

# 1 Talteori

Talteori er læren om de hele tal, og her spiller primtallene en helt central rolle. I de første afsnit introduceres grundlæggende teori om delelighed, primtal, antallet af divisorer, største fælles divisor og ikke mindst restklasser. I de senere afsnit introduceres mere avanceret teori som Eulers  $\phi$ -funktion, Fermats lille sætning, Eulers sætning, den kinesiske restklassesætning og flere sætninger om primtal. Kapitlet kræver ikke forhåndskendskab til talteori, men introducerer alle begreber. Man skal dog være forberedt på at niveauet vokser meget hurtigt, og at der er mange udfordrende opgaver undervejs.

## Indhold

<b>1 Talteori</b>	<b>1</b>
1.1 Delelighed, primtal og primfaktoropløsning . . . . .	1
1.2 Omskrivning vha. kvadratsætninger . . . . .	4
1.3 Antal divisorer . . . . .	6
1.4 Største fælles divisor og Euklids algoritme . . . . .	7
1.5 Restklasser . . . . .	10
1.6 Restklasseregning og kvadratiske rester . . . . .	13
1.7 Nyttige faktoriseringer . . . . .	15
1.8 Primiske rester og Eulers $\phi$ -funktion . . . . .	17
1.9 Wilsons sætning . . . . .	20
1.10 Fermats lille sætning og Eulers sætning . . . . .	21
1.11 Orden . . . . .	23
1.12 Følger . . . . .	25
1.13 Den kinesiske restklassesætning . . . . .	27
1.14 Mere om divisorer . . . . .	28
1.15 Den $p$ -adiske valuation . . . . .	30
1.16 Summer af to kvadrattal . . . . .	32
1.17 Primtallenes forunderlige verden . . . . .	34
1.18 Den kvadratiske reciprocitetssætning . . . . .	35
<b>2 Hints</b>	<b>38</b>
<b>3 Løsninger</b>	<b>39</b>
<b>Stikordsregister</b>	<b>62</b>

## 1.1 Delelighed, primtal og primfaktoropløsning

### Definition af delelighed, divisor og multiplum

Lad  $d$  og  $n$  være hele tal. Vi siger at  $d$  er *divisor* i  $n$ , eller at  $d$  *går op* i  $n$ , hvis der findes et helt tal  $q$  så

$$n = q \cdot d.$$

At  $d$  er divisor i  $n$ , skrives  $d \mid n$ . Når  $d$  er divisor i  $n$ , siger vi at  $n$  er *delelig* med  $d$ , og at  $n$  er et *multiplum* af  $d$ .

Fx er 12 delelig med tallene 1, 2, 3, 4, 6 og 12, og disse er netop samtlige positive divisorer i 12. Tallene  $-26$ ,  $0$ ,  $39$  og  $130$  er alle multipla af 13.

*Opgave 1.1.1.* Bestem samtlige positive divisorer i 60 og samtlige positive divisorer i 98.

### Sætning 1.1.1. Delelighedsregler

Lad  $a, b, c \in \mathbb{Z}$ .

1. Hvis  $a \mid b$  og  $b \mid c$ , da vil  $a \mid c$ .
2. Hvis  $a \mid b$ , da vil  $a \mid b \cdot c$ .
3. Hvis  $a \mid b$  og  $a \mid c$ , da vil  $a \mid b + c$  og  $a \mid b - c$ .

**Bevis.** 1. At  $a \mid b$  betyder at der findes et helt tal  $q_1$  så  $a \cdot q_1 = b$ . At  $b \mid c$  betyder at der findes et helt tal  $q_2$  så  $b \cdot q_2 = c$ . Dermed er

$$c = b \cdot q_2 = a \cdot q_1 \cdot q_2 = a \cdot (q_1 \cdot q_2),$$

hvilket viser at  $a \mid c$ .  $\square$

*Opgave 1.1.2.* Bevis resten af sætningen.

*Opgave 1.1.3.* Om de hele tal  $n$  og  $m$  oplyses at  $2 \mid n$  og  $6 \mid m$ . Hvilke af følgende tal er da med sikkerhed delelige med 4?

- a)  $n + m$ , b)  $nm - m$ , c)  $m^2 + n$ , d)  $m(m + n)$ , e)  $n(m + 1)$ .



Opgave 1.1.4. Om de hele tal  $m$  og  $n$  oplyses at  $n + m = n^2$ . Hvad kan man med sikkerhed slutte? a)  $n \mid m$ , b)  $m \mid n$ , c)  $n$  og  $m$  er ulige, d)  $n$  og  $m$  er lige.

### Definition af trivielle og ægte divisorer

De *trivielle divisorer* i et positivt heltal  $n$  er 1,  $-1$ ,  $n$  og  $-n$ . En divisor  $d$  i  $n$  kaldes en *ægte divisor* i  $n$  hvis den ikke er en triviel divisor.

### Definition af primtal og sammensatte tal

*Primtallene* er de positive heltal større end 1 som kun har trivielle divisorer. De første ti primtal er derfor

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

Positive heltal større end 1 som har en ægte divisor, kaldes *sammensatte tal*.

Opgave 1.1.5. Bestem alle primtallene op til 100.

### Definition af primfaktor

Et primtal der er divisor i et tal  $n$ , kaldes en *primfaktor* i  $n$ .

Fx er primfaktorerne i 60 netop 2, 3 og 5.

### Definition af primfaktoropløsning

At *primfaktoropløse* et tal betyder at skrive det som et produkt af primtal.

Fx er primfaktoropløsningen af 60 lig med  $2^2 \cdot 3 \cdot 5$ , primfaktoropløsningen af 13 lig med 13 og primfaktoropløsningen af 72 lig med  $2^3 \cdot 3^2$ .

Generelt er *primfaktoropløsningen* af et positivt heltal  $n$ ,  $n > 1$ ,

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

hvor  $p_i$ 'erne er forskellige primtal, og  $\alpha_i$ 'erne er positive heltal.

Om lidt skal vi se at alle positive heltal større end 1 har en primfaktoropløsning, og at denne er entydig på nær rækkefølgen af faktorerne. Primtallene fungerer altså som en slags byggesten som alle positive heltal større end 1 er bygget op af.

Opgave 1.1.6. Bestem primfaktoropløsningen af 1001 og af 11400. Bestem samtlige primfaktorer i 1024 og 1001.

**Sætning 1.1.2.** Ethvert positivt heltal  $n$  større end 1 har en primfaktor. Specielt er den mindste divisor i  $n$  større end 1 en primfaktor.

**Bevis.** Lad  $n$  være et positivt heltal større end 1, og lad  $p$  være den mindste divisor i  $n$  større end 1. Da må  $p$  være et primtal: Antag nemlig at  $p$  ikke er et primtal, dvs. at  $p$  har en ægte divisor større end 1. Denne divisor må også være divisor i  $n$  ifølge sætning 1.1.1 i modstrid med at  $p$  er den mindste. Dermed er  $p$  et primtal og altså en primfaktor i  $n$ .  $\square$

### Sætning 1.1.3. Aritmetikkens fundamentalsætning

Et positivt heltal  $n$  større end 1 har en primfaktoropløsning, og denne primfaktoropløsning er entydig (på nær faktorerens rækkefølge).

**Bevis. Eksistens:** Lad  $n$  være et positivt heltal større end 1, og lad  $p_1$  være en primfaktor i  $n$  (vi ved at en sådan findes ifølge sætning 1.1.2). Nu er  $n = p_1 \cdot q_1$ . Hvis  $q_1 = 1$ , har vi fundet en primfaktoropløsning af  $n$ . Ellers vælger vi en primfaktor  $p_2$  i  $q_1$ . Nu er  $n = p_1 \cdot p_2 \cdot q_2$ . Vi fortsætter på denne måde til vi får et  $q_r = 1$ , og da  $q_1, q_2, \dots$  er en aftagende følge af positive hele tal, må vi før eller siden få et  $q_r = 1$ . Dermed er  $n = p_1 \cdot p_2 \cdots p_r$ , hvor  $p_i$ 'erne er primtal, og  $n$  har altså en primfaktoropløsning.

**Entydighed:** Antag at der findes positive heltal med to forskellige primfaktoropløsninger, og lad  $n$  være det mindste af disse, så

$$p_1 \cdot p_2 \cdots p_r = n = q_1 \cdot q_2 \cdots q_s.$$

Ingen af primfaktorerne på venstresiden kan være lig med en af primfaktorerne på højresiden, for så ville vi ved at dividere med dette primtal få et tal mindre end  $n$  med to forskellige primfaktoropløsninger, i modstrid med at  $n$  er det mindste. Betragt nu primtallene  $p_1$  og  $q_1$ . Enten er  $p_1 < q_1$  eller omvendt. Antag uden tab af generalitet at  $p_1 < q_1$ , og betragt tallet

$$m = (q_1 - p_1) \cdot q_2 \cdot q_3 \cdots q_s.$$

Tallet  $m$  er mindre end  $n$  og har dermed ifølge antagelsen en entydig primfaktoropløsning. Men

$$\begin{aligned} m &= q_1 \cdot q_2 \cdots q_s - p_1 \cdot q_2 \cdot q_3 \cdots q_s \\ &= n - p_1 \cdot q_2 \cdot q_3 \cdots q_s \\ &= p_1(p_2 \cdot p_3 \cdots p_r - q_2 \cdot q_3 \cdots q_s), \end{aligned}$$

hvor sidste linje viser at der findes en primfaktoropløsning af  $m$  som indeholder primtallet  $p_1$ , mens

$$m = (q_1 - p_1) \cdot q_2 \cdot q_3 \cdots q_s$$

viser at  $m$  også har en primfaktoropløsning som ikke indeholder  $p_1$  da  $p_1$  ikke går op i  $q_1 - p_1$ . Dette er i modstrid med antagelsen, og alle positive heltal større end 1 har dermed en entydig primfaktoropløsning.  $\square$

En helt central følge af entydigheden af primfaktoropløsningen er at hvis  $a, b, n \in \mathbb{N}$ , hvor  $n = a \cdot b$ , da er primfaktoropløsningen af  $n$  lig med produktet af primfaktoropløsningen af  $a$  og primfaktoropløsningen af  $b$ . Dette leder til følgende korollar som det er vigtigt at forstå når man arbejder med delelighed.

**Korollar 1.1.4.** Lad  $p_1, p_2, \dots, p_r$  være  $r$  forskellige primtal, og lad yderligere  $\alpha_1, \alpha_2, \dots, \alpha_r$  være positive heltal. Et helt tal  $n$  er deleligt med produktet

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

netop hvis det er deleligt med hvert af tallene  $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_r^{\alpha_r}$ .

**Bevis.** Antag at  $n$  er deleligt med  $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ . Da følger det af sætning 1.1.1 at hvert af tallene  $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_r^{\alpha_r}$  går op i  $n$ .

Antag modsat at  $n$  er deleligt med hvert af tallene  $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_r^{\alpha_r}$ . Da  $p_i^{\alpha_i}$  går op i  $n$ ,  $i = 1, 2, \dots, r$ , kan  $n$  skrives på formen  $n = p_i^{\alpha_i} \cdot q$ . Fordi primfaktoropløsningen af  $n$  er entydig, betyder det at  $p_i^{\alpha_i}$  indgår i primfaktoropløsningen af  $n$ , for alle  $i = 1, 2, \dots, r$ , og altså at  $n$  kan skrives på formen  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \cdot q$ . Dette viser at  $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  går op i  $n$ .  $\square$

*Opgave 1.1.7.* Fire forskellige positive hele tal har produktet 2008. Hvad er summen af de fire tal?

*Opgave 1.1.8.* Hvor mange nuller ender tallet  $20!$  på? ( $20!$  betyder  $20 \cdot 19 \cdots 1$  og siges "20 fakultet").

*Opgave 1.1.9.* Går 4004 op i  $238 \cdot 65 \cdot 1221$ ?

#### Definition af kvadrattal

*Kvadrattallene* er alle tal der kan skrives på formen  $a^2$ , hvor  $a$  er et helt tal, dvs. tallene  $0, 1, 4, 9, 16, 25, \dots$

Det er en rigtig god idé at kende de første 20 kvadrattal.

*Opgave 1.1.10.* Vis at kvadrattallene større end 1 netop er de positive heltal  $n$ , hvor alle primfaktorer indgår i en lige potens i primfaktoropløsningen af  $n$ .

*Opgave 1.1.11.* Bestem det mindste positive heltal  $n$  så  $\sqrt{n \cdot 261}$  er et helt tal.

#### Sætning 1.1.5. Primtalsegenskaben

Lad  $p$  være et primtal, og lad  $a$  og  $b$  være hele tal. Hvis  $p \mid ab$ , da vil  $p \mid a$  eller  $p \mid b$ .

Dette er ikke altid tilfældet hvis  $p$  ikke er et primtal.

*Opgave 1.1.12.* Vis sætningen.



**Sætning 1.1.6.** Der findes uendeligt mange primtal.

**Bevis.** Antag modsat at der kun findes endeligt mange primtal, og lad disse være  $p_1, p_2, \dots, p_m$ . Betragt tallet

$$n = p_1 p_2 \cdots p_m + 1.$$

Da  $n > 1$ , har  $n$  en primfaktor  $p$ . Denne primfaktor  $p$  må være blandt primtallene  $p_1, p_2, \dots, p_m$ , dvs.  $p$  går både op i  $n$  og i  $p_1 p_2 \cdots p_m$ , og dermed i  $n - p_1 p_2 \cdots p_m = 1$ , hvilket er en modstrid. Altså er der uendeligt mange primtal.  $\square$

**Eksempel 1.1.1.** Hvis vi skal vise at et helt tal  $n$  er deleligt med fx 6, er det ifølge korollar 1.1.4 nok at vise at  $2 \mid n$  og  $3 \mid n$  da  $6 = 2 \cdot 3$ , og 2 og 3 er to forskellige primtal. Det er fx nemt at se at tallet 33333330 er deleligt med 6 da det er lige og deleligt med 3.

*Opgave 1.1.13.* Hvilke af følgende tal  $10046 \cdot 20396$ ,  $10982 \cdot 505$  og  $102971 \cdot 2031 \cdot 315$  er delelige med 10? Hvilke af følgende tal  $5025 \cdot 2092$ ,  $205 \cdot 262 \cdot 515$  og  $50035 \cdot 408$  er delelige med 100?

*Opgave 1.1.14.* Vis at produktet af tre på hinanden følgende heltal altid er deleligt med 6. Vis at produktet af fem på hinanden følgende heltal altid er deleligt med 60.

*Opgave 1.1.15.* Lad  $a$  og  $b$  være to positive heltal hvis sum er 2002. Er det muligt at 2002 går op i  $a b$ ? (Georg Mohr-Konkurrencen 2002) *Hint:* 3

**Sætning 1.1.7.** For ethvert positivt helt tal  $m$  findes  $m$  på hinanden følgende hele tal som ikke er primtal.

**Bevis.** Betragt de  $m$  på hinanden følgende hele tal

$$(m+1)! + 2, (m+1)! + 3, (m+1)! + 4, \dots, (m+1)! + m + 1.$$

Det første tal er 2 en ægte divisor, i det næste er 3, osv. Altså er ingen af de  $m$  på hinanden følgende tal primtal.  $\square$

## 1.2 Omskrivning vha. kvadratsætninger

I talteori ønsker vi ofte at faktorisere når det er muligt, da det er nemmere at sige noget om et produkt end om en sum, netop fordi vi ved produktet kan tænke i primfaktoropløsning. Hver gang vi ser et udtryk som  $a^2 - b^2$ , omskriver vi derfor straks til  $(a+b)(a-b)$ .

**Eksempel 1.2.1.** Hvis vi fx ønsker at bestemme alle primtal  $p$  og  $q$  som opfylder

$$p^2 - 2q^2 = 1,$$

kan vi omskrive og få

$$(p+1)(p-1) = 2q^2.$$

Da højresiden er lige, må  $p$  være ulige. Dermed vil 4 gå op i venstresiden, og dette giver at  $q$  er lige, dvs.  $q = 2$ . De eneste primtal som løser ligningen, er altså  $q = 2$  og  $p = 3$ .

**Eksempel 1.2.2.** Hvis vi skal finde samtlige heltallige løsninger til ligningen

$$n^2 + 389 = m^2,$$

omskriver vi straks til

$$389 = m^2 - n^2 = (m+n)(m-n).$$

Da 389 er et primtal, er det nemt at se at faktorerne  $m+n$  og  $m-n$  er  $\pm 389$  og  $\pm 1$ . Løsningerne er derfor  $(m, n) = (\pm 195, \pm 194)$ . Hvis 389 ikke var et primtal, fik vi lidt flere muligheder, men stadig kun endeligt mange.

Læg mærke til at det er fordi vi omskriver  $m^2 - n^2$  til et produkt, at vi meget nemt kan danne os overblik over de mulige løsninger, netop fordi vi kan se på primfaktoropløsningen.

Opgave 1.2.1. Bestem alle par  $(x, y)$  af positive heltal som opfylder ligningen  $x^6 = y^2 + 53$ .

Opgave 1.2.2. Vis at  $m^3 - m$  er delelig med 6 for alle hele tal  $m$ .

Opgave 1.2.3. I en retvinklet trekant hvori alle sidelængder er hele tal, har den ene katete længde 1994. Bestem længden af hypotenusen. (Georg Mohr-Konkurrencen 1994)

Opgave 1.2.4. Om tre hele tal  $p, q$  og  $r$  gælder at  $p + q^2 = r^2$ . Vis at  $6 \mid pqr$ . (Georg Mohr-Konkurrencen 2008)

**Eksempel 1.2.3.** Nogle gange skal der lidt mere sofistikerede omskrivninger vha. kvadratsætningerne til for at løse en problemstilling. Lad  $a$  være et positivt heltal større end 1. Hvis vi fx ønsker at vise at  $a^4 + a^2 + 1$  er et sammensat tal, kan vi omskrive på følgende måde.

$$a^4 + a^2 + 1 = (a^2 + 1)^2 - a^2 = (a^2 + 1 + a)(a^2 + 1 - a).$$

Heraf fremgår det klart at  $a^4 + a^2 + 1$  er et sammensat tal når  $a > 1$ .

Opgave 1.2.5. Vis at hvis der for to hele tal  $a$  og  $b$  gælder at  $a^2 + b^2 + 9ab$  er delelig med 11, da er også  $a^2 - b^2$  delelig med 11. (Georg Mohr-Konkurrencen 2004) *Hint:* 28

Opgave 1.2.6. Lad  $n$  og  $m$  være to hele tal som kan skrives som sum af to kvadrattal. Vis at da kan deres produkt  $mn$  også skrives som sum af to kvadrattal. (*Hint:* Skriv  $n$  og  $m$  som sum af to kvadrattal, bestem produktet  $nm$ , og omskriv vha. af kvadratsætningerne så det bliver en sum af to kvadrattal.)

