:** Et positivt helt tall  $p > 1$  kalles et primtall (**prime number**) hvis de eneste positive faktorene til  $p$  er 1 og  $p$ .

**Sammensatt tall:** Et positivt helt tall som ikke er et primtall, kalles for et sammensatt tall (**composite number**).

**Aritmetikkens fundamentalsetning:** Ethvert positivt helt tall kan skrives som et entydig produkt av primtall når primfaktorene skrives i økende rekkefølge. La  $P$  være mengden av alle primtall. Da kan ethvert positivt helt tall  $a$  skrives entydig på følgende form:

$$a = \prod_P p^{a_p} \quad \text{hvor hver} \quad a_p \geq 0.$$

(NB! Merk at  $a_p = 0$  for alle primtall  $p$  som ikke er faktor i  $a$ .)

**Setning:** Hvis  $n$  er et sammensatt helt tall, har  $n$  en primfaktor  $\leq \sqrt{n}$ .

2

**Gulvfunksjonen:** Funksjonen  $[x]$  kalles for **gulvet (the floor)** til  $x$ , og tilordner det største hele tallet  $\leq x$  til  $x$ .

**Divisjonsalgoritmen:** La  $a$  være et helt tall og  $d$  et positivt helt tall. Da finnes det entydige hele tall  $q$  og  $r$  med  $0 \leq r < d$  slik at  $a = dq + r$ . Tallet  $a$  kalles **dividenden (the dividend)**,  $d$  kalles **divisoren (the divisor)**,  $q$  kalles **kvotienten (the quotient)**, og  $r$  kalles **resten (the remainder / the residue)**. Vi har at  $q = \left\lfloor \frac{a}{d} \right\rfloor$ .

**a mod m:** La  $a$  være et helt tall, og la  $m$  være et positivt helt tall. Da betegner symbolet  $a \bmod m$  resten når  $a$  deles med  $m$ .

4

**Kongruent modulo  $m$ :** Hvis  $a$  og  $b$  er hele tall, og  $m$  er et positivt heltall, sier vi at  $a$  er kongruent med  $b$  modulo  $m$  hvis  $a \bmod m = b \bmod m$ . Notasjon:  $a \equiv b \pmod{m}$  leses som "a er kongruent med b modulo m", mens  $a \not\equiv b \pmod{m}$  leses som "a er ikke kongruent med b modulo m".

**Setning:** La  $m$  være et positivt heltall, og la  $a$  og  $b$  være hele tall. Da er følgende utsagn ekvivalente:

- $a \equiv b \pmod{m}$ .
- $a \bmod m = b \bmod m$ .
- Det finnes et heltall  $k$  slik at  $a = b + km$ .
- $m \mid (a - b)$ .

**Egenskaper til  $a \equiv b \pmod{m}$ :**

- Hvis  $a \equiv b \pmod{m}$ , så er  $b \equiv a \pmod{m}$ .
- Hvis  $a \equiv b \pmod{m}$  og  $b \equiv c \pmod{m}$ , så er  $a \equiv c \pmod{m}$ .

5

**Fermat's lille teorem:** Hvis  $p$  er et primtall og  $a$  er et heltall slik at  $p \neq a$ , så er  $a^{p-1} \equiv 1 \pmod{p}$ . For alle hele tall  $a$  har vi at  $a^p \equiv a \pmod{p}$ .

**Euler's totient funksjon:**  $\phi(n)$  er antallet positive heltall som er  $< n$  og relativt primisk med  $n$ . Hvis  $n = pq$  hvor  $p$  og  $q$  er to primtall, så er  $\phi(n) = (p-1)(q-1)$ .

**Euler's teorem:** Hvis  $m$  er et positivt heltall og  $a$  er et heltall slik at  $a$  og  $m$  er relativt primiske, så er  $a^{\phi(m)} \equiv 1 \pmod{m}$ .

7

## Regneregler for modular aritmetikk:

Regler for addisjon, subtraksjon og multiplikasjon i mengden  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ :  
 $[(a \bmod n) \pm (b \bmod n)] \bmod n = (a \pm b) \bmod n$ .  
 $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$ .

**Setning:** La  $a, b, c$  og  $d$  være hele tall, og la  $m$  være et positivt heltall. Hvis  $a \equiv b \pmod{m}$  og  $c \equiv d \pmod{m}$ , så er  $a + c \equiv b + d \pmod{m}$  og  $ac \equiv bd \pmod{m}$ .

**Setning:** La  $m$  være et positivt heltall, og la  $a, b$  og  $c$  være hele tall. Hvis  $ac \equiv bc \pmod{m}$  og  $\gcd(c, m) = 1$ , da er  $a \equiv b \pmod{m}$ .

**Multiplikativ invers:** La  $a$  og  $m > 1$  være hele tall. Tallet  $a^{-1}$  sies å være en (multiplikativ) invers til  $a$  modulo  $m$  hvis  $a^{-1} \cdot a \equiv 1 \pmod{m}$ .

**Setning:** Hvis  $a$  og  $m$  er hele tall slik at  $m > 1$  og  $\gcd(a, m) = 1$ , så finnes det en invers til  $a$  modulo  $m$ , og denne inversen er entydig modulo  $m$ .

6

**Setning:** Hvis  $p$  er et odde primtall, så har likningen  $x^2 \equiv 1 \pmod{p}$  kun to løsninger, nemlig  $x \equiv 1 \pmod{p}$  og  $x \equiv -1 \pmod{p}$ .

