

## TALTEORI

### Primfaktoropløsning og divisorer.

Disse noter forudsætter et grundlæggende kendskab til talteori som man kan få i Marianne Terps og Peter Trosborgs noter om talteori.

Noterne vil primært introducere forskellige opgaveteknikker hvor man skal se på primfaktoropløsning og divisorer.

## 1 Primfaktoropløsning

Ifølge aritmetikkens fundamentalsætning kan ethvert naturligt tal større end 1 primfaktoropløses på entydig måde, og dette er grundlaget for hele talteorien.

### 1.1 Sætning

Et naturligt tal  $n$  større end 1 med primfaktoropløsning

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

har  $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_m)$  forskellige divisorer.

**BEVIS.** Enhver divisor i  $n$  er på formen

$$p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m},$$

hvor  $\beta_i \in \{0, 1, \dots, \alpha_i\}$ . Dermed har  $n$  i alt  $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_m)$  forskellige divisorer.

### 1.2 Eksempel

Denne sætning medfører eksempelvis at samtlige tal med netop  $p$  divisorer hvor  $p$  er et primtal, netop er alle  $(p-1)$ 'te potenser af primtal.

### 1.3 Opgave

Et naturligt tal  $n$ , som højst er 500, har den egenskab at når man vælger et tal  $m$  tilfældigt blandt tallene  $1, 2, 3, \dots, 499, 500$ , så er sandsynligheden  $\frac{1}{100}$  for at  $m$  går op i  $n$ . Bestem den største mulige værdi af  $n$ . (Georg Mohr-Konkurrencen 2006)

### 1.4 Opgave

Lad  $n$  være produktet af samtlige tal mindre end en million med præcis 9 divisorer. Vis at  $n$  er et kvadrattal.

## 2 Divisorer

I mange typer opgaver kan det betale sig at se på hvilke mulige divisorer et udtryk kan have eller finde største fælles divisor for to udtryk.

## 2.1 Eksempel

I dette eksempel vil vi vise at hvis  $a, b, c$  og  $d$  er naturlige tal således at  $ab = cd$ , da er  $a^n + b^n + c^n + d^n$  et sammensat tal for alle naturlige tal  $n$ . Når vi skal vise at  $a^n + b^n + c^n + d^n$  er sammensat, skal vi gerne kunne faktorisere udtrykket, og derfor ønsker vi at se på hvilke fælles faktorer  $a, b, c$  og  $d$  har. Da  $ab = cd$ , kan vi se at en primdivisor i  $a$  også er divisor i  $c$  eller  $d$ . Dette udnytter vi til at indse at der findes naturlige tal  $r, s, u$  og  $v$  så  $a = ru$ ,  $b = sv$ ,  $c = rs$  og  $d = uv$ . Nu har vi klarlagt sammenhængen mellem de fire tal og kan derfor faktorisere:

$$a^n + b^n + c^n + d^n = r^n u^n + s^n v^n + r^n s^n + u^n v^n = (r^n + v^n)(s^n + u^n).$$

Da begge faktorer er større end 1 for alle naturlige tal  $n$ , er  $a^n + b^n + c^n + d^n$  et sammensat tal.

## 2.2 Opgave

Om tre naturlige tal  $a, b$  og  $c$  gælder at  $a$  er ulige, og at  $a, b$  og  $c$  ikke har en fælles divisor større end 1. Desuden er

$$\frac{2}{a} + \frac{1}{b} = \frac{1}{c}.$$

Bevis at  $abc$  er et kvadrattal.

## 2.3 Største fælles divisor

Den største fælles divisor og regnereglerne for den kan fx benyttes til at vise at brøken  $\frac{n^2+n-1}{n^2+2n}$  er uforkortelig for alle naturlige tal  $n$ , da dette er ensbetydende med at største fælles divisor mellem tæller og nævner er 1. Der gælder som bekendt følgende regneregler for den største fælles divisor

$$\gcd(a, b) = \gcd(a, b - ma), m \in \mathbb{Z}.$$

Dermed er

$$\begin{aligned} \gcd(n^2 + n - 1, n^2 + 2n) &= \gcd(n^2 + n - 1, n^2 + 2n - (n^2 + n - 1)) = \gcd(n^2 + n - 1, n + 1) = \\ &= \gcd(n^2 + n - 1 - n(n + 1), n + 1) = \gcd(-1, n + 1) = 1. \end{aligned}$$

## 2.4 Opgave

Vis at brøken

$$\frac{n^3 + 2n}{n^4 + 3n^2 + 1}$$

er uforkortelig for alle hele tal  $n$ .