Opgave 1.2.7. For hvilke positive heltal  $n$  er  $n^4 + 4$  et primtal? *Hint:* 8

Grunden til at vi gerne vil faktorisere, er som sagt at det i talteori er meget nemmere at sige noget om et produkt end om en sum. Indtil nu har vi kun omskrevet vha. kvadratsætningerne, men de kan ikke altid bruges når man vil omskrive til produkt.

**Eksempel 1.2.4.** Hvis vi fx vil bestemme samtlige par af positive heltal  $x$  og  $y$  som er løsning til ligningen

$$2x^2 + 5y^2 = 11(xy - 11),$$

ønsker vi at omskrive så der er et produkt på den ene side og et tal på den anden. I første omgang fås

$$11^2 = 11xy - 2x^2 - 5y^2.$$

Højresiden kan nu omskrives til produkt:

$$11^2 = (2x - y)(5y - x)$$

Pointen er som tidligere at vi nu har et produkt, hvor de ubekendte indgår, på den ene side af lighedstegnet og et tal på den anden. Det er ikke altid helt let at finde en omskrivning, men i dette eksempel kan man gætte sig frem til at produktet skal være på formen  $(ax - by)(cy - dx)$ , og herefter er det ikke så svært at finde  $a, b, c$  og  $d$ . Når vi først har omskrevet, kan vi løse ligningen sådan:

Hvis begge faktorer er negative, er  $2x < y < \frac{1}{5}x$ , hvilket er en modstrid da  $x$  er positiv. Dermed er begge faktorer positive. Det er nu nemt at tjekke mulighederne igennem, og man får at den eneste løsning er  $x = 14$  og  $y = 27$ . (Baltic Way 1998)

Opgave 1.2.8. Bestem alle par af positive heltal  $(x, y)$  som opfylder ligningen

$$2y^2x^2 + 16x^2 + y^2 = 448.$$

Opgave 1.2.9. Bestem alle par af positive heltal  $(x, y)$  som opfylder ligningen

$$x^2 + 2x - xy - 3y = 1997.$$

(Georg Mohr-Konkurrencen 1997)



### 1.3 Antal divisorer

Når man skal bestemme antallet af positive divisorer i et positivt heltal, er det en god idé at se på primfaktoropløsningen for at finde samtlige divisorer på en nem og overskuelig måde.

**Eksempel 1.3.1.** Hvis vi fx skal bestemme antallet af divisorer i

$$60 = 2^2 \cdot 3 \cdot 5,$$

så er samtlige divisorer

$$1, 2, 2^2, 3, 2 \cdot 3, 2^2 \cdot 3, 5, 2 \cdot 5, 2^2 \cdot 5, 3 \cdot 5, 2 \cdot 3 \cdot 5, 2^2 \cdot 3 \cdot 5.$$

Altså alle tal på formen  $2^a \cdot 3^b \cdot 5^c$ , hvor  $a = 0, 1, 2$ ,  $b = 0, 1$  og  $c = 0, 1$ .

Tallet 60 har derfor i alt  $3 \cdot 2 \cdot 2 = 12$  divisorer.

**Sætning 1.3.1.** Et positivt heltal  $n$  større end 1 med primfaktoropløsning

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

hvor  $p_i$ 'erne er forskellige primtal, har

$$(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_m)$$

forskellige positive divisorer.

*Opgave 1.3.1.* Bevis sætningen.

**Eksempel 1.3.2.** Hvis vi ønsker at bestemme alle positive heltal  $n$  med netop  $p$  divisorer, hvor  $p$  er et primtal, da skal vi finde alle

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

for hvilke

$$(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_m) = p.$$

Da  $p$  er et primtal, og alle faktorerne på venstresiden er større end 1, må  $m = 1$  og  $\alpha_1 = p - 1$ . Altså er samtlige positive heltal med netop  $p$  divisorer alle tal på formen  $q^{p-1}$ , hvor  $q$  er et primtal.

*Opgave 1.3.2.* Bestem alle positive heltal større end 1 som har et ulige antal positive divisorer.

*Opgave 1.3.3.* Et positivt heltal  $n$ , 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 størst mulige værdi af  $n$ . (Georg Mohr-Konkurrencen 2006)

*Opgave 1.3.4.* Lad  $n$  være produktet af samtlige positive heltal mindre end en million med præcis syv divisorer. Vis at  $n$  er et kubiktal, dvs. et tal på formen  $m^3$ , hvor  $m$  er et helt tal.

*Opgave 1.3.5.* Bestem samtlige positive heltal  $n$  som er delelige med 1001 og har præcis 1001 divisorer.

## 1.4 Største fælles divisor og Euklids algoritme

### Definition af største fælles divisor

Den *største fælles divisor* for to hele tal  $n$  og  $m$  er den største divisor der går op i både  $n$  og  $m$ . Den største fælles divisor betegnes  $\gcd(n, m)$  (**g**reatest **c**ommon **d**ivisor).

Fx er  $\gcd(12, 18) = 6$ ,  $\gcd(100, 125) = 25$  og  $\gcd(35, 36) = 1$ .

*Opgave 1.4.1.* Bestem  $\gcd(12, 45)$ ,  $\gcd(1000, 1205)$ ,  $\gcd(1024, 12)$ ,  $\gcd(88, 90)$  og  $\gcd(1002, 1003)$ .

*Opgave 1.4.2.* Lad  $n \in \mathbb{Z}$ . Bestem  $\gcd(n, n + 1)$ . Bestem  $\gcd(n, n + 2)$  når  $n$  er lige, og når  $n$  er ulige.

**Sætning 1.4.1.** Lad  $n$ ,  $m$  og  $q$  være hele tal. Da er

$$\gcd(n, m) = \gcd(m, n - qm).$$

**Bevis.** En fælles divisor i  $n$  og  $m$  er ifølge sætning 1.1.1 også divisor i  $m$  og  $n - qm$ . Tilsvarende er en fælles divisor i  $m$  og  $n - qm$  også divisor i  $m$  og  $n$  da  $n = (n - qm) + qm$ . Tallene  $n$  og  $m$  og tallene  $m$  og  $n - qm$  har altså præcis de samme fælles divisorer, og dermed også samme største fælles divisor.  $\square$

### Eksempel 1.4.1. Euklids algoritme

Når man skal bestemme største fælles divisor mellem to små tal, kan man fx se på deres primfaktoropløsning, men for større tal tager det tid at bestemme primfaktoropløsningen. Man kan i stedet bruge en anden metode til at bestemme største fælles divisor, nemlig *Euklids algoritme*. Denne algoritme bygger på sætning 1.4.1.

Først viser vi hvordan Euklids algoritme fungerer ved et eksempel. Vi ønsker at bestemme  $\gcd(1078, 70)$ . Først skrives 1078 som et produkt af 70 plus en rest  $r$ ,  $0 \leq r < 70$ . Derefter skrives 70 som et produkt af  $r$  plus en ny rest, osv. til vi får resten 0:

$$1078 = 15 \cdot 70 + 28$$

$$70 = 2 \cdot 28 + 14$$

$$28 = 2 \cdot 14 + 0.$$

Dette viser ifølge sætning 1.4.1 at

$$\begin{aligned} \gcd(1078, 70) &= \gcd(1078 - 15 \cdot 70, 70) = \gcd(28, 70) = \gcd(28, 70 - 2 \cdot 28) \\ &= \gcd(28, 14) = \gcd(28 - 2 \cdot 14, 14) = \gcd(0, 14) = 14. \end{aligned}$$

### Definition af Euklids algoritme

Generelt fungerer *Euklids algoritme* således: Lad  $n$  og  $m$  være ikke-negative heltal, hvor  $n \geq m$ . Først skrives  $n$  som et multiplum af  $m$  med en rest  $r_1$ ,  $0 \leq r_1 < m$ . Derefter skrives  $m$  som et multiplum af  $r_1$  med en rest  $r_2$ ,  $0 \leq r_2 < r_1$ , osv. indtil vi får resten 0. Resten bliver mindre for hvert skridt, dvs. på et eller andet tidspunkt er vi sikre på at få en rest på 0.

$$n = q_1 \cdot m + r_1, \quad 0 \leq r_1 < m$$

$$m = q_2 \cdot r_1 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = q_3 \cdot r_2 + r_3, \quad 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{k-2} = q_k \cdot r_{k-1} + r_k, \quad 0 \leq r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1} \cdot r_k + 0.$$

Af dette ses at

$$\gcd(n, m) = \gcd(m, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_k, 0) = r_k.$$



Opgave 1.4.3. Benyt Euklids algoritme til at bestemme  $\gcd(754, 338)$ .

### Definition af primisk og indbyrdes primisk

Lad  $a$  og  $b$  være to hele tal. Tallet  $a$  er *primisk* med  $b$  (eller omvendt) hvis deres eneste positive fælles divisor er 1, dvs. hvis  $\gcd(a, b) = 1$ . Når  $a$  er primisk med  $b$ , siger vi at  $a$  og  $b$  er *indbyrdes primiske*.

**Eksempel 1.4.2.** Idéen med at se på den største fælles divisor kan fx benyttes til at vise at brøken  $\frac{n^2+n-1}{n^2+2n}$  er uforkortelig for alle hele tal  $n \in \mathbb{Z} \setminus \{0, -2\}$  da dette er ensbetydende med at tæller og nævner er indbyrdes primiske. Vi benytter sætning 1.4.1 til at bestemme største fælles divisor mellem tæller og nævner:

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

Dette viser at brøken er uforkortelig for alle heltal  $n \in \mathbb{Z} \setminus \{0, -2\}$ .

Inden du regner flere opgaver, får du brug for en god lille regneregul om største fælles divisor:

**Sætning 1.4.2.** Lad  $a$ ,  $b$  og  $c$  være hele tal, hvor  $b$  og  $c$  er indbyrdes primiske. Da er

$$\gcd(a, b) = \gcd(ac, b).$$

Opgave 1.4.4. Vis sætningen.

**Eksempel 1.4.3.** Vi kan fx bruge sætning 1.4.2 hvis vi fx vil undersøge for hvilke hele tal  $n$  at  $\gcd(n^2+25, 4n+1)$  er størst. Da  $4n+1$  og 4 er indbyrdes primiske, er

$$\begin{aligned} \gcd(n^2 + 25, 4n + 1) &= \gcd(4(n^2 + 25), 4n + 1) \\ &= \gcd(4n^2 + 100 - n(4n + 1), 4n + 1) \\ &= \gcd(-n + 100, 4n + 1) \\ &= \gcd(4(-n + 100) + (4n + 1), 4n + 1) \\ &= \gcd(401, 4n + 1) \end{aligned}$$

Dette viser at  $\gcd(n^2 + 25, 4n + 1)$  højst er 401, og det er det, netop når  $4n + 1 = \pm 401$ . Eneste mulige  $n$  der løser denne ligning, er  $n = 100$ , dvs.  $\gcd(n^2 + 25, 4n + 1)$  er størst når  $n = 100$ .

Opgave 1.4.5. Vis at brøken

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

er uforkortelig for alle  $n \in \mathbb{Z}$ .

Opgave 1.4.6. Lad  $m \in \mathbb{Z}$ ,  $m \neq 1$ . Vis at brøken

$$\frac{m^4 + 3m^3 - 3m^2 + 2m - 2}{m - 1}$$

er uforkortelig. *Hint:* 20

Opgave 1.4.7. Bestem alle  $n \in \mathbb{Z}$  så

$$\frac{3n^2 + 3n + 9}{3n + 2}$$

er et helt tal. *Hint:* 14

Opgave 1.4.8. Lad  $a_n = n^2 + 500$  for alle  $n \in \mathbb{N}$ . Vis at der findes et helt tal  $N$  så  $\gcd(a_n, a_{n+1}) \leq N$  for alle  $n \in \mathbb{N}$ , og bestem det mindste heltal  $N$  med denne egenskab. *Hint:* 11

### Definition af af mindste fælles multiplum

Det *mindste fælles multiplum* af to positive hele tal  $a$  og  $b$  er det mindste positive hele tal som de begge går op i, og det betegnes  $\text{lcm}(a, b)$  (**l**east **c**ommon **m**ultiple).

Fx er  $\text{lcm}(4, 6) = 12$ ,  $\text{lcm}(5, 7) = 35$  og  $\text{lcm}(50, 100) = 100$ .

Opgave 1.4.9. Bestem  $\text{lcm}(10, 12)$ ,  $\text{lcm}(2 \cdot 3^4 \cdot 7^8, 2^2 \cdot 3^3 \cdot 7^3 \cdot 11)$  og  $\text{lcm}(13, 17)$ .

**Sætning 1.4.3.** Lad  $a$  og  $b$  være to positive hele tal. Lad  $p_1, p_2, \dots, p_n$  være samtlige primdivisorer i  $a$  og  $b$ ,  $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$  og  $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$ . Da er

$$\begin{aligned}\gcd(a, b) &= p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_n^{\min(\alpha_n, \beta_n)}, \\ \text{lcm}(a, b) &= p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdots p_n^{\max(\alpha_n, \beta_n)}, \\ a \cdot b &= \text{lcm}(a, b) \cdot \gcd(a, b).\end{aligned}$$

Opgave 1.4.10. Bevis sætningen.

### Sætning 1.4.4. Bezouts identitet

Lad  $n$  og  $m$  være hele tal. Da kan største fælles divisor mellem  $n$  og  $m$  skrives som en heltallig linearkombination af  $n$  og  $m$ , dvs. der findes hele tal  $s$  og  $t$  så

$$\gcd(n, m) = sn + tm.$$

Bemærk at tallene  $s$  og  $t$  ikke er entydige.

**Bevis.** Beviset bygger på Euklids algoritme. Vi viser ved induktion efter  $i$  at alle resterne  $r_i$ ,  $i = 1, 2, \dots, k$ , fra Euklids algoritme kan skrives som en heltallig linearkombination af  $n$  og  $m$  da dette specielt viser at  $r_k = \gcd(n, m)$  kan skrives sådan. Sæt  $r_0 = m$ , og husk at  $r_{i-1} = q_{i+1}r_i + r_{i+1}$  i Euklids algoritme.

Induktionsstart: Både  $r_0$  og  $r_1$  kan skrives som heltallige linearkombinationer af  $n$  og  $m$  da  $r_0 = m = 0 \cdot n + 1 \cdot m$  og  $r_1 = 1 \cdot n - q_1 \cdot m$ .

Induktionsskridt: Antag nu at for et  $j \geq 1$  kan  $r_i$  skrives som en heltallig linearkombination af  $n$  og  $m$  for alle  $i \leq j$ , og sæt  $r_i = s_i n + t_i m$ . Vi viser nu at  $r_{j+1}$  kan skrives som en heltallig linearkombination af  $n$  og  $m$ :

$$\begin{aligned}r_{j+1} &= r_{j-1} - q_{j+1}r_j = s_{j-1}n + t_{j-1}m - q_{j+1}(s_j n + t_j m) \\ &= (s_{j-1} - q_{j+1}s_j)n + (t_{j-1} - q_{j+1}t_j)m.\end{aligned}$$

Dermed er induktionen fuldført.  $\square$

**Eksempel 1.4.4.** I eksempel 1.4.1 viste vi ved at benytte Euklids algoritme at  $\gcd(1078, 70) = 14$ . Nu kan vi bruge algoritmen baglæns så at sige til at bestemme hele tal  $s$  og  $t$  så  $14 = s \cdot 1078 + t \cdot 70$ :

$$14 = 70 - 2 \cdot 28 = 70 - 2(1078 - 15 \cdot 70) = -2 \cdot 1078 + 31 \cdot 70.$$

Opgave 1.4.11. Bestem hele tal  $s$  og  $t$  så  $\gcd(754, 338) = s \cdot 754 + t \cdot 338$ .

Opgave 1.4.12. Bestem alle tal på formen  $s \cdot 15 + t \cdot 35$ ,  $s, t \in \mathbb{Z}$ .

**Sætning 1.4.5.** Lad  $a, b, c \in \mathbb{Z}$ . Der findes hele tal  $x$  og  $y$  som løser ligningen

$$c = ax + by,$$

netop hvis  $c$  er et multiplum af  $\gcd(a, b)$ . Med andre ord er  $c$  en heltallig linearkombination af  $a$  og  $b$  netop når  $c$  er et multiplum af deres største fælles divisor.

Opgave 1.4.13. Vis sætningen. *Hint:* 12



## 1.5 Restklasser

### Definition af division med rest

Lad  $n \in \mathbb{N}$  og  $m \in \mathbb{Z}$ . Da findes  $q, r \in \mathbb{Z}$ , hvor  $0 \leq r < n$ , så

$$m = q \cdot n + r.$$

Vi siger at  $m$  har *resten*  $r$  ved division med  $n$ .

Fx har  $m = 38$  resten  $r = 3$  ved division med  $n = 5$  da  $38 = 7 \cdot 5 + 3$ , og  $m = -27$  har resten  $r = 1$  ved division med  $n = 4$  da  $-27 = -7 \cdot 4 + 1$ .

Idéen i restklasseregning, som vi om lidt vil introducere mere formelt, er at man vælger et tal  $n$  og identificerer andre tal ved deres rest ved division med  $n$ .

Hvis vi fx ser på  $n = 5$ , så deler vi alle de hele tal ind i restklasser afhængigt af deres rest ved division med 5. Vi får altså fem restklasser - en for hver af de fem rester 0, 1, 2, 3, 4. Fx består restklassen 1 af tallene

$$\dots, -9, -4, 1, 6, 11, 16, \dots$$

Regning med restklasser er helt centralt i talteori fordi det i rigtig mange sammenhænge gør en problemstilling meget mere overskuelig hvis vi kun identificerer tal ved deres rest ved division med et positivt helt tal  $n$ . I resten af dette kapitel af det et af de mest grundlæggende værktøjer til løsning af komplicerede talteoretiske problemstillinger.

### Definition af kongruens

Lad  $n$  være et positivt heltal. Tallene  $a, b \in \mathbb{Z}$  siges at være *kongruente modulo*  $n$  hvis

$$n \mid a - b.$$

At  $a$  og  $b$  er kongruente modulo  $n$ , skrives

$$a \equiv b \pmod{n}.$$

At  $n \mid a - b$ , er ensbetydende med at  $a$  og  $b$  har samme rest ved division med  $n$ , dvs. to tal er kongruente modulo  $n$  netop hvis de har samme rest ved division med  $n$ . (Det overlades til læseren at bevise dette).

**Eksempel 1.5.1.** Hvis vi fx tager vores modulo 10-briller på, så kan vi ikke se forskel på  $-2$  og  $18$ . Der gælder nemlig at  $-2 \equiv 18 \pmod{10}$  da  $10$  går op i  $18 - (-2) = 20$ , eller sagt med andre ord da både  $-2$  og  $18$  har rest 8 ved division med  $10$ .

