Hvordan avgjøre om et heltall $a > 1$ er et primtall?

Regel Hvis $a > 1$ ikke er et primtall, så må det finnes et primtall $p \leq \lfloor \sqrt{a} \rfloor$ som går opp i a.

Eksempel 1 Er 101 et primtall?

$\lfloor \sqrt{101} \rfloor = 10$. Det holder derfor å undersøke om 2, 3, 5 eller 7 går opp i 101. Hvis ingen av dem går opp, er 101 et primtall.

Vi finner fort at ingen av dem går opp. Dermed er 101 et primtall.

Eksempel 2 Er 1001 primtall?

$\lfloor \sqrt{1001} \rfloor = 31$. Vi må prøve med 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. Vi ser at hverken 2, 3 eller 5 går opp. Men 7 går opp siden $1001 = 7 \cdot 143$.

Setning Det finnes uendelig mange primtall.

Bevis: Anta det motsatte, dvs. at det er endelig mange primtall. La de hete $p_1, p_2, p_3, \ldots\ldots p_n$. La $a = p_1 \cdot p_2 \cdot p_3 \cdot \cdots p_n + 1$. Da kan ikke a være primtall. Dermed må det finnes en i slik at p_i går opp i a. Dermed må også p_i gå opp i 1 siden $1 = a - p_1 \cdot p_2 \cdots p_n$. Umulig!

Eratosthenes sil (eng: sieve)

Vi kan finne primtall ved å sette opp alle tallene og så fortløpende fjerne de som 2 går opp, 3 går opp i, osv.

Eksempel Tallene fra 1 til 100

(2)	(3)	~~4~~	(5)	~~6~~	(7)	~~8~~	~~9~~	~~10~~
(11)	~~12~~	(13)	~~14~~	~~15~~	~~16~~	(17)	~~18~~	(19)	~~20~~
~~21~~	~~22~~	(23)	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	(29)	~~30~~
(31)	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	(37)	~~38~~	~~39~~	~~40~~
(41)	~~42~~	(43)	~~44~~	~~45~~	~~46~~	(47)	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	(53)	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	(59)	~~60~~
(61)	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	(67)	~~68~~	~~69~~	~~70~~
(71)	~~72~~	(73)	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	(79)	~~80~~
~~81~~	~~82~~	(83)	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	(89)	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	(97)	~~98~~	~~99~~	~~100~~

De som ikke er fjernet (de som er ringet inn) er primtall. Det er 25 stykker.

Største felles divisor (eng: greatest common divisor)

La a og b være to hele tall der ikke begge er 0. Største felles divisor for a og b er det største heltallet som går opp i både a og b. Dette betegnes ofte med $\gcd(a,b)$.

OBS $\gcd(a,b)$ er alltid et positivt tall.

Eksempel Hva er største felles divisor for 18 og 42?

$18 = 2 \cdot 3 \cdot 3$, $42 = 2 \cdot 3 \cdot 7$ Vi ser at både 2 og 3 går opp i begge. Dermed blir $\gcd(18,42) = 2 \cdot 3 = 6$.

Metode som finner hvor mange primtall det er fra 1 til n. Du må ha import java.util.*; hvis metoden skal brukes:

```
public static int antallPrimtall(int n)
{
  if (n < 2) return 0;

  BitSet sammensatt = new BitSet(n + 1);

    for (int k = 3; k*k <= n; k += 2)
    {
      if (!sammensatt.get(k))
        for (int i = k * k; i <= n; i += 2*k)
          sammensatt.set(i);
    }

  return (n+1)/2 - sammensatt.cardinality();
}
```

gcd ved hjelp av primfallsfaktorisering

Finn primfallsfaktoriseringen til a og b. Da vil gcd(a,b) vare produktet av de primfallsfaktorene som går opp i både a og b. Hvis et primtall p forekommer m ganger i a og n ganger i b, så tas det med så mange som den minste av m og n.

Eksempler 1) $a = 2 \cdot 3^2 \cdot 5 \cdot 7^3 \cdot 11 \quad b = 2^3 \cdot 3 \cdot 7$

$$\gcd(a,b) = 2 \cdot 3 \cdot 7$$

2) $a = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \quad b = 2^2 \cdot 3^4 \cdot 5 \cdot 7^2$

$$\gcd(a,b) = 2^2 \cdot 3^2 \cdot 5 \cdot 7$$

gcd ved hjelp av Euklids algoritme

Husk definisjonen av kvotient og rest:
Hvis a og b er to hele tall med $b>0$, så finnes entydige hele tall q og r slik at

$$a = q \cdot b + r \quad , \quad 0 \le r < b$$

Setning La $b>0$. Da er $\gcd(a,b) = \gcd(b,r)$.

Bevis La c være et heltall som går opp i både a og b. Vi har $r = a - qb$. Dermed vil c gå opp i r. Omvendt: La c være et heltall som går opp i både b og r. Da vil c gå opp i a siden $a = qb + r$.

Enkelt eksempel $a = 42$, $b = 18$

Skjema for Euklids algoritme →

a	b	r
42	18	6
18	6	0

Når resten har blitt 0, er det som står nederst i b-kolonnen lik $\gcd(a,b)$.

Litt større eksempel $a = 740$, $b = 420$

a	b	r
740	420	320
420	320	100
320	100	20
100	20	0

Vi får $\gcd(740, 420) = 20$

Javakode for Euklids algoritme:

```
public static int euklid(int a, int b)
{
  while (b > 0)
  {
    int r = a % b;
    a = b;
    b = r;
  }
  return a;
}
```

Relativt primiske tall

To hele tall a og b (der ikke begge er 0) kalles relativt primiske hvis $\gcd(a,b) = 1$.

Eksempel $a = 40$, $b = 21$

Siden $\gcd(a,b) = 1$, er a og b relativt primiske.

Parvis relativt primiske tall

Tre eller flere heltall kalles parvis relativt primiske hvis to og to av dem er relativt primiske.

Eksempel $a = 21$, $b = 22$, $c = 25$

$\gcd(a,b) = 1$, $\gcd(b,c) = 1$, $\gcd(a,c) = 1$.

Tallene 21, 22 og 25 er parvis relativt primiske.

Minste felles multiplum (eng: least common multiple)

Minste felles multiplum for to hele tall a og b er det minste positive heltallet som både a og b går opp.

Setning La $a > 0$ og $b > 0$. $ab = \gcd(a,b) \cdot \text{lcm}(a,b)$