## 2.5 Opgave

Lad  $a_n = n^2 + 500$  og  $g(n) = \gcd(a_n, a_{n+1})$ . Vis at  $g$  er en begrænset funktion, og bestem den største værdi af  $g$ .

## 2.6 Eksempel

Nu skal vi se et eksempel på hvordan man også i forbindelse med at bestemme største fælles divisor kan benytte moduloregning.

Lad  $a, m$  og  $n$  være naturlige tal, hvor  $m$  er ulige, og  $x > 1$ .

Vi vil nu bestemme  $\gcd(a^m - 1, a^n + 1)$ .

Sæt  $\gcd(a^m - 1, a^n + 1) = d$ . I stedet for at forsøge at reducere dette udtryk regner vi  $a^{nm}$  modulo  $d$  på to forskellige måder da det kan give os informationer om  $d$ .

$$a^{nm} = (a^m)^n \equiv 1^n \equiv 1 \pmod{d}.$$

Desuden er

$$a^{nm} = (a^n)^m \equiv (-1)^m \equiv -1 \pmod{d}.$$

Dermed er  $d = 2$  når  $a$  er ulige, og  $d = 1$  når  $a$  er lige.

## 2.7 Opgave

Bestem samtlige naturlige tal  $n, m > 2$  for hvilke  $2^n - 1$  går op i  $2^m + 1$ .

## 3 Potenser af heltal som divisorer

Når divisorerne er potenser af heltal, kan man udnytte dette.

### 3.1 Eksempel

I dette eksempel skal vi se på hvordan man udnytter at en potens af et helt tal er divisor i et produkt. Hvis vi ser på ligningen

$$x(x + 1) = y^n,$$

kan vi se at hvis der findes en heltallig løsning, da må både  $x$  og  $x + 1$  være  $n$ 'te potenser af et helt tal da to på hinanden følgende hele tal ikke har nogen fælles divisorer. Men da må  $1 = x + 1 - x = b^n - a^n$  hvilket ikke kan lade sig gøre når  $n > 1$ .

Vi udnytter altså her at to på hinanden følgende tal ikke har nogen fælles divisorer, til at indse at ligningen ikke har nogen heltallige løsninger. I det hele taget kan man udnytte at fælles divisorer for  $n$  og  $n + a$  også er divisorer i  $a$ .

### 3.2 Opgave

Vis at ligningen

$$x^3 + 3 = 4y(y + 1)$$

ikke har nogen heltallige løsninger.

### 3.3 Opgave

For hvilke naturlige tal  $m$  og  $n$ , hvor  $m$  er ulige, er  $m^n + 1$  et kvadrattal?

### 3.4 Opgave

Vis at der ikke findes naturlige tal  $x, y$  og  $n, n > 1$ , for hvilke

$$x(x+1)(x+2) = y^n.$$

#### Bemærkning

Generelt gælder at  $k$  på hinanden følgende tal,  $k > 1$ , aldrig er en  $n$ 'te potens af et helt tal, når  $n > 1$ .

### 3.5 Opgave

Bestem alle naturlige tal  $n$  for hvilke  $n2^{n-1} + 1$  er et kvadrattal.

### 3.6 Opgave

Bestem alle par  $x$  og  $y$  af hele tal for hvilke

$$1 + 2^x + 2^{2x+1} = y^2.$$

(IMO 2006)

## 4 Løsninger

**Opgave 1.3** Hvis sandsynligheden er  $\frac{1}{100}$  for at et tilfældigt valgt tal  $m$  blandt tallene  $1, 2, 3, \dots, 499, 500$  går op i  $n$ , må  $n$  have præcis 5 divisorer. Et tal med primfaktoropløsning  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i}$  har  $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_i)$  divisorer, dvs.  $n = p^4$  for et primtal  $p$ . Det største mulige  $n$  med den ønskede egenskab er derfor  $n = 3^4 = 81$ , da  $5^4 > 500$ .