Hvis vi tilsvarende tager vores modulo 7-briller på, kan vi ikke se forskel på fx  $8, 15, 71$  og  $701$  da de alle har rest 1 ved division med  $7$ .

### Definition af restklasse

*Restklassen* repræsenteret ved  $a$  modulo  $n$  er netop alle tal der er kongruente med  $a$  modulo  $n$ , dvs. de tal der har samme rest som  $a$  ved division med  $n$ . Altså netop tallene

$$\dots, -3n + a, -2n + a, -n + a, a, n + a, 2n + a, 3n + a, \dots$$

Der er uendelig mange repræsentanter for hver restklasse. Når vi taler om resten af et tal modulo  $n$ , mener vi resten  $r$  som opfylder at  $0 \leq r < n$ , og det er også den vi vil benytte som den primære repræsentant for en restklasse.

**Eksempel 1.5.2.** Restklassen repræsenteret ved 8 modulo 10 er tallene

$$\dots, -12, -2, 8, 18, 28, \dots$$

Restklassen repræsenteret ved 1 modulo 7 er tallene

$$\dots, -13, -6, 1, 8, 15, 22, \dots$$

Opgave 1.5.1. Lad  $n \in \mathbb{N}$  og  $a, b \in \mathbb{Z}$ . Bevis at  $a \equiv b \pmod{n}$  netop hvis de har samme rest ved division med  $n$ .

Opgave 1.5.2. Formulér med andre ord hvad det betyder at et helt tal  $a$  opfylder at  $a \equiv 0 \pmod{n}$ .

Opgave 1.5.3. Formulér med andre ord hvad det vil sige at de hele tal  $a$  og  $b$  opfylder at  $a \equiv b \pmod{2}$ .

Opgave 1.5.4. Undersøg om a)  $182 \equiv 92 \pmod{18}$ , b)  $-43 \equiv 1 \pmod{4}$  og c)  $111 \equiv 13 \pmod{11}$ .

**Sætning 1.5.1.** Lad  $n, k \in \mathbb{N}$  og  $a, b, c, d \in \mathbb{Z}$ . Da gælder følgende regneregler:

- i) Hvis  $a \equiv b \pmod{n}$  og  $c \equiv d \pmod{n}$ , da er  $a + c \equiv b + d \pmod{n}$ .
- ii) Hvis  $a \equiv b \pmod{n}$  og  $c \equiv d \pmod{n}$ , da er  $a - c \equiv b - d \pmod{n}$ .
- iii) Hvis  $a \equiv b \pmod{n}$  og  $c \equiv d \pmod{n}$ , da er  $a \cdot c \equiv b \cdot d \pmod{n}$ .
- iv) Hvis  $a \equiv b \pmod{n}$ , da er  $c \cdot a \equiv c \cdot b \pmod{n}$ .
- v) Hvis  $a \equiv b \pmod{n}$ , da er  $a^k \equiv b^k \pmod{n}$ .

**Bevis.** i) At  $a \equiv b$  og  $c \equiv d \pmod{n}$  betyder at  $n \mid a - b$  og  $n \mid c - d$ . Dermed må  $n \mid (a - b) + (c - d) = (a + c) - (b + d)$ , og altså  $a + c \equiv b + d \pmod{n}$ .

iii) At  $a \equiv b$  og  $c \equiv d \pmod{n}$  betyder at  $n \mid a - b$  og  $n \mid c - d$ . Dermed må  $n \mid c(a - b) + b(c - d) = ac - bd$ , og altså  $a \cdot c \equiv b \cdot d \pmod{n}$ .  $\square$

Opgave 1.5.5. Bevis resten af sætningen.

Sætningen viser at man kan omskrive en kongruensligning ligesom man kan omskrive en almindelig ligning når det gælder regningsarterne plus, minus og gange. Det samme gælder ikke umiddelbart for division. Fx er  $3 \cdot 4 \equiv 3 \cdot 2 \pmod{6}$ , mens  $4 \not\equiv 2 \pmod{6}$ .

**Eksempel 1.5.3.** Hvis man fx skal løse ligningen

$$x + 7 \equiv 2 \pmod{8},$$

kan man omskrive til  $x \equiv 2 - 7 \pmod{8}$  ifølge regneregler ii). Dermed er  $x \equiv -5 \equiv 3 \pmod{8}$ , dvs. løsningerne er netop restklassen 3 modulo 8. Løsningsmængden er altså

$$\{\dots, -13, -5, 3, 11, 19, \dots\}.$$

**Eksempel 1.5.4.** For at bestemme resten af tallet  $24^9 \cdot 18^{16} \cdot 101^7$  ved division med 5 kan vi regne modulo 5 og benytte regnereglerne i sætning 1.5.1 på denne måde:

$$24^9 \cdot 18^{16} \cdot 101^7 \equiv (-1)^9 \cdot 3^{16} \cdot 1^7 \equiv -1 \cdot (3^2)^8 \cdot 1 \equiv -1 \cdot (-1)^8 \equiv -1 \equiv 4 \pmod{5}.$$

Undervejs benytter vi fx regneregler v) til at konkludere at når  $24 \equiv -1 \pmod{5}$ , er  $24^9 \equiv (-1)^9 \pmod{5}$  osv. Desuden benyttes regneregler iii) fx til at konkludere at når  $24^9 \equiv (-1)^9$ ,  $18^{16} \equiv 3^{16}$  og  $101^7 \equiv 1^7 \pmod{5}$ , da er  $24^9 \cdot 18^{16} \cdot 101^7 \equiv (-1)^9 \cdot 3^{16} \cdot 1^7 \pmod{5}$ .

Opgave 1.5.6. Løs ligningen  $x - 12 \equiv 5 \pmod{11}$ .

Opgave 1.5.7. Bestem resten af  $27^{103} \cdot 17^2 \cdot 5^{14}$  ved division med 13.

Opgave 1.5.8. Bestem sidste ciffer i  $2007^{2007}$ . (Georg Mohr-Konkurrencen 2007)

**Sætning 1.5.2. Nulregel modulo primtal**

Lad  $p$  være et primtal, og lad  $a$  og  $b$  være hele tal. Da gælder nulreglen modulo  $p$ , dvs. at hvis  $a \cdot b \equiv 0 \pmod{p}$ , da er  $a \equiv 0$  eller  $b \equiv 0 \pmod{p}$ .

Opgave 1.5.9. Vis sætningen.



**Bemærkning.** Nulreglen gælder ikke for et sammensat tal  $n$ . Det kan man fx indse ved at betragte  $n = a \cdot b$ , hvor  $a$  og  $b$  er ægte divisorer i  $n$ . Her er  $a \cdot b \equiv 0 \pmod{n}$ , mens  $a \not\equiv 0 \pmod{n}$  og  $b \not\equiv 0 \pmod{n}$ .

**Eksempel 1.5.5.** Hvis vi skal løse ligningen

$$x^2 \equiv 4 \pmod{6},$$

ved vi at hvis et tal  $x$  er løsning, så er alle tal i den restklasse  $x$  repræsenterer modulo 6, også løsninger. Tilsvarende ved vi at hvis  $x$  ikke er en løsning til ligningen, da er der heller ikke andre repræsentanter for restklassen repræsenteret ved  $x$  modulo 6, som er løsninger. Det følger nemlig af sætning 1.5.1.

Når vi skal løse ligningen, kan vi altså nøjes med at tjekke en repræsentant for hver af de 6 restklasser modulo 6, fx repræsentanterne 0, 1, 2, 3, 4, 5. Ved indsættelse ses at det kun er  $x = 2$  og  $x = 4$  blandt disse tal der løser ligningen. Løsningsmængden består derfor af restklasserne repræsenteret ved 2 og 4 modulo 6.

*Opgave 1.5.10.* Løs ligningerne a)  $x^2 \equiv 4 \pmod{5}$ , b)  $x^2 \equiv 2 \pmod{5}$ , c)  $x^2 \equiv 1 \pmod{8}$ , d)  $x^2 \equiv 0 \pmod{2}$ .

**Sætning 1.5.3.** Hvis  $p$  er et primtal større end 2, da er de eneste løsninger til ligningen

$$x^2 \equiv 1 \pmod{p}$$

restklasserne 1 og  $-1$  modulo  $p$ .

*Opgave 1.5.11.* Bevis sætningen. (Husk at enhver matematiker straks omskriver vha. kvadratsætningerne når hun ser en differens mellem to kvadrattal!)

### Definition af tværsom

*Tværsommen* af et positivt heltal er summen af dets cifre. I det følgende betegner  $t(n)$  tværsommen af  $n \in \mathbb{N}$ . Fx er  $t(1245) = 1 + 2 + 4 + 5 = 12$ .

### Definition af den alternerende tværsom

Den *alternerende tværsom* af et tal  $n \in \mathbb{N}$  fås ved at tage første ciffer, trække det næste ciffer fra, lægge det næste til, osv. Fx er den alternerende tværsom af 913263 lig med  $9 - 1 + 3 - 2 + 6 - 3 = 12$ .

**Sætning 1.5.4.** Lad  $n \in \mathbb{N}$ .

- i) Tallet 3 går op i  $n$  netop hvis det går op i tværsommen af  $n$ .
- ii) Tallet 9 går op i  $n$  netop hvis det går op i tværsommen af  $n$ .
- iii) Tallet 11 går op i  $n$  netop hvis det går op i den alternerende tværsom af  $n$ .

**Bevis.** i) Lad  $a_m, a_{m-1}, \dots, a_1, a_0$  være cifrene i  $n$ , så

$$n = a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0.$$

Nu viser vi at  $n \equiv t(n) \pmod{3}$ .

$$\begin{aligned} n &= a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0 \\ &\equiv a_m \cdot 1^m + a_{m-1} \cdot 1^{m-1} + \dots + a_1 \cdot 1 + a_0 \\ &\equiv a_m + a_{m-1} + \dots + a_1 + a_0 = t(n) \pmod{3}. \end{aligned}$$

Dermed er  $n$  delelig med 3, netop når tværsommen er det.  $\square$

*Opgave 1.5.12.* Bevis resten af sætningen.

*Opgave 1.5.13.* Overvej hvordan man nemt kan afgøre om et tal er deleligt med 18 og med 22.

## 1.6 Restklasseregning og kvadratiske rester

I kapitel 1.2 løste vi ligninger med hele tal bl.a. ved at omskrive vha. kvadrat-sætninger og se på primfaktoropløsning. En anden metode er at regne modulo et tal for at få information om løsningerne. Det svære er som regel at gennemskue hvilket tal det kan betale sig at regne modulo. Først ser vi på kvadratiske rester da de i mange sammenhænge er interessante når man fx skal løse ligninger.

### Definition af kvadratisk rest

En restklasse  $a$  modulo  $n$  er en *kvadratisk rest* modulo  $n$  hvis ligningen

$$x^2 \equiv a \pmod{n}$$

har en heltallig løsning.

**Eksempel 1.6.1.** Man finder fx de kvadratiske rester modulo 8 ved at udregne kvadratet på samtlige rester:

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 1, 4^2 \equiv 0, 5^2 \equiv 1, 6^2 \equiv 4, 7^2 \equiv 1$$

modulo 8. Af dette kan man se at de kvadratiske rester modulo 8 netop er 0, 1 og 4, mens 2, 3, 5, 6, og 7 ikke er kvadratiske rester modulo 8.

Faktisk behøver man kun udregne kvadraterne på 0, 1, 2, 3, 4 for at bestemme de kvadratiske rester modulo 8 da  $a^2 \equiv (8-a)^2 \pmod{8}$ .

*Opgave 1.6.1.* Bestem de kvadratiske rester modulo 3, modulo 4 og modulo 5.

**Eksempel 1.6.2.** Man kan fx benytte kvadratiske rester til at vise at summen af kvadraterne på tre på hinanden følgende tal ikke kan være et kvadrattal. Tre på hinanden følgende tal har resterne 0, 1 og 2 (i en eller anden rækkefølge) modulo 3, og dermed er summen af kvadraterne på dem

kongruent med

$$0^2 + 1^2 + 2^2 \equiv 0 + 1 + 1 = 2 \pmod{3}.$$

Da 2 ikke er kvadratisk rest modulo 3, kan summen af de tre kvadrater ikke være et kvadrattal.

Her undersøgte vi om ligningen

$$n^2 + (n+1)^2 + (n+2)^2 = m^2$$

havde heltallige løsninger  $n$  og  $m$  ved at regne modulo 3 for at få information om  $n$  og  $m$ . Dette viste at  $m^2 \equiv 2 \pmod{3}$ , dvs. vi fik en ligning der ikke havde løsninger, og vi kunne derfor konstatere at den oprindelige ligning heller ikke havde løsninger. Hvis vi havde opnået en ligning der havde løsninger ved at regne modulo 3, kunne vi ikke omvendt konstatere at den oprindelige ligning havde løsninger, men vi kunne måske finde information om hvilken rest eventuelle løsninger skulle have modulo 3.

*Opgave 1.6.2.* a) Vis at summen af kvadraterne af fire på hinanden følgende hele tal ikke kan være et kvadrattal. b) Vis at summen af kvadraterne af fem på hinanden følgende hele tal ikke kan være et kvadrattal. c) Vis at summen af kvadraterne af seks på hinanden følgende hele tal ikke kan være et kvadrattal.

*Hint:* 33

**Eksempel 1.6.3.** Hvis man vil vise at en ligning hvor der indgår kvadratet på en af de ubekendte, ikke har løsninger, er det ofte en god ide at forsøge at reducere problemstillingen til en ligning af typen  $x^2 \equiv a \pmod{n}$  da ikke alle rester er kvadratiske rester modulo  $n$ .

Hvis vi ønsker at vise at ligningen

$$15x^2 - 7y^2 = 9,$$

ikke har nogen heltallige løsninger, regner vi modulo et helt tal for at forsøge at opnå en ligning af typen  $x^2 \equiv a \pmod{n}$  som ikke har nogen heltallige løsninger. Da primfaktorerne i 15, 7 og 9 er 3, 5 og 7, er det oplagt



at forsøge at regne modulo et af disse tal. For at illustrere metoden prøver vi med alle disse tre tal.

Først regner vi modulo 3. Dette giver  $7y^2 \equiv 0 \pmod{3}$ , og dermed ifølge nulreglen at  $y$  er delelig med 3 da 3 er et primtal. Vi kan nu sætte  $y = 3y_1$  og indsætte dette i ligningen. Dette giver

$$15x^2 - 63y_1^2 = 9$$

som reduceres til

$$5x^2 - 21y_1^2 = 3.$$

Hvis vi igen regner modulo 3, fås  $5x^2 \equiv 0 \pmod{3}$ , hvilket viser  $x$  er delelig med 3. Vi kan nu sætte  $x = 3x_1$  og omskrive ligningen til

$$45x_1^2 - 21y_1^2 = 3,$$

og yderligere til

$$15x_1^2 - 7y_1^2 = 1.$$

Regner vi igen modulo 3, skal  $y_1^2 \equiv 2 \pmod{3}$ , men 2 er ikke kvadratisk rest modulo 3. Ligningen har derfor ingen heltallige løsninger.

Hvis vi i stedet regner modulo 5, får vi

$$3y^2 \equiv 4 \pmod{5}.$$

Da vi gerne vil opnå en ligning af typen  $y^2 \equiv a \pmod{5}$ , overvejer vi om der ikke er et tal  $c$  vi kan gange med på begge sider så  $c \cdot 3 \equiv 1 \pmod{5}$ . Det er ikke svært at se at  $c = 2$  opfylder dette. Ved at gange med 2 på begge sider fås

$$y^2 \equiv 3 \pmod{5},$$

men 3 er ikke kvadratisk rest modulo 5. Ligningen har altså ingen heltallige løsninger.

Regner vi derimod modulo 7, får vi

$$x^2 \equiv 2 \pmod{7},$$

og da 2 er kvadratisk rest modulo 7, fortæller det os kun at  $x \equiv 3$  eller  $x \equiv 4 \pmod{7}$ . Det ser altså ikke umiddelbart ud til at virke.

I dette eksempel kan man altså både regne modulo 3 og modulo 5, men det er langt det hurtigste at regne modulo 5. I praksis må man forsøge sig lidt frem for at finde ud af hvad der virker.

*Opgave 1.6.3.* Vis at ligningen  $x^2 + 10 = 5^y$  ikke har nogen positive heltallige løsninger.

*Opgave 1.6.4.* Bestem alle heltallige løsninger til ligningen  $x^2 - 3y^2 = 17$ .

*Opgave 1.6.5.* Findes der fire forskellige heltal med den egenskab at produktet af vilkårlige to lagt til 2006, giver et kvadrattal? (Baltic Way 2006) *Hint:* 9

*Opgave 1.6.6.* Bestem alle heltallige løsninger til  $x^2 + y^2 + z^2 = 2xyz$ . *Hint:* 34

**Sætning 1.6.1.** Lad  $p$  være et ulige primtal. Da er netop halvdelen af alle tallene  $1, 2, \dots, p-1$  kvadratiske rester modulo  $p$ .

*Opgave 1.6.7.* Bevis sætningen. *Hint:* 24

**Eksempel 1.6.4.** Nu skal vi se på ligninger som kan løses ved at regne modulo et bestemt tal, men som ikke involverer kvadratiske rester. Vi ønsker at bestemme alle positive heltallige løsninger til ligningen

$$1 + 3^n = 2^m.$$

Da der står en potens af 2 på den ene side af lighedstegnet, regner vi først modulo 8 og udnytter at når  $m \geq 3$ , da er  $2^m \equiv 0 \pmod{8}$ . Hvis  $n$  er lige, er  $3^n \equiv 1 \pmod{8}$ , og hvis  $n$  er ulige, er  $3^n \equiv 3 \pmod{8}$ . Blot ved at se på ligningen modulo 8 kan man altså konstatere at der ikke findes løsninger når  $m \geq 3$ . Det ses nu let at den eneste løsning er  $n = 1$  og  $m = 2$ .

*Opgave 1.6.8.* Bestem alle positive heltallige løsninger til  $7^n = 3 + 2^m$ .

*Opgave 1.6.9.* Bestem alle positive heltallige løsninger til  $6(x! + 3) = y^2 + 5$ .

Opgave 1.6.10. For hvilke positive hele tal  $n$  går 1599 op i  $46^n + 34^n - 7^n - 5^n$ ?  
(Hint:  $1599 = 39 \cdot 41$ .)

