

## TALTEORI

### Wilson's sætning og Euler-Fermats sætning.

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 divisorer eller benytte Wilson's sætning eller Euler-Fermats sætning.

## 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  $x, m$  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 findes er 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 Wilson's sætning

I Marianne Terps og Peter Trosborgs noter om talteori er Wilson's sætning bevist så her refererer vi den blot.

### 4.1 Wilson's sætning

For ethvert primtal  $p$  gælder

$$(p-1)! \equiv -1 \pmod{p}.$$

### 4.2 Eksempel

Wilson's sætning kan bl.a. benyttes til at vise at hvis  $p$  er et primtal som har rest 1 ved division med 4, da er  $-1$  kvadratisk rest modulo  $p$ , dvs. at ligningen  $x^2 \equiv -1 \pmod{p}$  har en løsning.

Lad nemlig  $p$  være et primtal på formen  $p = 4m + 1$ . Ifølge Wilson's sætning gælder

$$-1 \equiv (p-1)! \equiv 1 \cdot 2 \cdot \dots \cdot 2m \cdot (-2m) \cdot \dots \cdot (-2) \cdot (-1) \equiv ((2m)!)^2 \pmod{p}.$$

Dvs. at  $((2m)!)^2 \equiv -1 \pmod{p}$ , og dermed ses at  $-1$  er kvadratisk rest modulo  $p$ . Senere skal vi se at  $-1$  ikke er kvadratisk rest modulo primtal på formen  $4m + 3$ .

### 4.3 Opgave

Bestem samtlige naturlige tal  $n$  for hvilke  $n$  går op i  $(n-1)! + 1$ .

### 4.4 Opgave

Er det muligt at dele en mængde bestående af ti på hinanden følgende naturlige tal i to disjunkte delmængder, som samlet indeholder alle ti tal, således at produktet af elementerne i hver af de to delmængder bliver det samme tal?

## 5 Euler-Fermats sætning

I talteori opgaver hvor der indgår potenser, kan det være en hjælp at kende Euler-Fermats sætning. Sætningen er bevist i Marianne Terps og Peter Trosborgs noter om talteori så her refererer vi den blot.

### 5.1 Euler-Fermat

Lad  $n$  være et naturligt tal, og  $a$  et helt tal således at  $(a, n) = 1$ . Da gælder

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

### 5.2 Fermats lille sætning

Fermats lille sætning er et specialtilfælde af Euler-Fermat:

For et primtal  $p$  og et helt tal  $a$  hvor  $(p, a) = 1$ , gælder

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

### 5.3 Eksempel

Euler-Fermats sætning kan bl.a. benyttes til at reducere potensen hvis man fx ønsker at udregne  $6^{162} \pmod{25}$ . Da  $\phi(25) = \phi(5^2) = (5-1)5 = 20$ , er  $6^{162} = 6^2(6^{20})^8 \equiv 6^2 \equiv 11 \pmod{25}$ .

### 5.4 Inverse elementer

Hvis  $a$  og  $n$  er to indbyrdes primiske hele tal, da kan Euler-Fermats sætning benyttes til at konstruere en invers til  $a \pmod{n}$ . En invers til  $a$  er et helt tal  $a^{-1}$  som opfylder  $a \cdot a^{-1} \equiv 1 \pmod{n}$ . Ifølge Euler-Fermats sætning er  $a^{\phi(n)-1}$  en invers til  $a$  da  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

### 5.5 Sætning

Lad  $(a, n) = 1$ , og antag at  $a^m \equiv 1 \pmod{n}$ . Da gælder at

$$a^{(\phi(n), m)} \equiv 1 \pmod{n}.$$

**BEVIS:** Den største fælles divisor af to tal kan altid skrives som en linearkombination af tallene, dvs. der findes hele tal  $s$  og  $t$  så  $(\phi(n), m) = s\phi(n) + tm$ . Dermed er

$$a^{(\phi(n), m)} = a^{s\phi(n) + tm} = (a^{\phi(n)})^s (a^m)^t \equiv 1 \pmod{n}.$$

### 5.6 Eksempel

Findes der et helt tal  $n$  hvis cifre er lutter 1-taller således at  $n$  er delelig med 1999? Ja, det kan man benytte Euler-Fermats sætning til at vise. Da 1999 er et primtal, er  $\phi(1999) = 1998$ . Der gælder nu at

$$10^{1998} \equiv 1 \pmod{1999}.$$

Dermed går 1999 op i  $10^{1998} - 1 = 9 \cdot \underbrace{1111111 \dots 111}_{1998}$ , og da  $(1999, 9) = 1$ , må 1999 gå op

i  $\underbrace{1111111 \dots 111}_{1998}$ .

Opgaven kan faktisk også løses alene ved brug af skuffeprincippet og simple overvejelser om rester.

### 5.7 Opgave

Vis at hvis  $m$  er et naturligt tal der ikke er delelig med 2, 3 eller 5, da findes et helt tal  $n$  hvis cifre er lutter 1-taller således at  $n$  er delelig med  $m$ .

### 5.8 Opgave

Lad  $a$  og  $n$  være to indbyrdes primiske hele tal. Vis at hvis  $m$  er det mindste naturlige tal så

$$a^m \equiv 1 \pmod{n},$$

da er  $m$  divisor i  $\phi(n)$ .

### 5.9 Opgave

Lad  $m$  være et ulige naturligt tal, og betragt følgen  $a_0 = m$  og  $a_n = 2a_{n-1} + 1$  for  $n \in \mathbb{N}$ . Vis at der findes uendeligt mange tal i følgen som er delelige med  $m$ .

### 5.10 Opgave

Antag at  $n, k \geq 2$  er to naturlige tal.