**Opgave 1.4** Tal med netop  $3^2$  divisorer må ifølge sætning 1.1 være på formen  $p^8$  eller  $p^2 q^2$  hvor  $p$  og  $q$  er primtal. Et sådant tal er derfor altid et kvadrattal, og produktet af sådanne tal er derfor også et kvadrattal.

**Opgave 2.2** Af ligningen ses at  $2bc + ac = ba$ . Da  $a$  er ulige, må  $a|bc$ ,  $b|ac$  og  $c|ab$ . Dermed findes naturlige tal  $u, v$  og  $w$ , så  $au = bc$ ,  $bv = ac$  og  $cw = ab$ . Af dette får vi

$$a^2 = vw, \quad b^2 = uw, \quad c^2 = uv. \quad **)$$

Vi vil nu vise at  $\gcd(u, v) = \gcd(u, w) = \gcd(v, w) = 1$ . Lad  $p$  være en primdivisor i  $u$ . Af \*\*) ses nu at  $p$  også er primdivisor i  $b$  og  $c$ , og dermed ikke i  $a$  da  $a, b$  og  $c$  ikke har nogen fælles divisorer. Da  $a^2 = vw$ , går  $p$  heller ikke op i  $v$  og  $w$ . På denne måde ses at  $\gcd(u, v) = \gcd(u, w) = \gcd(v, w) = 1$ .

Vi har nu at  $a^2 = uv$  og  $\gcd(u, v) = 1$ . Dermed må  $u$  og  $v$  være kvadrattal. Tilsvarende ses at  $w$  er et kvadrattal. Da  $abc = uvw$ , må  $abc$  være et kvadrattal.

**Opgave 2.4** Brøken er uforkortelig når største fælles divisor for nævner og tæller er 1.

$$\gcd(n^4 + 3n^2 + 1, n^3 + 2n) = \gcd(n^2 + 1, n^3 + 2n) = \gcd(n^2 + 1, n) = \gcd(1, n) = 1.$$

**Opgave 2.5** Først finder vi et udtryk for  $g(n)$  der viser at  $g$  er begrænset.

$$g(n) = \gcd(n^2 + 500, n^2 + 2n + 1 + 500) = \gcd(n^2 + 500, 2n + 1).$$

Da  $2n + 1$  er ulige, ændrer det ikke ved den største fælles divisor at gange det første tal med 2. Derfor får vi at

$$\begin{aligned} g(n) &= \gcd(2n^2 + 1000, 2n + 1) = \gcd(1000 - n, 2n + 1) = \\ &= \gcd(2000 - 2n, 2n + 1) = \gcd(2001, 2n + 1). \end{aligned}$$

Heraf ses at  $g$  altid er divisor i 2001, og da  $g(1000) = 2001$  er det også den maksimale værdi for  $g$ .

**Opgave 2.7** Sæt  $m = dn + r$ ,  $0 \leq r < n$ . Da er

$$2^m + 1 = 2^{dn+r} + 1 = (2^n)^{d2^r} + 1 \equiv 1^{d2^r} + 1 \equiv 2^r + 1 \pmod{2^n - 1}.$$

Da  $n > r$ , er der ingen naturlige tal  $m, n > 2$  som opfylder betingelserne.

**Opgave 3.2** Ved omrokering får vi

$$x^3 = 4y^2 + 4y - 3 = (2y + 1)^2 - 4 = (2y - 1)(2y + 3).$$

Da  $\gcd(2y - 1, 2y + 3) = \gcd(2y - 1, 4) = 1$ , er både  $2y - 1$  og  $2y + 3$  kubiktal, men der findes ikke to kubiktal hvis forskel er 4. Dermed har ligningen ingen heltallige løsninger.