Opgave 1.6.11. Antag at  $n \in \mathbb{N}$ , og at  $d_1 < d_2 < d_3 < d_4$  er de fire mindste positive divisorer i  $n$ . Bestem samtlige  $n$  som opfylder at

$$n = d_1^2 + d_2^2 + d_3^2 + d_4^2.$$

Hint: 43

Opgave 1.6.12. Bestem alle heltallige løsninger til  $19x^3 - 84y^2 = 1984$ . Hint: 4

Opgave 1.6.13. Bestem det mindste  $k \in \mathbb{N}$  således at der findes  $n, m \in \mathbb{N}$  med  $k = 19^n - 5^m$ . (Baltic Way 1999) Hint: 46

## 1.7 Nyttige faktoriseringer

Nu skal vi se på nogle nyttige faktoriseringer som man har brug for i rigtig mange sammenhænge.

Opgave 1.7.1. Reducér udtrykkene

$$\frac{a^2 - b^2}{a - b}, \quad \frac{a^3 - b^3}{a - b}, \quad \frac{a^4 - b^4}{a - b}, \quad \frac{a^3 + b^3}{a + b} \quad \text{og} \quad \frac{a^5 + b^5}{a + b}.$$

**Sætning 1.7.1.** Lad  $n$  være et positivt heltal. Da er

- i)  $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + b^{n-1})$ .
- ii) For ulige  $n$ :  $a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + b^{n-1})$ .
- iii)  $a^{2^n} - b^{2^n} = (a - b)(a + b)(a^2 + b^2) \dots (a^{2^{n-1}} + b^{2^{n-1}})$ .

**Bevis.** i) og ii) følger umiddelbart når man ganger parenteserne på højresiden sammen:

$$\begin{aligned} & (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + b^{n-1}) \\ &= a^n - a^{n-1} \cdot b + a^{n-1} \cdot b - a^{n-2} \cdot b^2 + a^{n-2} \cdot b^2 - a^{n-3} \cdot b^3 + \dots + a \cdot b^{n-1} - b^n \\ &= a^n - b^n \end{aligned}$$

$$\begin{aligned} & (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots + b^{n-1}) \\ &= a^n + a^{n-1} \cdot b - a^{n-1} \cdot b + a^{n-2} \cdot b^2 + a^{n-2} \cdot b^2 + a^{n-3} \cdot b^3 + \dots + a \cdot b^{n-1} + b^n \\ &= a^n + b^n \end{aligned}$$

Ved at omskrive vha. kvadratsætningerne  $n$  gange fås iii):

$$\begin{aligned} a^{2^n} - b^{2^n} &= (a^{2^{n-1}} - b^{2^{n-1}})(a^{2^{n-1}} + b^{2^{n-1}}) \\ &= (a^{2^{n-2}} - b^{2^{n-2}})(a^{2^{n-2}} + b^{2^{n-2}})(a^{2^{n-1}} + b^{2^{n-1}}) \\ &\quad \vdots \\ &= (a - b)(a + b)(a^2 + b^2) \dots (a^{2^{n-1}} + b^{2^{n-1}}). \quad \square \end{aligned}$$



**Eksempel 1.7.1.** Faktoriseringerne kan fx benyttes hvis man ønsker at vise at  $a^9 + b^9$  delelig med 81, når  $a + b$  er delelig med 9.

Antag at  $a + b$  er delelig med 9, og altså at  $a \equiv -b \pmod{9}$ . Først faktorerer vi  $a^9 + b^9$  vha. sætning 1.7.1.

$$\begin{aligned} a^9 + b^9 &= \\ (a + b)(a^8 - a^7b + a^6b^2 - a^5b^3 + a^4b^4 - a^3b^5 + a^2b^6 - ab^7 + b^8). \end{aligned}$$

Vi ved at  $a + b$  er delelig med 9, dvs. vi skal blot vise at den anden faktor også er delelig med 9, for at vise at  $a^9 + b^9$  er delelig med  $9^2 = 81$ . Da  $a \equiv -b \pmod{9}$ , er

$$\begin{aligned} a^8 - a^7b + a^6b^2 - \dots + a^2b^6 - ab^7 + b^8 &\equiv b^8 + b^8 + \dots + b^8 \\ &= 9b^8 \\ &\equiv 0 \pmod{9}. \end{aligned}$$

Dermed er  $a^9 + b^9$  delelig med 81.

*Opgave 1.7.2.* Lad  $a$  og  $b$  være hele tal, og lad  $n$  være et positivt heltal. Vis at hvis  $d$  er en positiv divisor i  $n$ , da går  $a^d - b^d$  op i  $a^n - b^n$ .

*Opgave 1.7.3.* Vis at hvis  $a^n - 1$  er et primtal for positive hele tal  $a$  og  $n$  med  $n > 1$ , da er  $a = 2$ , og  $n$  er et primtal.

*Opgave 1.7.4.* Bestem det største hele tal  $n$  så  $n + 10$  går op i  $n^3 + 100$ .

**Sætning 1.7.2.** Lad  $n$  være et positivt heltal større end 1 med primfaktoropløsning  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ . Tallet  $\sigma(n)$  er summen af alle positive divisorer i  $n$ . Så gælder

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

*Opgave 1.7.5.* Vis sætningen.

*Opgave 1.7.6.* Lad  $n \geq 3$  være et ulige tal. Vis at  $n^2$  går op i  $1^n + 2^n + \dots + n^n$ .  
*Hint: 27*

### Definition af den $p$ -adiske valuation

For et helt tal  $n$  og et primtal  $p$  er den  $p$ -adiske valuation  $v_p(n)$  det største hele tal  $\alpha$  som opfylder at  $p^\alpha$  går op i  $n$ . Specielt er  $v_p(0) = \infty$ .

Fx er  $v_2(24) = 3$ ,  $v_3(16) = 0$  og  $v_5(100) = 2$ .

Den  $p$ -adiske valuation kan i mange sammenhænge være praktisk. I kapitel 1.15 går vi i dybden med flere af dens egenskaber, men for nu nøjes vi med en grundlæggende regneregul, som vi allerede har brugt flere gange uden at nævne den, og som følger direkte af Aritmetikens fundamentalsætning.

**Sætning 1.7.3.** Lad  $a$  og  $b$  være hele tal og  $p$  et primtal. Da er

$$v_p(a \cdot b) = v_p(a) + v_p(b).$$

*Opgave 1.7.7.* Lad  $p$  være et primtal og  $a$  et positivt heltal, hvor  $v_p(a - 1) > 0$ . Lad yderligere  $k$  være et positivt heltal som ikke er delelig med  $p$ . Vis at da er

$$v_p(a - 1) = v_p(a^k - 1).$$

*Opgave 1.7.8.* Bestem  $v_2(3^{1024} - 1)$ .

*Opgave 1.7.9.* Antag at  $m$  er et ulige positivt tal som ikke er delelig med 5, og at  $a$  og  $n$  er positive heltal. Vis at hvis  $2^m + 3^m = a^n$ , da er  $n = 1$ . *Hint: 5*

*Opgave 1.7.10.* Lad  $a$ ,  $b$  og  $m$  være positive heltal. Vis at

$$\gcd(m^a - 1, m^b - 1) = m^{\gcd(a,b)} - 1.$$

*Hint: 47*

*Opgave 1.7.11.* Vis at ethvert tal der består af  $2^n$  ens cifre, har mindst  $n$  forskellige primfaktorer. *Hint: 7*

En anden nyttig formel er binomialformlen:

#### Sætning 1.7.4. Binomialformlen

Lad  $n$  være et positivt helt tal. Da er

$$(a + b)^n = a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-1} a^1 b^{n-1} + b^n.$$

**Bevis.** Formlen følger af at når man ganger ud, svarer hvert led til at man vælger  $a$  fra  $i$  parenteser og  $b$  fra  $n - i$  parenteser, dvs. alle led er på formen  $a^i b^{n-i}$ , og leddet  $a^i b^{n-i}$  forekommer netop  $\binom{n}{i}$  gange.  $\square$

**Eksempel 1.7.2.** Binomialformlen kan fx bruges hvis vi ønsker at bestemme de to sidste cifre i  $3^{86}$ . Bemærk at

$$3^{86} = 9^{43} = (10 - 1)^{43} \equiv \binom{43}{42} 10 - 1 = 430 - 1 \equiv 29 \pmod{100}.$$

Her udnytter vi at alle på nær de to sidste led når vi udregner  $(10 - 1)^{43}$  vha. binomialformlen, er delelige med 100. Dette er en metode der kan bruges i mange sammenhænge.

*Opgave 1.7.12.* Bestem de fire sidste cifre i  $99^{703}$ .

*Opgave 1.7.13.* Lad  $a$  og  $b$  være to positive indbyrdes primiske heltal, hvor  $b > 1$ . Bestem det største hele tal  $n$  så  $(b^2 + a)^b - a^b$  er delelig med  $b^n$ . *Hint:* 44

## 1.8 Primiske rester og Eulers $\phi$ -funktion

### Definition af primisk rest

Lad  $n \in \mathbb{N}$  og  $a \in \mathbb{Z}$ . Tallet  $a$  er en *primisk rest* modulo  $n$  hvis  $\gcd(a, n) = 1$ .

**Sætning 1.8.1.** Lad  $n \in \mathbb{N}$  og  $a, b \in \mathbb{Z}$ .

- i) Hvis  $a \equiv b \pmod{n}$ , og  $a$  er en primisk rest modulo  $n$ , da er  $b$  også en primisk rest modulo  $n$ .
- ii) Hvis  $a$  og  $b$  er primiske rester modulo  $n$ , da er  $ab$  også en primisk rest modulo  $n$ .

**Bevis.** i) Antag at  $\gcd(n, a) = 1$ . Hvis  $a \equiv b \pmod{n}$ , vil  $n \mid a - b$ , og der findes dermed et  $q \in \mathbb{Z}$  så  $a = qn + b$ . Hvis  $d$  er divisor i  $\gcd(n, b)$ , må  $d$  derfor også være divisor i  $a$  og altså i  $\gcd(n, a) = 1$ . Dermed er  $b$  også en primisk rest modulo  $n$ .

ii) Antag at  $\gcd(n, a) = 1$  og  $\gcd(n, b) = 1$ . Dette viser at  $n$  og  $a$  ikke har en fælles primfaktor, og at  $n$  og  $b$  ikke har en fælles primfaktor. Da primfaktoropløsningen af  $ab$  er produktet af primfaktoropløsningen af  $a$  og primfaktoropløsningen af  $b$ , kan  $n$  og  $ab$  heller ikke have en fælles primfaktor, og dermed er  $ab$  også en primisk rest modulo  $n$ .  $\square$

### Definition af primisk restklasse

Sætningens første del viser at hvis en repræsentant for en restklasse er en primisk rest modulo  $n$ , da er alle andre repræsentanter for restklassen også primiske med  $n$ . Vi kan derfor nu definere en primisk restklasse:

En restklasse repræsenteret ved tallet  $a$  modulo  $n$  kaldes *primisk* med  $n$  hvis  $a$  er primisk med  $n$ .

Sætningens anden del viser at når vi ganger to primiske rester, får vi igen en primisk rest.



### Definition af Eulers $\phi$ -funktion

Lad  $n \in \mathbb{N}$ . Eulers  $\phi$ -funktion  $\phi(n)$  er per definition antallet af primiske restklasser modulo  $n$ .

Fx er restklasser modulo 12 repræsenteret ved 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. Af disse er det netop restklasserne 1, 5, 7, 11 der er primiske med 12, dvs. at  $\phi(12) = 4$ .

Opgave 1.8.1. Bestem  $\phi(3)$ ,  $\phi(4)$ ,  $\phi(5)$ , ...,  $\phi(19)$ .

**Sætning 1.8.2.** For et primtal  $p$  gælder at

$$\phi(p) = p - 1.$$

**Bevis.** Samtlige restklasser modulo  $p$  er repræsenteret ved  $0, 1, 2, \dots, p-1$ , og blandt disse er det kun 0 der ikke er primisk med  $p$ . Dermed er  $\phi(p) = p - 1$ .

□

**Sætning 1.8.3.** For et primtal  $p$  og  $\alpha \in \mathbb{N}$  gælder at

$$\phi(p^\alpha) = p^{\alpha-1}(p-1).$$

**Bevis.** Samtlige restklasser modulo  $p^\alpha$  er repræsenteret ved  $0, 1, 2, \dots, p^\alpha - 1$ , og blandt disse er det netop de  $p^{\alpha-1}$  multipla af  $p$

$$0, p, 2p, \dots, (p^{\alpha-1} - 1)p$$

der ikke er primiske med  $p^\alpha$ . Altså er

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1). \quad \square$$

Inden vi ser mere på Eulers  $\phi$ -funktion, skal vi se på hvorfor primiske rester er så interessante. Da vi tidligere løste ligninger ved at betragte dem modulo et positivt heltal  $n$ , manglede vi en forkortningsregel der sagde at  $a \cdot b \equiv a \cdot c \pmod{n}$  medfører at  $b \equiv c \pmod{n}$ . Det viser sig at denne regel gælder når  $a$  er en primisk rest modulo  $n$ , og det er en helt central årsag til at primiske rester er så interessante.

### Definition af multiplikativ invers

Lad  $n \in \mathbb{N}$ , og lad  $a \in \mathbb{Z}$ . Et helt tal  $b$  som opfylder at

$$a \cdot b \equiv 1 \pmod{n}$$

kaldes en *multiplikativ invers* til  $a$  modulo  $n$ , eller nogle gange blot en *invers* til  $a$  modulo  $n$ . Den multiplikative inverse til  $a$  betegnes  $a^{-1}$ , og den er ifølge sætningen nedenfor entydig modulo  $n$  hvis den findes.

**Sætning 1.8.4.** Lad  $n \in \mathbb{N}$ . Tallet  $a \in \mathbb{Z}$  har en multiplikativ invers modulo  $n$  netop når  $a$  er en primisk rest modulo  $n$ . Den multiplikative inverse er entydigt bestemt modulo  $n$ .

**Bevis.** Antag at  $a$  er en primisk rest modulo  $n$ , dvs. at  $\gcd(n, a) = 1$ . Ifølge Bezouts identitet findes  $s, t \in \mathbb{Z}$  så  $1 = sa + tn$ . Tallet  $s$  opfylder altså at  $as \equiv 1 \pmod{n}$ , hvilket viser at der findes en multiplikativ invers til  $a$  modulo  $n$ .

For at vise at den multiplikative inverse er entydigt bestemt, antager vi at  $ab \equiv 1 \pmod{n}$  og  $ac \equiv 1 \pmod{n}$ . Dette viser at

$$c \equiv (ba)c \equiv b(ac) \equiv b \pmod{n}.$$

Altså er den multiplikative inverse restklasse til  $a$  entydigt bestemt modulo  $n$ .

Antag til slut at  $a$  ikke er en primisk rest modulo  $n$ . Da vil  $d = \gcd(n, a) > 1$  gå op i både  $n$  og alle multipla af  $a$ , og der findes derfor ikke et helt tal  $s$  så  $sa \equiv 1 \pmod{n}$ . □

**Sætning 1.8.5.** Lad  $n \in \mathbb{N}$  og  $a, b, c \in \mathbb{Z}$ . Hvis  $a$  er primisk med  $n$  gælder at

$$a \cdot b \equiv a \cdot c \pmod{n} \Rightarrow b \equiv c \pmod{n}.$$

**Bevis.** Antag at  $a$  er primisk med  $n$ , og at  $a \cdot b \equiv a \cdot c \pmod{n}$ . Da  $a$  er primisk med  $n$ , ved vi fra sætning 1.8.4 at  $a$  har en multiplikativ invers  $a^{-1}$ , dvs. at

$$a^{-1} \cdot a \cdot b \equiv a^{-1} \cdot a \cdot c \pmod{n},$$

og altså  $b \equiv c \pmod{n}$ .  $\square$

**Eksempel 1.8.1.** Denne sætning er en slags forkortningsregel, og den gør det muligt at løse ligninger af typen

$$ax + b \equiv c \pmod{n},$$

når  $a$  er primisk med  $n$ .

Hvis vi fx ønsker at løse ligningen

$$5x + 1 \equiv 7 \pmod{9},$$

kan vi først trække 1 fra på begge sider:

$$5x \equiv 6 \pmod{9}.$$

For at fjerne 5-tallet skal vi nu gange med den multiplikative inverse til 5 modulo 9. Ved at prøve sig lidt frem ses at denne er 2. Ved at gange med 2 på begge sider fås

$$x \equiv 2 \cdot 6 \equiv 3 \pmod{9}.$$

Løsningen til ligningen er altså restklassen 3 modulo 9.

*Opgave 1.8.2.* a) Bestem samtlige primiske restklasser modulo 15, og bestem den multiplikative inverse til hver af dem. b) Løs ligningen  $7x + 19 \equiv 36 \pmod{15}$ .

*Opgave 1.8.3.* Lad  $p$  være et primtal. Vis at de eneste restklasser modulo  $p$  som er deres egen multiplikative inverse, er restklasserne 1 og  $p - 1$ .

**Sætning 1.8.6.** Lad  $k \in \mathbb{N}$ , og lad  $a_0, a_1, \dots, a_{k-1}$  være repræsentanter for samtlige restklasser modulo  $k$ . Hvis  $m, r \in \mathbb{Z}$ , og  $m$  er primisk med  $k$ , da repræsenterer de  $k$  tal

$$ma_0 + r, \quad ma_1 + r, \quad ma_2 + r, \quad \dots, \quad ma_{k-1} + r$$

også samtlige restklasser modulo  $k$ .

**Bevis.** Hvis vi viser at de  $k$  restklasser repræsenteret ved

$$ma_0 + r, \quad ma_1 + r, \quad ma_2 + r, \quad \dots, \quad ma_{k-1} + r$$

alle er forskellige modulo  $k$ , da må de netop repræsentere samtlige  $k$  restklasser modulo  $k$ . Antag at  $ma_i + r \equiv ma_j + r \pmod{k}$ . Da  $k$  og  $m$  er indbyrdes primiske, kan vi forkorte med  $m$  når vi regner modulo  $k$ , og dermed er

$$ma_i + r \equiv ma_j + r \Leftrightarrow ma_i \equiv ma_j \Leftrightarrow a_i \equiv a_j \pmod{k}.$$

Dette viser at de  $k$  restklasser

$$ma_0 + r, \quad ma_1 + r, \quad ma_2 + r, \quad \dots, \quad ma_{k-1} + r$$

alle er forskellige og derfor udgør samtlige restklasser.  $\square$

**Sætning 1.8.7.** Lad  $m, k \in \mathbb{N}$ , og antag at  $m$  og  $k$  er indbyrdes primiske. Da er

$$\phi(mk) = \phi(m) \cdot \phi(k).$$



**Bevis.** Lad  $m, k \in \mathbb{N}$ , og antag at  $m$  og  $k$  er indbyrdes primiske. De  $mk$  restklasser modulo  $mk$  er repræsenteret ved resterne  $0, 1, 2, \dots, mk-1$ . Vi opstiller nu disse rester således

$$\begin{array}{cccccc}
 0 & 1 & 2 & \dots & m-1 & \\
 m & m+1 & m+2 & \dots & m+(m-1) & \\
 2m & 2m+1 & 2m+2 & \dots & 2m+(m-1) & \\
 \vdots & \vdots & \vdots & & \vdots & \\
 (k-1)m & (k-1)m+1 & (k-1)m+2 & \dots & (k-1)m+(m-1) & 
 \end{array}$$

Der er netop  $\phi(m)$  rester som er primiske med  $m$  blandt resterne  $0, 1, 2, \dots, m-1$ , dvs. at de rester i skemaet som er primiske med  $m$  netop er placeret i  $\phi(m)$  søjler. Hver af disse søjler indeholder ifølge sætning 1.8.6 netop samtlige restklasser modulo  $k$ , dvs. der er netop  $\phi(k)$  af dem som er primiske med  $k$ . Samlet er antallet af restklasser som både er primiske med  $k$  og primiske med  $m$  altså  $\phi(m)\phi(k)$ . De restklasser som både er primiske med  $m$  og primiske med  $k$ , er netop dem der er primiske med  $mk$ . Dette giver det ønskede.  $\square$

**Sætning 1.8.8.** Lad  $n \in \mathbb{N}$  med primfaktoropløsning  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ , hvor  $p_i$ 'erne er forskellige. Da er

$$\phi(n) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_m^{\alpha_m-1}(p_m-1).$$

Opgave 1.8.4. Bevis sætningen.