Vis at da er mindst et af tallene  $p = n + k^n$  og  $q = nk^{(k^n-1)} + 1$  ikke et primtal.

### 5.11 Opgave

Bestem alle naturlige tal  $n$ , således at  $3^n + 1$  er delelig med  $n^2$ . (Baltic Way 2006)

## 6 Primtal på formen $p = 4m + 3$

Primtal af formen  $p = 4m + 1$  og primtal af formen  $p = 4m + 3$  har forskellige egenskaber, og her vil vi se på et par af disse.

### 6.1 Sætning

Der gælder at  $-1$  er kvadratisk rest modulo primtal på formen  $p = 4m + 1$ , mens  $-1$  ikke er kvadratisk rest modulo primtal på formen  $p = 4m + 3$ .

**BEVIS:** Vi har tidligere sæt at  $-1$  er kvadratisk rest modulo primtal  $p$  på formen  $p = 4m + 1$ . Antag nu at der findes et helt tal  $x$  så  $x^2 \equiv -1 \pmod{p}$ , hvor  $p = 4m + 3$ . Dette giver at

$$x^{4m+2} = (x^2)^{2m+1} \equiv (-1)^{2m+1} \equiv -1 \pmod{p},$$

men ifølge Euler-Fermat er  $x^{4m+2} \equiv 1 \pmod{p}$ , hvilket er en modstrid.

### 6.2 Sætning

Lad  $p$  være et primtal på formen  $p = 4m + 3$ . Hvis  $p$  går op i summen af to kvadrattal  $a^2 + b^2$ , da går  $p$  op i både  $a$  og  $b$ .

**BEVIS:** Antag at  $a^2 + b^2 \equiv 0 \pmod{p}$ , og at  $a$  ikke er delelig med  $p$ . Da findes en invers  $a^{-1}$  til  $a$  modulo  $p$ , og dermed har vi

$$a^2(a^{-1})^2 + b^2(a^{-1})^2 \equiv 0 \pmod{p}.$$

Dette giver

$$1 + (ba^{-1})^2 \equiv 0 \pmod{p},$$

hvilket er en modstrid da  $-1$  ikke er kvadratisk rest modulo  $p$ . Derfor må  $p$  gå op i  $a$  og dermed også i  $b$ .

### 6.3 Korollar

Et specialtilfælde af sætningen er at et primtal  $p$  på formen  $p = 4m + 3$  ikke kan skrives som sum af to kvadrattal. Primtal på formen  $p = 4m + 1$  kan derimod altid skrives som sum af to kvadrattal, og det skal vi se nærmere på om lidt.

### 6.4 Opgave

Om et helt tal  $n$  oplyses at  $n$  er kvadrattal, og at samtlige primfaktorer i  $n$  er på formen  $4m + 3$ . (At et tal er kvadrattal betyder at alle primtal i primfaktoropløsningen indgår i 1. potens.)

Vis at  $n$  ikke kan skrives som sum af to kvadrattal.

### 6.5 Opgave

Vis at  $n^2 + 3$  ikke er et kubiktal for noget naturligt tal  $n$ . (Vink: Udnyt ovenstående teori samt at  $m^3 + 1 = (m + 1)(m^2 - m + 1)$ .)

For at bevise at primtal på formen  $p = 4m + 1$  kan skrives som sum af to kvadrater, har vi brug for følgende sætning.

### 6.6 Thues sætning

Lad  $n$  være et helt tal større end 1, og lad  $k$  være det mindste hele tal så  $k > \sqrt{n}$ , dvs. at  $k - 1 \leq \sqrt{n}$ .

Antag at  $a$  er et tal som er primisk med  $n$ . Da findes hele tal  $x$  og  $y$ ,  $x, y \in \{1, 2, \dots, k - 1\}$ , så

$$ay \equiv x \pmod{n} \text{ eller } ay \equiv -x \pmod{n}.$$

#### BEVIS.

Betragt alle tal på formen  $ay' + x'$  hvor  $x', y' \in \{0, 1, 2, \dots, k - 1\}$ . Da der er  $k^2 > n$  par  $x', y'$ , findes ifølge skuffeprincippet mindst to par så  $ax' + y'$  har samme rest modulo  $n$ . Der findes altså  $x_1, x_2, y_1, y_2 \in \{0, 1, 2, \dots, k - 1\}$ , så  $a(y_1 - y_2) \equiv x_2 - x_1 \pmod{n}$ , hvor  $x_1 \neq x_2$  eller  $y_1 \neq y_2$ .

Antag at  $x_1 = x_2$ . Da vil  $n$  gå op i  $a(y_1 - y_2)$ , og da  $(a, n) = 1$  vil  $n$  gå op i  $y_1 - y_2$ , dvs.  $y_1 = y_2$  da  $y_1, y_2 \in \{0, 1, 2, \dots, k - 1\}$ . Hvis vi antager at  $y_1 = y_2$ , får vi tilsvarende at  $x_1 = x_2$ . Dermed er

$$0 < |x_1 - x_2|, |y_1 - y_2| \leq k - 1.$$

Sæt nu  $y = |y_1 - y_2|$  og  $x = |x_1 - x_2|$ . Da er

$$ay \equiv x \pmod{n} \text{ eller } ay \equiv -x \pmod{n}.$$

### 6.7 Opgave

Lad  $p$  være et primtal på formen  $p = 4m + 1$ . Udnyt Thues sætning samt at  $-1$  er kvadratisk rest modulo  $p$ , til at vise at  $p$  kan skrives som sum af to kvadrater.

## **6.8 Opgave**

Hvilke positive hele tal  $n$  kan skrives som sum af to kvadrater? (Bemærk at nul også regnes for et kvadrat)