**Opgave 3.3** Hvis  $m^n + 1$  er et kvadrattal, findes et naturligt tal  $x$  så

$$m^n = x^2 - 1 = (x - 1)(x + 1).$$

Da  $m$  er ulige, er  $x$  lige, dvs. at  $\gcd(x - 1, x + 1) = 1$ . Dermed findes to naturlige tal  $a$  og  $b$  således at  $x - 1 = a^n$  og  $x + 1 = b^n$ . Men da er  $2 = (x + 1) - (x - 1) = b^n - a^n$ , hvilket giver at  $n = 1$ .

Tallet  $m^n + 1$  er dermed et kvadrattal, når  $n = 1$  og  $m = (2k - 1)^2 - 1$  for alle  $k \in \mathbb{N}$ .

**Opgave 3.4** Antag at der findes en løsning, og sæt  $w = x + 1$ . Da er

$$y^n = (w - 1)w(w + 1) = w(w^2 - 1).$$

Da  $\gcd(w, w^2 - 1) = 1$ , findes naturlige tal  $a$  og  $b$  således at  $w = a^n$  og  $w^2 - 1 = b^n$ . Dermed er  $1 = w^2 - (w^2 - 1) = (a^2)^n - b^n$ , hvilket er en modstrid da  $n > 1$ .

**Opgave 3.5** Ved at tjekke  $n = 1, 2, 3, 4, 5, 6$  indses at blandt disse opfylder kun  $n = 5$  det ønskede.

Vi viser indirekte at der ikke er flere  $n$  der opfylder betingelsen.

Antag at  $n > 6$ , og at  $m^2 = n2^{n-1} + 1$ . Da er

$$(m + 1)(m - 1) = n2^{n-1},$$

dvs. at  $2^{n-2} | m + 1 \vee 2^{n-2} | m - 1$ . Dermed er  $m \geq 2^{n-2} - 1$ , og

$$m^2 \geq (2^{n-2} - 1)^2 > 2^{2n-5} \geq n2^{n-1} + 1 = m^2,$$

da  $2^{n-4} > n$  når  $n > 6$ . Men dette er en modstrid.

**Opgave 3.6** Det er indlysende at der ikke er nogle løsninger for  $x < 0$ , og for  $x = 0$  er der to løsninger  $(0, 2)$  og  $(0, -2)$ .

Antag at  $x > 0$ . Hvis  $(x, y)$  er en løsning, da er også  $(x, -y)$  en løsning, og derfor kan vi antage at også  $y > 0$ . Vi omskriver nu ligningen til

$$2^x(1 + 2^{x+1}) = (y - 1)(y + 1),$$

hvilket viser at  $y$  er ulige. Da netop en af faktorerne  $y - 1$  og  $y + 1$  er delelig med 4, får vi at  $x > 2$ , samt at en af faktorerne er delelig med  $2^{x-1}$ .

Sæt nu

$$y = 2^{x-1}m + \epsilon, \text{ hvor } m \text{ er ulige, og } \epsilon = \pm 1.$$

Når vi indsætter dette i ligningen, får vi

$$2^x(1 + 2^{x+1}) = (2^{x-1}m + \epsilon)^2 - 1 = 2^{2x-2}m^2 + 2^x m \epsilon,$$

eller ækvivalent

$$1 + 2^{x+1} = 2^{x-2}m^2 + m\epsilon.$$

Derfor er

$$1 - \epsilon m = 2^{x-2}(m^2 - 8).$$

Hvis  $\epsilon = 1$ , må  $m^2 - 8 \leq 0$ , hvilket giver  $m = 1$ . Dermed er  $1 - 1 = 2^{x-2}(1 - 8)$  hvilket er umuligt.

Hvis  $\epsilon = -1$ , må

$$1 + m = 2^{x-2}(m^2 - 8) \geq 2(m^2 - 8),$$

dvs. at  $2m^2 - m - 17 \leq 0$ . Dette giver at  $m = 1$  eller  $m = 3$ . Det er igen nemt at se at  $m = 1$  ikke er en løsning. Hvis  $m = 3$ , får vi at  $x = 4$ , dvs. at  $y = 23$ , og disse værdier opfylder den oprindelige ligning.

Dermed er samtlige løsninger  $(0, 2)$ ,  $(0, -2)$ ,  $(4, 23)$  og  $(4, -23)$ .