Opgave 1.8.5. Bestem  $\phi(120)$  og  $\phi(98)$ .

Opgave 1.8.6. Bestem alle  $n$  så  $\phi(n) = 8$ , og alle  $m$  så  $\phi(m) = 14$ .

Opgave 1.8.7. Lad  $n, \alpha \in \mathbb{N}$ . Vis at  $\phi(n^\alpha) = n^{\alpha-1}\phi(n)$ .

Opgave 1.8.8. Lad  $n$  være et heltal større end 1. Vis at

$$\sum_{d|n} \phi(d) = n,$$

hvor  $d$  er samtlige positive divisorer i  $n$ . *Hint:* 6

## 1.9 Wilsons sætning

### Sætning 1.9.1. Wilsons sætning

For ethvert primtal  $p$  gælder

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

**Bevis.** For  $p = 2$  er  $(2-1)! = 1 \equiv -1 \pmod{2}$ . Antag at  $p$  er et primtal større end 2. Ifølge opgave 1.8.3 er de eneste af de primiske rester modulo  $p$  som er deres egen inverse, resterne 1 og  $p-1$ . Hvis vi betragter de primiske rester  $1, 2, \dots, p-1$  kan alle pånær 1 og  $p-1$  parres med deres inverse. Dermed er

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}. \quad \square$$

Opgave 1.9.1. Bestem alle positive heltal  $n$  for hvilke  $n$  går op i  $(n-1)! + 1$ .

Opgave 1.9.2. Er det muligt at dele en mængde bestående af ti på hinanden følgende positive heltal i to disjunkte delmængder som samlet indeholder alle ti tal, så produktet af elementerne i hver af de to delmængder bliver det samme tal? (*Disjunkte* mængder er mængder der ikke har nogen elementer til fælles). *Hint:* 40

**Bemærkning.** Det er et kendt resultat af matematikerne Erdős og Selfridge at produktet af to eller flere på hinanden følgende positive heltal aldrig er en potens af et helt tal. Det var i mange år en formodning og blev først vist generelt af de to matematikere i 1974. (En *potens af et helt tal* er et tal på formen  $n^m$ , hvor  $m, n \in \mathbb{Z}$ , og  $m > 1$ ).

Af dette følger også at produktet af to eller flere på hinanden følgende positive heltal ikke er et kvadrattal, og at man derfor ikke kan skrive dette produkt som produktet af to ens faktorer.

Opgave 1.9.3. Vis at hvis et primtal er på formen  $p = 4n+1$ , da er  $-1$  kvadratisk rest modulo  $p$ . *Hint:* 39

## 1.10 Fermats lille sætning og Eulers sætning

### Sætning 1.10.1. Eulers sætning

Lad  $n \in \mathbb{N}$  og  $a \in \mathbb{Z}$ . Hvis  $a$  er primisk med  $n$ , er

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

**Bevis.** Lad  $a_1, a_2, \dots, a_{\phi(n)}$  være repræsentanter for de i alt  $\phi(n)$  primiske restklasser modulo  $n$ . Tallene

$$a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{\phi(n)}$$

er også primiske rester ifølge sætning 1.8.1, og de er desuden forskellige ifølge sætning 1.8.5 da vi kan forkorte med  $a$  når  $a$  er primisk med  $n$ . De er altså også netop samtlige primiske rester modulo  $n$ . Dermed er

$$\begin{aligned} a_1 \cdot a_2 \cdots a_{\phi(n)} &\equiv (a \cdot a_1)(a \cdot a_2) \cdots (a \cdot a_{\phi(n)}) \\ &= a^{\phi(n)} \cdot a_1 \cdot a_2 \cdots a_{\phi(n)} \pmod{n}. \end{aligned}$$

Da  $a_i$ 'erne alle er primiske med  $n$ , kan vi forkorte og få

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

Et vigtigt specialtilfælde af Eulers sætning er Fermats lille sætning:

### Sætning 1.10.2. Fermats lille sætning

Lad  $p$  være et primtal, og lad  $a \in \mathbb{Z}$  være primisk med  $p$ . Da er

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

**Korollar 1.10.3.** Lad  $p$  være et primtal, og lad  $a \in \mathbb{Z}$ . Da er

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

Opgave 1.10.1. Bevis korollaret.

Opgave 1.10.2. Vis at  $a^{13} \equiv a \pmod{2730}$  for alle hele tal  $a$ .

Eulers sætning kan også bruges til at vise en af mange interessante forskelle på primtal på formen  $4m + 1$  og primtal på formen  $4m + 3$ .

**Sætning 1.10.4.** Hvis et primtal er på formen  $p = 4m + 1$  for et helt tal  $m$ , da er  $-1$  kvadratisk rest modulo  $p$ .

Hvis et primtal er på formen  $p = 4m + 3$  for et helt tal  $m$ , da er  $-1$  ikke kvadratisk rest modulo  $p$ .

**Bevis.** Ifølge opgave 1.9.3 er  $-1$  er kvadratisk rest modulo et primtal  $p$  på formen  $p = 4m + 1$ .

Antag nu at  $p$  er et primtal  $p$  på formen  $p = 4m + 3$ , og at der findes et helt tal  $x$  så  $x^2 \equiv -1 \pmod{p}$ . Da er

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

men ifølge Eulers sætning er  $x^{4m+2} \equiv 1 \pmod{p}$ , hvilket er en modstrid. Altså er  $-1$  ikke kvadratisk rest for noget primtal på formen  $p = 4n + 3$ .  $\square$

**Eksempel 1.10.1.** Eulers sætning kan også benyttes til at reducere eksponenten hvis man fx ønsker at udregne  $6^{162} \pmod{25}$ . Da

$$\phi(25) = \phi(5^2) = (5-1)5 = 20,$$

og 6 er primisk med 25, er  $6^{20} \equiv 1 \pmod{25}$  ifølge Eulers sætning. Dermed er

$$6^{162} = 6^2(6^{20})^8 \equiv 6^2 \cdot 1^8 \equiv 11 \pmod{25}.$$

Opgave 1.10.3. Bestem  $17^{1601} \pmod{32}$ .



**Sætning 1.10.5.** Lad  $n, a, b \in \mathbb{N}$ , og lad  $m \in \mathbb{Z}$  være en primisk rest modulo  $n$ . Antag at  $a \equiv b \pmod{\phi(n)}$ . Da er

$$m^a \equiv m^b \pmod{n}.$$

Opgave 1.10.4. Bevis sætningen.

**Eksempel 1.10.2.** Nu kan vi endnu mere direkte reducere eksponenten ved et regne modulo  $\phi(n)$ . Hvis vi fx ønsker at bestemme de to sidste cifre i  $797^{323}$ , skal vi regne modulo 100. Da  $\phi(100) = \phi(2^2)\phi(5^2) = 40$ , og 797 er primisk med 100, kan vi regne modulo 100 på grundtallet 797 og modulo  $\phi(100) = 40$  på eksponenten 323:

$$797^{323} \equiv (-3)^3 \equiv 73 \pmod{100}.$$

Opgave 1.10.5. Findes der hele tal  $x_1, x_2, \dots, x_k$  med sum 1492 som opfylder at  $x_1^7 + x_2^7 + \dots + x_k^7 = 70707$ ?

Opgave 1.10.6. Bestem de to sidste cifre i  $3^{214} \cdot 97^{828} \cdot 13^{521}$ .

Opgave 1.10.7. Bestem sidste cifre i  $\underbrace{7^{7^{7^{\dots}}}}_{1000}$ .

Opgave 1.10.8. Bestem de tre sidste cifre i  $4007^{4003^{4001}}$ .

Opgave 1.10.9. Bestem de sidste tre cifre i  $2003^{2002^{2001}}$ . *Hint: 35*

**Eksempel 1.10.3.** Findes der et helt tal  $n$  hvis cifre er lutter 1-taller, således at  $n$  er delelig med 1999?

Ja, og det kan man benytte Eulers sætning til at vise. Tal hvis cifre kun er 1-taller, er på formen

$$\frac{10^m - 1}{9},$$

og derfor er vi interesserede i at finde et  $m$  så  $10^m - 1$  er delelig med 1999.

Da 1999 er et primtal, er 10 og 1999 indbyrdes primiske og  $\phi(1999) = 1998$ . Ifølge Eulers sætning er

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

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

Opgaven er fra Georg Mohr-Konkurrencen 1999, og den kan faktisk også løses alene ved brug af skuffeprikket og simple overvejelser om rester.

Opgave 1.10.10. Vis at hvis  $m \in \mathbb{N}$  ikke er delelig med 2 eller 5, da findes uendeligt mange hele tal  $n$  hvis cifre er lutter 1-taller, så  $n$  er delelig med  $m$ . (*Advarsel: Pas på primfaktoren 3.*)

Opgave 1.10.11. Antag at  $n, k \geq 2$  er to hele tal. Vis at da er mindst et af tallene  $p = n + k^n$  og  $q = nk^{(k^n - 1)} + 1$  ikke et primtal. *Hint: 22*

## 1.11 Orden

**Eksempel 1.11.1.** Betragt følgen af potenser

$$2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, \dots$$

modulo 5:

$$1, 2, 4, 3, 1, 2, 4, 3, 1, \dots$$

Vi lægger hurtigt mærke til at følgen modulo 5 er periodisk med periode-længde 4. Tallet  $m = 4$  er det mindste positive hele tal så  $2^m \equiv 1 \pmod{5}$ , og det er oplagt at perioden derfor vil gentage sig med længde 4.

Som vi skal se i den følgende definition, kalder vi 4 for ordenen af 2 modulo 5.

### Definition af orden

Lad  $n \in \mathbb{N}$ , og lad  $a \in \mathbb{Z}$  være primisk med  $n$ . Ordenen af  $a$  modulo  $n$  er det mindste positive heltal  $m$  så  $a^m \equiv 1 \pmod{n}$ . Ordenen betegnes  $\text{ord}_n(a)$ .

Bemærk at det følger af Eulers sætning at der findes et sådant tal.

Opgave 1.11.1. Bestem  $\text{ord}_9(2)$ ,  $\text{ord}_8(3)$  og  $\text{ord}_{10}(7)$ .

**Sætning 1.11.1.** Lad  $n, k \in \mathbb{N}$ , og lad  $a \in \mathbb{Z}$  være primisk med  $n$ . Da er

$$a^k \equiv 1 \pmod{n}$$

hvis og kun hvis  $\text{ord}_n(a)$  er divisor i  $k$ .

Specielt er  $\text{ord}_n(a)$  divisor i  $\phi(n)$ .

Opgave 1.11.2. Bevis sætningen.

**Sætning 1.11.2.** Lad  $n, m, k \in \mathbb{N}$ , og lad  $a \in \mathbb{Z}$  være primisk med  $n$ . Antag at  $a^m \equiv 1 \pmod{n}$  og  $a^k \equiv 1 \pmod{n}$ . Da gælder at

$$a^{\text{gcd}(m,k)} \equiv 1 \pmod{n}.$$

Opgave 1.11.3. Bevis sætningen.

**Eksempel 1.11.2.** Hvis vi ønsker at løse ligningen

$$x^3 \equiv 1 \pmod{64},$$

så kan vi udnytte at et  $x$  der opfylder ligningen, må være primisk med 64, dvs. der gælder ifølge Eulers sætning at  $x^{\phi(64)} \equiv 1 \pmod{64}$ . Ifølge sætning 1.8.3 er  $\phi(64) = \phi(2^6) = 2^5 = 32$ . Nu ved vi at  $x$  opfylder at  $x^3 \equiv 1 \pmod{64}$  og  $x^{32} \equiv 1 \pmod{64}$ . Det følger derfor af sætning 1.11.2 at

$$1 \equiv x^{\text{gcd}(3,32)} = x \pmod{64},$$

dvs. den eneste løsning til ligningen  $x^3 \equiv 1 \pmod{64}$  er restklassen 1 modulo 64.

### Definition af Mersennetal

Tallene  $M_n = 2^n - 1$ , hvor  $n \in \mathbb{N}$ , kaldes *Mersennetal*, og man har vist at  $M_n$  er et primtal for  $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 87$  samt en del flere. Man formoder at der findes uendeligt mange Mersennetal som er primtal, men det er ikke bevist. Det største kendte Mersenneprimtal er i skrivende stund  $M_{82.589.933}$ , og det blev fundet i 2018.

Opgave 1.11.4. Lad  $p$  være et ulige primtal. Vis at hvis  $q$  er primfaktor i Mersennetallet  $M_p = 2^p - 1$ , da er  $q$  på formen  $q = 2pk + 1$  for et positivt heltal  $k$ .  
*Hint:* 1

Opgave 1.11.5. Lad  $a > 1$  og  $n$  være positive heltal. Vis at hvis  $p$  er en ulige primfaktor i  $a^{2^n} + 1$ , da er  $p - 1$  delelig med  $2^{n+1}$ .  
*Hint:* 42



**Eksempel 1.11.3.** Lad  $n$  være et ulige tal større end 1. For at vise at  $n$  ikke går op i  $3^n + 1$ , antager vi det modsatte og søger at opnå en modstrid.

Antag derfor at der findes et ulige tal  $n$  større end 1 så  $n$  går op i  $3^n + 1$ . Lad  $p$  være den mindste primfaktor i  $n$ . Det smarte ved at vælge den mindste primfaktor i  $n$  er at da har  $n$  og  $\phi(p) = p - 1$  ingen fælles primfaktorer, dvs.  $\gcd(n, p - 1) = 1$ . Dette kan vi nemlig udnytte når vi ser på ordenen af 3 modulo  $p$  på følgende måde.

Da  $p \mid 3^n + 1$ , er  $3^n \equiv -1 \pmod{p}$ , og  $p \neq 3$ . Dette kan fortælle os noget om ordenen af 3 modulo  $p$ . Vi har nemlig nu at

$$3^{2n} \equiv (3^n)^2 \equiv (-1)^2 \equiv 1 \pmod{p},$$

og altså at  $\text{ord}_p(3)$  går op i  $2n$  ifølge sætning 1.11.1. Da  $\text{ord}_p(3)$  også går op i  $\phi(p) = p - 1$ , må  $\text{ord}_p(3)$  gå op i  $\gcd(2n, p - 1)$ . Fordi  $p$  er ulige, og  $\gcd(n, p - 1) = 1$ , må  $\gcd(2n, p - 1) = 2$ . Men da er  $\text{ord}_p(3) = 1$  eller  $\text{ord}_p(3) = 2$ , og altså  $3 \equiv 1 \pmod{p}$  eller  $3^2 \equiv 1 \pmod{p}$ , hvilket ikke er sandt for noget ulige primtal. Vi har derfor opnået en modstrid og vist at  $n$  ikke går op i  $3^n + 1$  for noget ulige tal  $n$  større end 1.

**Bemærkning.** I eksemplet valgte vi den mindste primfaktor  $p$  i  $n$  fordi vi så ved at  $\phi(p) = p - 1$  er primisk med  $n$ , og det er et trick der er værd at skrive sig bag øret da det er anvendeligt i en del sammenhænge.

*Opgave 1.11.6.* Vis at  $2^n - 1$  ikke er delelig med  $n$  for noget positivt heltal  $n$ ,  $n > 1$ .

*Opgave 1.11.7.* Lad  $p$  være et ulige primtal, og lad  $q$  og  $r$  være primtal således at  $p$  går op i  $q^r + 1$ . Vis at enten går  $2r$  op i  $p - 1$ , eller også går  $p$  op i  $q^2 - 1$ .

*Hint:* 13

*Opgave 1.11.8.* Bestem alle primtal  $p$  og  $q$  så  $pq$  går op i  $(5^p - 2^p)(5^q - 2^q)$ .

### Definition af Fermattal

Fermattallene er  $f_n = 2^{2^n} + 1$  for  $n = 0, 1, 2, \dots$ . Fermat studerede disse tal og opdagede at  $f_0, f_1, f_2, f_3$  og  $f_4$  var primtal. Han kom derfor med den forkerte påstand i 1650 at alle Fermattal er primtal. Der er p.t. ikke fundet nogen primtal for  $n \geq 5$ , og man ved i dag at Fermattallene  $f_5, f_6, f_7, \dots, f_{33}$  ikke er primtal.

Fermattallene vokser dog så stærkt at det absolut ikke er simpelt at undersøge om et Fermattal er et primtal, og det har taget mange år og en stor indsats fra mange matematikere at nå frem til det man ved om Fermattal i dag. Selv om man ved at Fermattallene  $f_5, f_6, f_7, \dots, f_{33}$  ikke er primtal, kender man ikke primfaktoriseringen af dem alle, fx kender man for  $f_{20}$  og  $f_{24}$  ikke en eneste faktor i dem, men har blot vist at de må være sammensatte tal.

Du kan læse mere om Fermattal i kapitel 1.17.

*Opgave 1.11.9.* Betragt Fermattallet  $f_n = 2^{2^n} + 1$ . Vis at hvis  $f_n$  går op i  $3^{(f_n-1)/2} + 1$ , da er  $f_n$  et primtal. *Hint:* 32

*Opgave 1.11.10.* Bestem alle par  $(x, p)$  af positive heltal så  $p$  er et primtal,  $x \leq 2p$ , og  $x^{p-1}$  går op i  $(p-1)^x + 1$ . (IMO shortlist 1999) *Hint:* 15

## 1.12 Følger

En del opgaver til internationale matematikkonkurrencer handler om følger af heltal som man typisk skal vise har en bestemt egenskab, fx at de er periodiske fra et vist trin, ikke indeholder kvadrattal, ....