Den kontrapositive versjonen av denne setningen, gir oss en primtallstest:

**Primtallstest:** La  $x$  og  $n$  være hele tall slik at  $n > 0$ . Hvis likningen  $x^2 \equiv 1 \pmod{n}$  har andre løsninger enn  $x \equiv 1 \pmod{n}$  og  $x \equiv -1 \pmod{n}$ , så er  $n$  et sammensatt tall.

Den kontrapositive versjone av Fermat's lille teorem gir oss også en primtallstest:

**Primtallstest:** La  $a$  og  $n$  være positive hele tall slik at  $n \neq a$ . Hvis  $a^{n-1} \not\equiv 1 \pmod{n}$ , så er  $n$  et sammensatt tall.

Disse primtallstestene kan kombineres i algoritmen WITNESS (side 222).

8

**Setning:** La  $a = bq + r$  hvor  $a$ ,  $b$ ,  $q$  og  $r$  er hele tall. Da er  $\gcd(a, b) = \gcd(b, r)$ .

**Euklids algoritme:** En algoritme for å beregne største felles divisor ved å bruke divisjonsalgoritmen og resultatet  $\gcd(a, b) = \gcd(b, r)$  gjentatte ganger.

**Setning:** Hvis  $a$  og  $b$  er positive hele tall, så finnes det hele tall  $s$  og  $t$  slik at  $\gcd(a, b) = sa + tb$ . **Den utvidete Euklidske algoritmen** finner også tallene  $s$  og  $t$  i tillegg til  $\gcd(a, b)$ .

**Setning:** Hvis  $a$ ,  $b$  og  $c$  er positive hele tall slik at  $\gcd(a, b) = 1$  og  $a|bc$ , da må  $a|c$ .

**Setning:** Hvis  $p$  er et primtall og  $p|a_1 a_2 \dots a_n$  hvor hver  $a_i$  er et helt tall, da må  $p|a_i$  for en eller annen  $i$ .

9

**Orden:** La  $a$  og  $n$  være relativt primiske positive hele tall. Da kaller vi det minste positive hele tallet slik at  $a^x \equiv 1 \pmod{n}$  for ordenen **(the order)** til  $a$  modulo  $n$ .

**Setning:** Hvis  $a$  og  $n$  er relativt primiske hele tall med  $n > 0$ , så er det positive hele tallet  $x$  en løsning av kongruensen  $a^x \equiv 1 \pmod{n}$  hvis og bare hvis  $\text{ord}_n a \mid x$ . Spesielt må  $\text{ord}_n a \mid \phi(n)$ .

**Setning:** Hvis  $a$  og  $n$  er relativt primiske hele tall med  $n > 0$ , så er  $a^i \equiv a^j \pmod{n}$  hvor  $i$  og  $j$  er ikkenegative hele tall hvis og bare hvis  $i \equiv j \pmod{\text{ord}_n a}$ .

11

La  $\mathbf{Z}_n = \{0, 1, 2, \dots, n-1\}$ , og la  $\mathbf{Z}_n^* = \{a \mid 1 \leq a \leq n-1 \text{ og } \gcd(a, n) = 1\}$ . Mengden  $\mathbf{Z}_n^*$  kalles for den multiplikative gruppen til  $\mathbf{Z}_n$  og har  $\phi(n)$  elementer.

**Primitiv rot:** Et tall  $a \in \mathbf{Z}_n^*$  som har den egenskapen at potensene  $a, a^2, a^3, \dots, a^{\phi(n)}$  utgjør hele  $\mathbf{Z}_n^*$ , kalles for en primitiv rot (**primitive root**) til  $n$ . Vi sier også at  $a$  er en **generator** for  $\mathbf{Z}_n^*$ .

**Setning:** Bare hele tall som kan skrives på formen  $2, 4, p^r$  og  $2p^r$  hvor  $r$  er et positivt helt tall, og  $p$  er et odde primtall, har en primitiv rot.

10

**Indeks:** La  $n$  være et positivt helt tall med primitiv rot  $r$ . Hvis  $a$  er et positivt helt tall slik at  $\gcd(a, n) = 1$ , så kaller vi det entydige hele tallet  $x$  slik at  $1 \leq x \leq \phi(n)$  og  $r^x \equiv a \pmod{n}$  for indeksen til  $a$  med grunntall  $r$  modulo  $n$ . Vi skriver  $a \equiv r^{\text{ind}_{r,n} a} \pmod{n}$ .

**Regneregler for indekser:**

- $\text{ind}_{r,n} 1 = 0 \pmod{\phi(n)}$ .
- $\text{ind}_{r,n} r = 1 \pmod{\phi(n)}$ .
- $\text{ind}_{r,n}(xy) = [\text{ind}_{r,n}(x) + \text{ind}_{r,n}(y)] \pmod{\phi(n)}$ .
- $\text{ind}_{r,n}(y^k) = [k \cdot \text{ind}_{r,n}(y)] \pmod{\phi(n)}$ .

På grunn av likheten mellom indekser og logaritmer, kaller vi ofte indekser for **diskrete logaritmer**.

12

## Diskret-logaritme-problemet:

Betrakt likningen  $y = g^x \pmod p$ .

Hvis  $y$ ,  $g$  og  $p$  er gitt, er det (generelt) vanskelig å finne  $x$  om  $p$  er et svært stort primtall. Tidskompleksiteten for den beste algoritmen til å beregne den diskrete logaritmen er gitt ved:

$$e^{(\ln p)^{\frac{1}{3}}(\ln(\ln p))^{\frac{2}{3}}}.$$