### Definition af periodiske følger

En følge  $a_1, a_2, a_3 \dots$  kaldes *periodisk* hvis der findes et positivt helt tal  $m$  så  $a_{n+m} = a_n$  for alle  $n \in \mathbb{N}$ . Periodens længde er det mindste positive hele tal  $m$  med denne egenskab.

Følgen  $a_1, a_2, a_3, \dots$  kaldes *periodisk fra et vist trin* hvis der findes positive hele tal  $m$  og  $k$  så  $a_{n+m} = a_n$  for alle  $n \geq k$ .

### Eksempel 1.12.1. Betragt følgen modulo et smart tal

I følgen

$$1, 9, 7, 7, 4, 7, 5, 3, 9, 4, 1, \dots$$

er hvert ciffer fra og med det femte summen af de fire foregående modulo 10. I dette eksempel skal vi undersøge hvilken af disse talkombinationer der kan indgå i følgen: a) 1,2,3,4, b) 3,2,6,9, c) 0,1,9,7.

Da der kun findes et endeligt antal kombinationer med fire cifre, og det næste ciffer i følgen er entydigt bestemt af de fire foregående, vil følgen være periodisk fra et vist trin. Men da man ud fra fire cifre i følgen også entydigt kan bestemme det foregående ciffer, kan man fortsætte den uendeligt i begge retninger med en fast periode. Derfor er den periodisk helt fra starten.

I mange opgaver med følger kan man netop konkludere at følgen må være periodisk fra et vist trin da der kun er endeligt mange muligheder. Herefter skal man så overveje om det først er fra et vist trin at den er periodisk, eller om den som i dette eksempel er periodisk fra starten.

At følgen er periodisk betyder at 1,9,7,7 optræder igen længere fremme i følgen, og cifferet lige inden kan man regne ud, må være 0. Dermed optræder kombinationen 0, 1, 9, 7 i følgen.

Vi mangler stadig at finde ud af om 1,2,3,4 og 3,2,6,9 indgår i følgen. Da den er periodisk, kan man jo i princippet blive ved til man har fundet hele perioden, og så se om de indgår. Dette er dog ikke altid en god strategi da længden af perioden kan være temmelig stor. Det kan som regel betale sig at lede efter et andet system i følgen med en kortere periode. Reducerer vi i dette eksempel følgens cifre modulo 2, får vi 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, .... Her ud fra kan vi se at følgen har 1, 1, 1, 1, 0 som periode når vi regner modulo 2, og dette udelukker a) og b).

I dette eksempel blev følgens tal konstrueret modulo tallet 10, men det viste sig smart at reducere følgen yderligere modulo 2. At følgen er konstrueret modulo 10, og næste tal i følgen er entydigt bestemt ud fra de fire foregående, giver ifølge skuffeprikket at den er periodisk, og det er et standardtrick der kan benyttes i mange sammenhænge. Dette brugte vi til at vise at en kombination faktisk fandtes. Da vi regnede modulo 2 var til gengæld for at vise at noget ikke fandtes, så teknikken kan benyttes til begge dele.

*Opgave 1.12.1.* Følgen  $a_1, a_2, \dots$  er givet ved  $a_1 = a_2 = 1$  og  $a_{n+2} = a_n a_{n+1} + 1$  for  $n \geq 1$ . Vis at der ikke findes noget  $n$ ,  $n > 2$ , så  $a_n$  er et kvadrattal.

*Opgave 1.12.2.* Fibonaccitallene er defineret ved  $F_0 = 0$ ,  $F_1 = 1$  og  $F_n = F_{n-1} + F_{n-2}$  for  $n \geq 2$ . Vis at for ethvert helt tal  $k$  findes et positivt helt tal  $m$  så  $k$  går op i  $F_m$ .

*Opgave 1.12.3.* En følge af positive hele tal  $a_0, a_1, a_2, \dots$  er givet ved

$$a_0 = m \quad \text{og} \quad a_{n+1} = a_n^5 + 487, \quad n \geq 0.$$

Bestem de værdier af  $m$  for hvilke følgen indeholder flest muligt kvadrattal. (NMC 2006)

*Opgave 1.12.4.* Lad  $a_1, a_2, \dots$  være en følge af heltal med uendeligt mange positive og uendeligt mange negative tal. Antag at der for ethvert positivt heltal  $n$  fås  $n$  forskellige rester når tallene  $a_1, a_2, \dots, a_n$  deles med  $n$ . Vis at ethvert helt tal optræder netop én gang i talfølgen. (IMO 2005)



### Eksempel 1.12.2. Omskrivning af følge til ny følge

Når man skal arbejde med nogle følger, er det nemmere at omskrive til en anden følge og arbejde med den.

Om en følge af heltal  $a_0, a_1, a_2, \dots$  oplyses at  $a_0 < a_1$  og

$$a_n = 3a_{n-1} - 2a_{n-2} \text{ for } n > 1.$$

Vi ønsker at vise at  $a_m \equiv a_{m+1} \pmod{2^m}$  for alle positive heltal  $m$ .

Følgen er ikke periodisk, og da det tal vi er interesserede i at regne modulo, afhænger af indekset, kan vi heller ikke betragte følgen modulo et fast tal. I stedet udnytter vi rekursionsformlen  $a_n = 3a_{n-1} - 2a_{n-2}$  og omskriver på følgende måde:

$$a_n - a_{n-1} = 2a_{n-1} - 2a_{n-2} = 2(a_{n-1} - a_{n-2}),$$

Vi kan nu betragte en ny følge  $b_n = a_n - a_{n-1}$  hvis rekursionsformel er meget simplere, nemlig  $b_n = 2b_{n-1}$ . Dermed fås rekursivt at

$$b_{n+1} = 2b_n = \dots = 2^n b_1.$$

Altså er  $a_{m+1} - a_m = 2^m b_1$ , og derfor må  $a_m \equiv a_{m+1} \pmod{2^m}$  for alle positive heltal  $m$ .

Opgave 1.12.5. En følge  $x_0, x_1, x_2, \dots$  er givet ved  $x_0 = a$ ,  $x_1 = 2$  og

$$x_n = 2x_{n-1}x_{n-2} - x_{n-1} - x_{n-2} + 1, \quad n > 1.$$

Find alle hele tal  $a$  så  $2x_{3n} - 1$  er et kvadrattal for alle  $n \geq 1$ .

Opgave 1.12.6. Lad  $a$  være et helt tal. Følgen  $x_0, x_1, \dots$  er defineret ved  $x_0 = a$ ,  $x_1 = 3$  og

$$x_n = 2x_{n-1} - 4x_{n-2} + 3$$

for alle  $n > 1$ . Bestem det største hele tal  $k_a$  for hvilket der findes et primtal  $p$  så  $p^{k_a}$  går op i  $x_{2011} - 1$ . (BW 2011) *Hint: 21*

Opgave 1.12.7. Lad  $a_1$  og  $a_2$  være to positive hele tal. En følge af positive hele tal  $a_0, a_1, a_2, \dots$  er givet ved

$$a_{k+1} = \frac{a_k + a_{k-1}}{2015^i}, \quad k > 0,$$

hvor  $i$  for hvert  $k$  er den maksimale potens af 2015 som går op i  $a_k + a_{k-1}$ . Vis at hvis følgen er periodisk fra et vist trin, da er længden af perioden delelig med 3. (BW 2014) *Hint: 2*

Opgave 1.12.8. En følge af positive heltal  $a_1, a_2, a_3, \dots$  opfylder at hvis  $m, n \in \mathbb{N}$ ,  $m < n$  og  $m$  går op i  $n$ , da vil  $a_m$  gå op i  $a_n$ , og  $a_m < a_n$ . Bestem den mindst mulige værdi af  $a_{2000}$ . (Baltic Way 2000)

### 1.13 Den kinesiske restklassesætning

I nogle opgaver har man brug for at undersøge om der findes løsninger  $x$  til kongruenssystemer af typen

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \dots, \quad x \equiv a_m \pmod{n_m}.$$

Dette handler den kinesiske restklassesætning om.

#### Sætning 1.13.1. Den kinesiske restklassesætning

Lad  $n$  være et positivt heltal og  $n = n_1 n_2 \dots n_m$ , hvor  $\gcd(n_i, n_j) = 1$  når  $i \neq j$ . Da findes uendeligt mange heltallige løsninger  $x$  til kongruenssystemet

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_m \pmod{n_m}. \end{aligned}$$

Samtlige løsninger udgør netop en restklasse modulo  $n$ .

**Bevis.** Sætningen vises ved induktion efter  $m$ . Den er oplagt sand for  $m = 1$ . Betragt nu tilfældet  $m = 2$ . Vi ønsker at bestemme en løsning  $x$  til

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2}. \end{aligned}$$

En sådan løsning må være på formen  $x = a_1 + qn_1$ , hvor  $q \in \mathbb{Z}$  opfylder at  $a_1 + qn_1 \equiv a_2 \pmod{n_2}$ . Da  $\gcd(n_1, n_2) = 1$ , findes en invers  $n_1^{-1}$  til  $n_1$  modulo  $n_2$ . Dermed må  $q \equiv (a_2 - a_1)n_1^{-1} \pmod{n_2}$  opfylde det ønskede, dvs. at  $x = a_1 + (a_2 - a_1)n_1^{-1}n_1$  løser kongruenssystemet. Altså har kongruenssystemet løsninger.

Vi viser nu at samtlige løsninger netop udgør en restklasse modulo  $n$ . Det er klart at hvis  $y \equiv x \pmod{n}$ , da er  $y$  også en løsning. Antag nu at  $x$  og  $y$  er løsninger. Da vil både  $n_1$  og  $n_2$  gå op i  $x - y$ , og da  $\gcd(n_1, n_2) = 1$ , vil også  $n$  gå op i  $x - y$ . Dermed udgør løsningerne netop en restklasse modulo  $n$ .

Vi skal nu til selve induktionsskridtet, men har faktisk lavet alt arbejdet i tilfældet  $m = 2$ . Antag nu at sætningen gælder for  $m$ . Vi ønsker nu at vise at sætningen også gælder for  $m + 1$ . Lad  $n = n_1 n_2 \dots n_{m+1}$ , hvor  $\gcd(n_i, n_j) = 1$  når  $i \neq j$ . Betragt kongruenssystemet

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_{m+1} \pmod{n_{m+1}}. \end{aligned}$$

Ifølge induktionsantagelsen udgør samtlige løsninger til de  $m$  første kongruenser netop en restklasse modulo  $n' = n_1 n_2 \dots n_m$ . Lad  $a'$  være en repræsentant for denne restklasse. Løsningerne til kongruenssystemet

$$\begin{aligned} x &\equiv a' \pmod{n'} \\ x &\equiv a_{m+1} \pmod{n_{m+1}} \end{aligned}$$

er identiske med løsningerne til det oprindelige kongruenssystem, og de udgør ifølge induktionsantagelsen én restklasse modulo  $n' n_{m+1} = n$  da  $\gcd(n', n_{m+1}) = 1$ . Dermed er sætningen bevist.  $\square$

**Eksempel 1.13.1.** Vi ønsker ved hjælp af den kinesiske restklassesætning at bestemme samtlige løsninger til kongruenssystemet

$$\begin{aligned} x &\equiv 3 \pmod{7} \\ x &\equiv 2 \pmod{17}. \end{aligned}$$

Den første ligning viser at  $x = 3 + q \cdot 7$ . For at den anden ligning også er opfyldt, må  $3 + q \cdot 7 \equiv 2 \pmod{17}$ . Ved at prøve os lidt frem ses at 5 er invers til 7 modulo 17 da  $5 \cdot 7 \equiv 1 \pmod{17}$ . Dermed er  $x = 3 + (2 - 3)5 \cdot 7 = -32$  en løsning til kongruenssystemet, og vi ved fra den kinesiske restklassesætning at samtlige løsninger er  $x = -32 + k \cdot 7 \cdot 17$ ,  $k \in \mathbb{Z}$ .



Opgave 1.13.1. Bestem samtlige heltallige løsninger til kongruenssystemet

$$\begin{aligned}x &\equiv 3 \pmod{6} \\x &\equiv 6 \pmod{19}.\end{aligned}$$

**Eksempel 1.13.2.** I det foregående eksempel så vi hvordan man kan benytte den kinesiske restklassesætning til at bestemme samtlige løsninger til et kongruenssystem, men i nogle opgaver har man blot behov for at vide at der findes en løsning.

I dette eksempel vil vi vise at der findes 1000 (eller så mange det skal være) på hinanden følgende hele tal som alle er delelige med et kubiktal større end 1. Først vælger vi 1000 forskellige primtal  $p_1, p_2, \dots, p_{1000}$ . Ifølge den kinesiske restklassesætning har følgende kongruenssystem en løsning:

$$\begin{aligned}x+1 &\equiv 0 \pmod{p_1^3} \\x+2 &\equiv 0 \pmod{p_2^3} \\&\vdots \\x+1000 &\equiv 0 \pmod{p_{1000}^3}.\end{aligned}$$

Hvis  $x$  er en løsning, da er  $x+1, x+2, \dots, x+1000$  tusind på hinanden følgende hele tal som alle er delelige med et kubiktal.

Opgave 1.13.2. Vis at for alle positive heltal  $n$  findes der  $n$  på hinanden følgende hele tal, så tal nummer  $i$  er delelig med en  $i$ 'te potens af et helt tal større end 1.

Opgave 1.13.3. Vis at for alle positive heltal  $n$  og  $m$  findes  $n$  på hinanden følgende positive heltal, så hvert af disse er deleligt med mindst  $m$  forskellige primtal.

Opgave 1.13.4. Vis at der eksisterer en følge af positive heltal  $a_1, a_2, \dots$ , så summen af vilkårlige  $n$  på hinanden følgende elementer er delelig med  $n^2$ . (Baltic Way 2006).

## 1.14 Mere om divisorer

**Eksempel 1.14.1.** I dette eksempel vil vi vise at hvis  $a, b, c$  og  $d$  er positive heltal, hvor  $ab = cd$ , da er

$$a^n + b^n + c^n + d^n$$

et sammensat tal for alle positive heltal  $n$ .

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 primfaktor i  $a$  også er divisor i  $c$  eller  $d$ . Dermed findes hele tal  $r$  og  $u$  så  $a = ru$ , hvor  $r \mid c$  og  $u \mid d$ . Dette udnytter vi til at indse at der findes positive heltal  $r, s, u$  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 positive heltal  $n$ , er

$$a^n + b^n + c^n + d^n$$

et sammensat tal.

Opgave 1.14.1. Om tre positive heltal  $a, b$  og  $c$  gælder at  $a$  er ulige, og at der ikke findes et positivt heltal  $d$  større end 1 som går op i alle tre tal  $a, b$  og  $c$ . Desuden er

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

Bevis at  $abc$  er et kvadrattal. *Hint: 37*

Opgave 1.14.2. Bestem alle positive heltallige løsninger  $x, y$  og  $z$  til ligningen

$$\frac{13}{x^2} + \frac{1999}{y^2} = \frac{z}{1997}.$$

**Eksempel 1.14.2.** Når divisorerne er potenser af heltal, kan man udnytte dette. 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 når  $n > 1$ . I det hele taget kan man udnytte at fælles divisorer for  $n$  og  $n+a$  også er divisorer i  $a$ .

**Bemærkning.** Ovenstående eksempel er et specialtilfælde af den tidligere omtalte sætning af Erdős og Selfridge der siger at produktet af to eller flere på hinanden følgende positive heltal aldrig er en potens af et helt tal.

Opgave 1.14.3. Vis at ligningen

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

ikke har nogen heltallige løsninger.

Opgave 1.14.4. For hvilke positive heltal  $m$  og  $n$ , hvor  $m$  er ulige, er  $m^n + 1$  et kvadrattal?

Opgave 1.14.5. Vis at der ikke findes positive heltal  $x$ ,  $y$  og  $n$ ,  $n > 1$ , for hvilke

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

Du må ikke bruge sætningen af Erdős og Selfridge!

Opgave 1.14.6. Bestem alle positive heltal  $n$  så  $n2^{n-1} + 1$  er et kvadrattal.

Opgave 1.14.7. Bestem alle par  $x$  og  $y$  af hele tal for hvilke

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

(IMO 2006) *Hint:* 19

**Eksempel 1.14.3.** Nu skal vi se et eksempel på hvordan man kan bestemme den største fælles divisor vha. moduloregning.

Lad  $a$ ,  $m$  og  $n$  være positive heltal, hvor  $m$  er ulige og  $a > 1$ . 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  $1 \equiv -1 \pmod{d}$ , og altså  $d = 1$  eller  $d = 2$ . Det er nemt at se at  $d = 2$  når  $a$  er ulige, og  $d = 1$  når  $a$  er lige.

I dette eksempel kombinerede vi den viden vi havde om en fælles divisor  $d$ , til at bestemme  $d$  vha. moduloregning, og det kan ofte være en god strategi.

Opgave 1.14.8. Bestem samtlige positive heltal  $n, m > 2$  for hvilke  $2^n - 1$  går op i  $2^m + 1$ .

**Sætning 1.14.1.** Lad  $a$ ,  $n$  og  $m$  være positive heltal, hvor  $a > 1$ . Sæt  $d = \gcd(n, m)$ ,  $n = dn'$  og  $m = dm'$ . Da gælder

$$\gcd(a^m + 1, a^n + 1) = \begin{cases} a^d + 1 & \text{hvis både } n' \text{ og } m' \text{ er ulige,} \\ 2 & \text{hvis enten } n' \text{ eller } m' \text{ er lige, og } a \text{ er ulige,} \\ 1 & \text{hvis enten } n' \text{ eller } m' \text{ er lige, og } a \text{ er lige.} \end{cases}$$

$$\gcd(a^m - 1, a^n + 1) = \begin{cases} a^d + 1 & \text{hvis } m' \text{ er lige,} \\ 2 & \text{hvis } m' \text{ er ulige, og } a \text{ er ulige,} \\ 1 & \text{hvis } m' \text{ er ulige, og } a \text{ er lige.} \end{cases}$$



**Bevis.** I foregående eksempel har vi vist en del af sætningen, nemlig at

$$\gcd\left((a^d)^{m'} - 1, (a^d)^{n'} + 1\right) = \begin{cases} 2 & \text{hvis } m' \text{ er ulige, og } a \text{ er ulige,} \\ 1 & \text{hvis } m' \text{ er ulige, og } a \text{ er lige.} \end{cases}$$

Resten af beviset overlades til læseren i en opgave.  $\square$

For at bevise resten af sætningen er det nyttigt med følgende lemma, men det kan også gøres på måder hvor man ikke får brug for lemmaet.

**Lemma 1.14.2.** Lad  $x$  være et positivt heltal. For to positive heltal  $s$  og  $t$ , hvor  $\gcd(s, t) = 1$ , gælder at

$$\gcd\left(\sum_{i=0}^{s-1} (-1)^i x^i, \sum_{i=0}^{t-1} (-1)^i x^i\right) = 1.$$

*Opgave 1.14.9.* Vis lemma 1.14.2. *Hint:* 41

*Opgave 1.14.10.* Vis sætning 1.14.1.

*Opgave 1.14.11.* Vis at to forskellige Fermattal er indbyrdes primiske. (Husk at Fermattallene er tal på formen  $f_n = 2^{2^n} + 1$  for  $n = 0, 1, 2, \dots$ ).

*Opgave 1.14.12.* Vis at Fermattallet  $f_n$  går op i  $2^{f_n} - 2$  for alle ikke-negative heltal  $n$ .

## 1.15 Den $p$ -adiske valuation

Vi starter med de mest grundlæggende regneregler for den  $p$ -adiske valuation, hvor vi allerede tidligere har nævnt den første i sætning 1.7.3.

### Sætning 1.15.1. Regneregler for den $p$ -adiske valuation

Lad  $p$  være et primtal, og lad  $a$  og  $b$  være hele tal. Da er

1.  $v_p(ab) = v_p(a) + v_p(b)$ .
2.  $v_p(\gcd(a, b)) = \min(v_p(a), v_p(b))$ .
3.  $v_p(\text{lcm}(a, b)) = \max(v_p(a), v_p(b))$ .
4.  $v_p(a + b) \geq \min(v_p(a), v_p(b))$ .
5. Hvis  $v_p(a) \neq v_p(b)$ , da er  $v_p(a + b) = \min(v_p(a), v_p(b))$ .

*Opgave 1.15.1.* Bevis sætning 1.15.1.

*Opgave 1.15.2.* Lad  $b$  og  $n$  være positive heltal med  $n > 1$ . Antag at der for ethvert positivt heltal  $k$  findes et heltal  $a_k$  så  $k$  går op i  $b - a_k^n$ . Vis at da må  $b = A^n$  for et helt tal  $A$ . (IMO shortlist 2007)

En anden grundlæggende sætning om den  $p$ -adiske valuation er Legendres formel, der viser hvordan man beregner  $v_p(n!)$ .

### Sætning 1.15.2. Legendres formel

For et primtal  $p$  og et positivt helt tal  $n$  gælder at

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots = \frac{n - s_p(n)}{p - 1},$$

hvor  $s_p(n)$  er summen af cifrene når  $n$  skrives i  $p$ -talsystemet.

**Bevis.** Bemærk først at ifølge sætning 1.15.1, 1), er

$$v_p(n!) = v_p(1) + v_p(2) + \dots + v_p(n).$$

Vi tæller hvor mange gange  $p$  går op i  $n!$  på følgende måde: Tallet  $p$  går op i netop  $\left\lfloor \frac{n}{p} \right\rfloor$  blandt tallene  $1, 2, \dots, n$ . Tallet  $p^2$  går op i netop  $\left\lfloor \frac{n}{p^2} \right\rfloor$  blandt tallene  $1, 2, \dots, n$ , osv. Hvis der for et  $k \in \{1, 2, \dots, n\}$  gælder at  $v_p(k) = \alpha$ , da går  $p, p^2, \dots, p^\alpha$  op i  $k$ , mens  $p^{\alpha+1}, p^{\alpha+2}, \dots$  ikke går op i  $k$ . Det betyder at  $k$  bidrager med 1 til hver af  $\left\lfloor \frac{n}{p} \right\rfloor, \left\lfloor \frac{n}{p^2} \right\rfloor, \dots, \left\lfloor \frac{n}{p^\alpha} \right\rfloor$ , men ikke til nogen af  $\left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor, \left\lfloor \frac{n}{p^{\alpha+2}} \right\rfloor, \dots$ . Dermed må

$$v_p(n!) = v_p(1) + v_p(2) + \dots + v_p(n) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

som ønsket.

Betragt nu  $n$  skrevet i  $p$ -talssystemet  $n = \sum_{i=0}^k a_i p^i$ , hvor  $a_i$ 'erne er hele tal som opfylder at  $0 \leq a_i < p$  for alle  $i = 1, 2, \dots, k$ . Nu er  $s_p(n) = \sum_{i=0}^k a_i$ , og vi har

$$\begin{aligned} v_p(n!) &= \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \sum_{j=1}^k \left\lfloor \frac{a_k p^k + a_{k-1} p^{k-1} + \dots + a_0 p^0}{p^j} \right\rfloor \\ &= \sum_{j=1}^k (a_k p^{k-j} + a_{k-1} p^{k-1-j} + \dots + a_j p^{j-j}) \\ &= \sum_{i=1}^k a_i (p^{i-1} + p^{i-2} + \dots + p^0) \\ &= \sum_{i=1}^k a_i \cdot \frac{p^i - 1}{p - 1} = \sum_{i=0}^k a_i \cdot \frac{p^i - 1}{p - 1} \\ &= \frac{\sum_{i=0}^k a_i p^i - \sum_{i=0}^k a_i}{p - 1} = \frac{n - s_p(n)}{p - 1}. \quad \square \end{aligned}$$

**Opgave 1.15.3.** Bestem alle positive heltal  $n$  så  $2^{n-1}$  går op i  $n!$ .

### Sætning 1.15.3. Lifting the exponent lemma (LTE)

Lad  $p$  være et primtal, og lad  $a$  og  $b$  være to hele tal som er primiske med  $p$ .

Når  $p$  er ulige, gælder

- 1)  $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$ , hvis  $p \mid a - b$ .
- 2)  $v_p(a^n + b^n) = v_p(a + b) + v_p(n)$ , hvis  $p \mid a + b$ , og  $n$  er ulige.

Når  $p = 2$ , gælder

- 3)  $v_2(a^n - b^n) = v_2(a - b)$ , hvis  $n$  er ulige.
- 4)  $v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1$ , hvis  $n$  er lige.

**Bevis.** Vi viser 1), mens resten overlades til læseren i en opgave. Beviset føres ved induktion efter  $v_p(n)$ . Lad  $p$  være et ulige primtal, og lad  $a$  og  $b$  være to hele tal som er primiske med  $p$ , og hvor  $p$  går op i  $a - b$ .

For induktionsstarten betragter vi både tilfældet hvor  $v_p(n) = 0$ , og hvor  $v_p(n) = 1$ . Antag først at  $v_p(n) = 0$ . Ifølge sætning 1.15.1, 1), er

$$v_p(a^n - b^n) = v_p(a - b) + v_p(a^{n-1} + a^{n-2}b + \dots + b^{n-1}).$$

Da  $a \equiv b \pmod{p}$ , og  $a$  og  $b$  er primiske med  $p$ , er

$$a^{n-1} + a^{n-2}b + \dots + b^{n-1} \equiv n a^{n-1} \pmod{p},$$

og  $v_p(a^n - b^n) = v_p(a - b) = v_p(a - b) + v_p(n)$ .

Antag nu at  $v_p(n) = 1$ , og at  $n = pn'$ . Dermed er  $v_p(n') = 0$ , og det følger af det vi netop har vist, at

$$v_p(a^n - b^n) = v_p((a^p)^{n'} - (b^p)^{n'}) = v_p(a^p - b^p).$$



Sæt nu  $a = b + kp$ . Ifølge binomialformlen 1.7.4, sætning 1.15.1, 1) og 5), og fordi  $p$  går op i  $\binom{p}{i}$  for alle  $i = 1, 2, 3, \dots, p-1$ , må

$$\begin{aligned} v_p(a^p - b^p) &= v_p((b + kp)^p - b^p) \\ &= v_p\left(\binom{p}{1}b^{p-1}kp + \binom{p}{2}b^{p-2}(kp)^2 + \dots + \binom{p}{p}(kp)^p\right) \\ &= v_p\left(\binom{p}{1}b^{p-1}kp\right) = v_p(p^2 b^{p-1} k) = v_p(p^2) + v_p(b^{p-1}) + v_p(k) \\ &= 2 + v_p(k) = 2 + v_p(a - b) - 1 = v_p(a - b) + v_p(n) \end{aligned}$$

da  $k = \frac{a-b}{p}$ , og  $b$  er primisk med  $p$ . Dermed er induktionsstarten på plads.

Nu er vi nået til induktionsskridtet. Antag at 1) er sand for alle  $n$ , hvor  $v_p(n) = N$  for et givet positivt heltal  $N$ . Se nu på et  $n$  med  $v_p(n) = N + 1$ , og sæt  $n = p^{N+1}n'$ . Da er

$$\begin{aligned} v_p(a - b) &= v_p\left(\left(a^{p^N}\right)^{pn'} - \left(b^{p^N}\right)^{pn'}\right) \\ &= v_p\left(a^{p^N} - b^{p^N}\right) + 1 = v_p(a - b) + N + 1 = v_p(a - b) + v_p(n). \end{aligned}$$

Hermed er induktionen fuldført.  $\square$

*Opgave 1.15.4.* Bevis resten af LTE (sætning 1.15.3).

*Opgave 1.15.5.* Bestem alle positive hele tal  $n$  så der for ethvert ulige tal  $a$  gælder at  $2^{2017}$  går op i  $a^n - 1$ . (China Girls Math Olympiad 2017)

*Opgave 1.15.6.* Lad  $p > 2025$  være et primtal. Lad desuden  $a$  og  $b$  være to positive heltal hvor  $v_p(a + b) = 1$  og  $v_p(a^{2025} + b^{2025}) > 1$ . Vis at  $v_p(a^{2025} + b^{2025}) \geq 2025$ .

*Opgave 1.15.7.* Bestem det mindste positive hele tal  $n$  så  $2^{1000}$  går op i  $2025^n - 1$ . *Hint:* 18

*Opgave 1.15.8.* Bestem alle positive hele tal  $n$  så  $n^2$  går op  $2^n + 1$ . (IMO 1990) *Hint:* 10

*Opgave 1.15.9.* Findes der et positivt helt tal  $n$  så  $n$  har præcis 2000 forskellige primdivisorer, og så  $n$  går op i  $2^n + 1$ ? (IMO 2000) *Hint:* 25

## 1.16 Summer af to kvadrattal

Primtal på formen  $p = 4m + 1$  og primtal på formen  $p = 4m + 3$  har forskellige egenskaber. Fx har vi tidligere vist at  $-1$  er kvadratisk rest modulo et ulige primtal  $p$  netop når  $p$  er på formen  $p = 4m + 1$ .

I dette kapitel vil vi vise at et ulige primtal  $p$  kan skrives som en sum af to kvadrattal netop når  $p$  er på formen  $p = 4m + 1$ . Og endnu mere generelt: Et positivt heltal  $n$  kan skrives som sum af to kvadrattal netop når alle primfaktorer i  $n$  på formen  $4m + 3$  indgår i en lige potens i primfaktoropløsningen af  $n$ . Inden vi er klar til det, har vi brug for nogle hjælpesætninger.

**Sætning 1.16.1.** 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

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

Altså er

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

hvilket er en modstrid da  $-1$  ikke er kvadratisk rest modulo  $p$  ifølge sætning 1.10.4. Derfor må  $p$  gå op i  $a$  og dermed også i  $b$ .  $\square$

**Korollar 1.16.2.** Primtal  $p$  på formen  $p = 4m + 3$  kan ikke skrives som sum af to kvadrattal.

**Bevis.** Det følger umiddelbart af sætning 1.16.1.  $\square$

Primtal på formen  $p = 4m + 1$  kan derimod altid skrives som sum af to kvadrattal, og det skal vi se nærmere på om lidt.

### Definition af kvadrattal

Et positivt helt tal kaldes *kvadrattal* hvis alle primtal i primfaktoropløsningen af tallet kun indgår i 1. potens.

*Opgave 1.16.1.* Om et helt tal  $n$  oplyses at  $n$  er kvadrattal, og at samtlige primfaktorer i  $n$  er på formen  $4m + 3$ . Vis at  $n$  ikke kan skrives som sum af to kvadrattal.

*Opgave 1.16.2.* Vis at  $n^2 + 3$  ikke er et kubiktal for noget positivt heltal  $n$ . *Hint:* 45

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

### Sætning 1.16.3. Thues sætning

Lad  $n$  være et helt tal større end 1, og lad  $k$  være det hele tal som opfylder at  $k - 1 \leq \sqrt{n} < k$ . Antag at  $a \in \mathbb{Z}$  er primisk med  $n$ . Da findes  $x, y \in \{1, 2, \dots, k - 1\}$ , så

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

**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 skuffeprikket mindst to par så  $ay' + x'$  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  $\gcd(a, n) = 1$ , 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  $x_1 = x_2$ , hvilket er en modstrid.

Dermed er

$$0 < |x_1 - x_2| \leq k - 1 \quad \text{og} \quad 0 < |y_1 - y_2| \leq k - 1.$$

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

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

**Sætning 1.16.4.** Et ulige primtal  $p$  kan skrives som sum af to kvadrater netop når  $p$  er på formen  $p = 4m + 1$ .

*Opgave 1.16.3.* Bevis sætning 1.16.4. *Hint:* 29

### Sætning 1.16.5. Sum af to kvadrattal

Et positivt heltal  $n$  kan skrives som sum af to kvadrattal, netop når alle primfaktorer i  $n$  på formen  $4m + 3$  indgår i en lige potens i primfaktoropløsningen af  $n$ .

*Opgave 1.16.4.* Bevis sætningen.



## 1.17 Primtallenes forunderlige verden

Vi har allerede set at der er uendelig mange primtal, og dette resultat har været kendt i hvert fald siden Euklid skrev sine elementer ca. 300 f.v.t. Primtallene er fascinerende og uforudsigelige, og der er stadig mange formodninger om primtal som venter på at blive bevist.

Her skal vi se på både formodninger og resultater om primtal som det ligger uden for disse noters rækkevidde at komme med et bevis for.

### Formodning 1.17.1. Tvillingepriamtal

Tvillingepriamtal er to på hinanden følgende ulige tal som begge er primtal, fx er 5 og 7, 11 og 13 samt 17 og 19 tvillingepriamtal. Det formodes at der findes uendeligt mange tvillingepriamtal, men det er endnu ikke lykkes nogen at bevise det. Det er stadig et af de helt store uløste spørgsmål i talteori.

*Opgave 1.17.1.* Trillingepriamtal er tre på hinanden følgende ulige tal som alle er primtal. Hvor mange primtalstrillinger findes der?

### Formodning 1.17.2. Goldbachs formodning

Goldbachs formodning fra 1742 siger at alle positive lige tal større end 2 kan skrives som en sum af to primtal. Fx  $4 = 2 + 2$ ,  $6 = 3 + 3$ ,  $8 = 3 + 5$ , osv.

Det er indtil videre vist at dette er sandt for alle lige tal mindre end  $4 \cdot 10^{18}$ , men at vise det generelt er stadig et stort uløst problem, som mange i tidens løb uden held har kæmpet med.

Der er ikke noget (kendt) system i den måde primtallene fordeler sig på, og det er nok en del af årsagen til at primtallene er så fascinerende. Man ved alligevel ca. hvor mange primtal der er op til et helt tal  $n$  for meget store værdier af  $n$ .

### Sætning 1.17.1. Primalssætningen

Lad  $\pi(n)$  betegne antallet af primtal mindre end  $n$ . Da er

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1,$$

Der findes også endnu bedre tilnærmelser til  $\pi(n)$  end  $\frac{n}{\ln n}$ .

### Sætning 1.17.2. Bertrands postulat

Bertrands postulat siger at for et positivt heltal  $n$ ,  $n > 3$ , findes mindst ét primtal  $p$  så

$$n < p < 2n - 2.$$

Bertrand kom med dette postulat i 1845, og påstanden blev allerede vist af Chebyshev i 1850, men navnet Bertrands *postulat* har alligevel hængt ved.

*Opgave 1.17.2.* Vis at  $\binom{2n}{n}$  ikke er et kvadrattal for noget positivt heltal  $n$ .

*Opgave 1.17.3.* Lad  $n$  være et positivt heltal. Vis at de  $2n$  tal  $1, 2, 3, \dots, 2n$  kan parres til  $n$  par så summen af hvert par er et primtal. *Hint:* 16

### Sætning 1.17.3. Dirichlets sætning

Lad  $a$  og  $b$  være to indbyrdes primiske positive heltal. Da indeholder den aritmetiske progression

$$b, a + b, 2a + b, 3a + b, 4a + b, \dots$$

uendeligt mange primtal. Eller sagt med andre ord: Der er uendeligt mange primtal på formen  $an + b$ .

Denne sætning blev først vist af Dirichlet i 1837.

Der findes ikke noget elementært bevis for sætningen, men man kan vise specialtilfælde af den som fx at der findes uendeligt mange primtal på formen  $3n + 2$ ,  $4n + 1$ ,  $4n + 3$  og  $6n + 5$ .

**Eksempel 1.17.1.** For at vise at der findes uendelig mange primtal på formen  $3n + 2$ , antager vi, som i Euklids bevis for at der findes uendeligt mange primtal, at der kun findes endeligt mange. Kald disse  $p_1, p_2, \dots, p_r$ , og betragt tallet

$$N = 3p_1 p_2 p_3 \cdots p_r + 2$$

Da  $N \equiv 2 \pmod{3}$ , kan  $N$  ikke kun have primfaktorer på formen  $3n + 1$ , og  $N$  har derfor en primfaktor på formen  $q = 3n + 2$ , men dette er en modstrid da ingen af primtallene  $p_1, p_2, \dots, p_r$  går op i  $N$ .

Hvis man skal vise at der er uendeligt mange primtal på formen  $4n + 1$ , kræver det en smule mere snilde og teori. Her er det ikke nok at betragte primfaktorer i  $4p_1 p_2 \cdots p_r + 1$ , da produktet af primtal på formen  $4n + 3$  godt kan have rest 1 modulo 4, og vi får derfor brug for teori om forskellige egenskaber ved primtal på formen  $4n + 1$  og på formen  $4n + 3$ . Fx ved vi at  $-1$  kun er kvadratisk rest modulo ulige primtal på formen  $4n + 1$ . Dette kan udnyttes på følgende måde: Antag igen at der kun findes endeligt mange primtal på formen  $4n + 1$ , og lad disse være  $p_1, p_2, p_3, \dots, p_r$ . Betragt tallet

$$N = (2p_1 p_2 \cdots p_r)^2 + 1.$$

Læg mærke til at vi på denne måde har konstrueret et tal  $N$  så  $-1$  er kvadratisk rest modulo alle divisorer  $q$  i  $N$  da

$$(2p_1 p_2 \cdots p_r)^2 \equiv -1 \pmod{q}.$$

En primfaktor  $q$  i  $N$  er derfor på formen  $4n + 1$ , men dette er en modstrid da ingen af primtallene  $p_1, p_2, \dots, p_r$  går op i  $N$ . Dermed findes der uendeligt mange primtal på formen  $4n + 1$ .

*Opgave 1.17.4.* Vis at der findes uendeligt mange primtal på formen  $4n + 3$ , på formen  $6n + 5$  og på formen  $2^k n + 1$ , hvor  $k$  er et positivt heltal. Du må selvfølgelig ikke benytte Dirichlets sætning. *Hint:* 30, 23, 17

## 1.18 Den kvadratiske reciprocitetssætning

Den kvadratiske reciprocitetssætning viser en meget smuk sammenhæng mellem kvadratiske rester, og den er et godt værktøj til at tjekke om et tal er kvadratisk rest modulo et andet tal. Men før vi når til den, skal vi se på Legendresymbolet og Eulers kriterium.

### Definition af Legendresymbolet

Lad  $p$  være et ulige primtal, og lad  $a \in \mathbb{Z}$  være primisk med  $p$ . Legendresymbolet

$$\left(\frac{a}{p}\right)$$

er da 1 hvis  $a$  er kvadratisk rest modulo  $p$ , og  $-1$  hvis  $a$  ikke er.

*Opgave 1.18.1.* Lad  $p$  være et ulige primtal. Vis at

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0.$$

### Sætning 1.18.1. Eulers kriterium

Lad  $p$  være et ulige primtal, og lad  $a \in \mathbb{Z}$  være primisk med  $p$ . Da er

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

**Bevis.** Hvis  $a$  er kvadratisk rest modulo  $p$ , har kongruensligningen  $x^2 \equiv a \pmod{p}$  en løsning  $x$ . Altså er

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$$

ifølge Fermats lille sætning.

Hvis  $a$  ikke er kvadratisk rest modulo  $p$ , da ved vi ifølge sætning 1.8.4 at for hver primisk rest  $x \in \{1, 2, \dots, p-1\}$  findes en unik primisk rest  $y = x^{-1}a$  så  $xy \equiv a \pmod{p}$ , hvor  $x \neq y$ . Dermed kan alle resterne  $1, 2, \dots, p-1$  parres to



og to så produktet af hvert par er  $a$ . Altså er

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}$$

ifølge Wilsons sætning.  $\square$

**Korollar 1.18.2.** Lad  $p$  være et ulige primtal, og lad  $a, b \in \mathbb{Z}$  være primiske med  $p$ . Da er

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

**Bevis.** Korollaret følger umiddelbart af Eulers kriterium.  $\square$

**Korollar 1.18.3.** Lad  $p$  være et ulige primtal. Da er

$$1) \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{hvis } p \equiv 1 \pmod{4} \\ -1 & \text{hvis } p \equiv -1 \pmod{4} \end{cases}$$

$$2) \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{hvis } p \equiv 1 \text{ eller } p \equiv 7 \pmod{8} \\ -1 & \text{hvis } p \equiv 3 \text{ eller } p \equiv 5 \pmod{8} \end{cases}$$

Del 1) er allerede vist tidligere, men tages alligevel med her.

**Bevis.** Del 1) følger umiddelbart af Eulers kriterium, men vi har også bevist det tidligere i sætning 1.10.4.

I del 2) viser vi kun tilfældet hvor  $p \equiv 1 \pmod{4}$ , og overlader tilfældet  $p \equiv 3 \pmod{4}$  til læseren i en opgave. Hvis  $p \equiv 1 \pmod{4}$  er

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdots \left(2 \cdot \frac{p-1}{2}\right) \equiv 2 \cdot 4 \cdot 6 \cdots (p-1)$$

$$\equiv 2 \cdot 4 \cdot 6 \cdots \left(\frac{p-1}{2}\right) \cdot \left(-\frac{p-3}{2}\right) \cdots (-5) \cdot (-3) \cdot (-1)$$

$$\equiv (-1)^{\frac{p-1}{4}} \left(\frac{p-1}{2}\right)! \pmod{p}$$

Ifølge Eulers kriterium gælder nu at

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod{p}.$$

Dermed er  $\left(\frac{2}{p}\right) = 1$  når  $p \equiv 1 \pmod{8}$ , og  $\left(\frac{2}{p}\right) = -1$  når  $p \equiv 5 \pmod{8}$ .  $\square$

*Opgave 1.18.2.* Vis korollar 1.18.3, 2), for  $p \equiv 3 \pmod{4}$ .

**Sætning 1.18.4.** Lad  $a$  være et helt tal og  $b$  et positivt helt tal større end 1 med primfaktoropløsning

$$b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}.$$

Da er  $a$  kvadratisk rest modulo  $b$  hvis og kun hvis  $a$  er kvadratisk rest modulo  $p_i^{\alpha_i}$  for alle  $i = 1, 2, \dots, n$ .

*Opgave 1.18.3.* Bevis sætning 1.18.4.

*Opgave 1.18.4.* Lad  $n$  være et ulige positivt heltal og  $p$  en primdivisor i  $2^n - 1$ . Vis at  $p \equiv \pm 1 \pmod{8}$ .

*Opgave 1.18.5.* Lad  $x$  og  $y$  være indbyrdes primiske hele tal. Vis at hvis  $p$  er en ulige primdivisor i  $x^2 + 2y^2$ , da er  $p \equiv 1$  eller  $p \equiv 3 \pmod{8}$ . *Hint:* 26

**Definition af Sophie Germain-primtal**

Et *Sophie Germain-primtal* er et primtal  $p$  så  $2p + 1$  også er et primtal. Disse primtal er bl.a. interessante da  $\phi(2p + 1)$  er det dobbelte af primtallet  $p$  og  $\phi(2p + 1)$  derfor kun har to ikke-trivielle positive divisorer.

*Opgave 1.18.6.* Vis at hvis  $p$  er et primtal, og  $p \equiv 3 \pmod{4}$ , da er  $2p + 1$  divisor i Mersennetallet  $M_p = 2^p - 1$  netop hvis  $p$  er et Sophie Germain-primtal. *Hint:*

**Bemærkning.** Kriteriet i opgave 1.18.6 viser fx at Mersennetallet  $M_{11} = 2^{11} - 1$  ikke er et primtal da 11 er et Sophie Germain-primtal fordi  $2 \cdot 11 + 1 = 23$  også er et primtal, og 23 dermed er divisor i  $M_{11} = 2047$ .

Opgave 1.18.7. Find mindst ét primtal  $p > 11$  for hvilket  $M_p = 2^p - 1$  ikke er et primtal.

Opgave 1.18.8. Vis at ligningen  $16 = x^8 \pmod{p}$  har en heltallig løsning for alle ulige primtal  $p$ .

Opgave 1.18.9. Fermattallene er som tidligere nævnt  $f_n = 2^{2^n} + 1$ , for  $n = 1, 2, 3, \dots$ . Vis at hvis  $p$  er en primdivisor i  $f_n$ ,  $n > 2$ , da er  $p \equiv 1 \pmod{2^{n+2}}$ .

Hint: 38

**Bemærkning.** Det var vha. kriteriet i opgave 1.18.9 at Euler gættede at  $641 = 5 \cdot 2^{5+2} + 1$  var primfaktor i  $f_5 = 2^{2^5} + 1$ .

**Sætning 1.18.5.** Lad  $x$  og  $y$  være to indbyrdes primiske heltal og  $a, b, c$  hele tal. Hvis  $p$  er en primdivisor i  $ax^2 + bxy + cy^2$  som ikke går op i  $abc$ , da er

$$D = b^2 - 4ac$$

kvadratisk rest modulo  $p$ .

Opgave 1.18.10. Bevis sætning 1.18.5.

**Sætning 1.18.6. Den kvadratiske reciprocitetssætning**

Lad  $p$  og  $q$  være to forskellige ulige primtal. Da er

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

**Bemærkning.** Euler formulerede den kvadratiske reciprocitetssætning i 1783, men uden bevis. Det blev Gauss der i 1801 fik udgivet det første korrekte bevis for sætningen efter fejlslagne forsøg fra bl.a. Legendre. Den kvadratiske reciprocitetssætning kaldes af mange *Aritmetikkens perle*, og det var Gauss' favoritsætning inden for talteori. Der findes nu mange helt forskellige beviser for sætningen, men de er alle for omfangsrige til disse noter.

Opgave 1.18.11. Undersøg om 37 og 143 er kvadratiske rester modulo 2003. (2003 er et primtal).

Opgave 1.18.12. Lad  $p$  være et ulige primtal. Vis at

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{hvis } p \equiv \pm 1 \pmod{12} \\ -1 & \text{hvis } p \equiv \pm 5 \pmod{12} \end{cases}$$

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{hvis } p \equiv \pm 1 \pmod{5} \\ -1 & \text{hvis } p \equiv \pm 2 \pmod{5} \end{cases}$$

Opgave 1.18.13. Bestem samtlige par af hele tal  $(x, y)$  som opfylder ligningen  $162x^2 = 7 + 151y^2$ .

Opgave 1.18.14. Lad  $a, b$  og  $c$  være positive heltal som er parvis indbyrdes primiske. Vis at hvis  $a^2 - ab + b^2 = c^2$ , da er enhver primdivisor i  $c$  på formen  $6k + 1$ .

Opgave 1.18.15. Vis at hvis  $p = 2^n + 1$ ,  $n > 1$ , er et primtal, da går  $p$  op i  $3^{\frac{p-1}{2}} + 1$ .

Opgave 1.18.16. Bestem alle positive heltal  $k$  for hvilke der findes et heltal  $a$  så  $2007$  går op i  $(a+k)^3 - a^3$ .

Opgave 1.18.17. Vis at hvis et positivt heltal  $a$  er kvadratisk rest modulo alle primtal, da er  $a$  et kvadrattal.

Opgave 1.18.18. Lad  $n$  være et positivt heltal større end 2. Vis at Fermattallet  $f_n$  har en primfaktor større end  $2^{n+4}(n+2)$ . Hint: 31



## 2 Hints

1. Betragt  $\text{ord}_q(2)$ .
2. Lad  $m$  være det største hele tal så  $2^m$  går op i alle elementer i følgen, og betragt følgen  $b_n = \frac{a_n}{2^m}$ .
3. Udnyt at  $ab = a(2002 - a)$ .
4. Kubiske rester modulo 7.
5. Vis at  $v_5(2^m + 3^m) = 1$ .
6. Husk sætning 1.7.2.
7. Faktoriser  $10^{2^n} - 1$ .
8. Omskriv først til  $n^4 + 4 = (n^2 + 2)^2 - (2n)^2$ .
9. Antag at det er sandt, og vis at det fører til en modstrid. Brug kvadratiske rester.
10. For  $n > 1$  betragt den mindste primdivisor  $p$  i  $n$ .
11. Regn på  $\text{gcd}(a_n, a_{n+1})$ , og udnyt undervejs at hvis  $s, t \in \mathbb{Z}$  og  $t$  er ulige, da er  $\text{gcd}(s, t) = \text{gcd}(2s, t)$ .
12. Vis først at hvis  $c = ax + by$ ,  $x, y \in \mathbb{Z}$ , da må  $\text{gcd}(a, b)$  gå op i  $c$ . Vis efterfølgende at hvis  $c$  er et multiplum af  $\text{gcd}(a, b)$ , da findes ifølge Bezouts identitet  $x, y \in \mathbb{Z}$  så  $c = ax + by$ .
13. Betragt  $\text{ord}_p(q)$ .
14. Udnyt at  $3n + 2$  og  $3$  er indbyrdes primiske.
15. Lad  $q$  være den mindste primfaktor i  $x$ , og se på  $\text{ord}_q(p - 1)$ .
16. Benyt induktion efter  $n$ .
17. Indirekte: Betragt  $(2p_1 p_2 p_3 \cdots p_r)^{2^{k-1}} + 1$  hvor  $p_1, p_2, \dots$  er samtlige primtal på formen  $2^k n + 1$ .
18. Vis først at  $n$  er en potens af 2.
19. Omskriv ligningen til  $2^x + 2^{2x+1} = (y - 1)(y + 1)$ .
20. Hvorfor er  $\text{gcd}(m^4, m - 1) = 1$ ?
21. Betragt i stedet følgen  $y_n = x_n - 1$ .
22. Antag at  $p$  er et primtal, og vis at da går  $p$  op i  $q$ .
23. Indirekte: Betragt  $6p_2 p_3 p_4 \cdots p_r + 5$  hvor  $p_1, p_2, \dots$  er samtlige primtal på formen  $6n + 5$  og  $p_1 = 5$ .
24. Vis at hvis  $x, y \in \{1, 2, \dots, p - 1\}$  er to forskellige rester modulo  $p$  som opfylder at  $x^2 \equiv y^2 \pmod{p}$ , da er  $x + y = p$ .
25. Vis ved induktion efter  $N$ : For ethvert positivt heltal  $N$  findes et positivt ulige tal  $n$  med præcis  $N$  forskellige primdivisorer som opfylder at  $n$  går op i  $2^n + 1$ .
26. Udnyt at  $y$  har en multiplikativ invers  $y^{-1}$  modulo  $p$ .
27. Vis at hvis  $a + b$  er delelig med  $n$ , da er  $a^n + b^n$  delelig med  $n^2$ .
28. Vis først at  $(a - b)^2$  er delelig med 11.
29. 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 kvadrattal.
30. Indirekte: Betragt  $4p_2 p_3 p_4 \cdots p_r + 3$  hvor  $p_1, p_2, \dots$  er samtlige primtal på formen  $4n + 3$  og  $p_1 = 3$ .
31. Udnyt opgave 1.18.9.
32. Betragt  $\text{ord}_{f_n}(3)$ .
33. I alle tre delopgaver er det smart at regne modulo 4.
34. Vis at  $2^n$  går op i både  $x$ ,  $y$  og  $z$  for alle positive heltal  $n$ .
35. Den store udfordring er at bestemme  $2002^{2001} \pmod{400}$ . For at bestemme denne rest er det smart at regne modulo  $2^4$  og modulo  $5^2$ , og derefter kombinere resultaterne.
36. Betragt  $\text{ord}_{2p+1}(2)$ .
37. Vis at der findes positive hele tal  $u, v$  og  $w$  så  $au = bc$ ,  $bv = ac$ ,  $cw = ab$  hvor  $u, v$  og  $w$  er parvis indbyrdes primiske.
38. Betragt  $\text{ord}_p(2)$ .
39. Udnyt Wilsons sætning til at finde et  $x$  der opfylder at  $x^2 \equiv -1 \pmod{p}$ .
40. Regn modulo 11.
41. Antag modsat at det ikke er sandt, og lad  $s'$  og  $t'$  være to positive heltal med den mindste sum for hvilke det ikke er sandt.
42. Lad  $p$  være en ulige primfaktor i  $a^{2^n} + 1$ , og betragt  $\text{ord}_p(a)$ .
43. Inddel i  $n$  lige og  $n$  ulige, og se på kvadratiske rester modulo 4.
44. Se på  $(b^2 + a)^b - a^b$  modulo  $b^4$ .
45.  $m^3 + 1 = (m + 1)(m^2 - m + 1)$ .
46. Se på sidste ciffer i  $k$ .
47. Brug Bezouts identitet.

### 3 Løsninger

**Opgave 1.1.1.** Samtlige divisorer i 60 er 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60. Samtlige divisorer i 98 er 1, 2, 7, 14, 49, 98.

**Opgave 1.1.2.** 2) At  $a \mid b$ , betyder at der findes et helt tal  $q$  så  $b = a \cdot q$ . Dermed er  $b \cdot c = a \cdot q \cdot c = a \cdot (q \cdot c)$ , og det viser at  $a \mid b \cdot c$ .

3) At  $a \mid b$  og  $a \mid c$ , betyder at der findes hele tal  $q_1$  og  $q_2$  så  $b = a \cdot q_1$  og  $c = a \cdot q_2$ . Dermed er  $b + c = a(q_1 + q_2)$  og  $b - c = a(q_1 - q_2)$ , og det viser at  $a \mid b + c$  og  $a \mid b - c$ .

**Opgave 1.1.3.** Antag at  $n$  og  $m$  er hele tal så  $2 \mid n$  og  $6 \mid m$ . Da er  $n = 2n'$  og  $m = 6m'$ , og dette viser at  $m(m + n) = 6m'(6m' + 2n') = 4(9m'^2 + 3n')$  altid er delelig med 4. Ingen af de andre tal er altid delelig med 4: a)  $n + m$  er ikke altid delelig med 4, fx ikke for  $n = 2$  og  $m = 12$ . b)  $nm - m$ , c)  $m^2 + n$  og e)  $n(m + 1)$  er ikke altid delelig med 4, fx ikke for  $n = 2$  og  $m = 6$ .

**Opgave 1.1.4.** Antag at  $m$  og  $n$  er hele tal som opfylder at  $n + m = n^2$ . Da er  $m = n(n - 1)$ , hvilket viser at  $n \mid m$ . Man kan til gengæld ikke slutte at b)  $m \mid n$ , c)  $n$  og  $m$  er ulige, eller d)  $n$  og  $m$  er lige, da fx  $n = 3$  og  $m = 6$  ikke opfylder hverken b), c) eller d).

**Opgave 1.1.5.** ..., 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

**Opgave 1.1.6.**  $1001 = 7 \cdot 11 \cdot 13$ .  $11400 = 2^3 \cdot 3 \cdot 5^2 \cdot 19$ . Tallet  $1024 = 2^{10}$  har kun en enkelt primfaktor, nemlig 2. Primfaktorerne i 1001 er 7, 11 og 13.

**Opgave 1.1.7.** Da primfaktoropløsningen af 2008 er  $2008 = 2^3 \cdot 251$ , er eneste mulighed for de fire tal 1, 2,  $2^2$ , 251. Dermed er deres sum 258.

**Opgave 1.1.8.** I primfaktoropløsningen af  $20!$  er potensen af 5 netop  $5^4$  mens potensen af 2 er større end  $2^4$ . Derfor ender  $20!$  på netop fire nuller.

**Opgave 1.1.9.** Tallet 4004 går ikke op i  $238 \cdot 65 \cdot 1221$  da 4 går op i 4004, men ikke i  $238 \cdot 65 \cdot 1221$ .

**Opgave 1.1.10.** Lad  $m$  være et positivt heltal større end 1 med primfaktoropløsning  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ , hvor  $p_i$ 'erne er forskellige primtal. Da er primfaktoropløsningen af  $m^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r}$ . Dette viser at alle primfaktorer

i et kvadrattal indgår i en lige potens i primfaktoropløsningen. Antag omvendt at  $n$  er et positivt heltal, hvor alle primfaktorer i  $n$  indgår i en lige potens i primfaktoropløsningen. Da er  $n = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r}$ , dvs.  $n = m^2$ , hvor  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ , og det viser at  $n$  er et kvadrattal.

**Opgave 1.1.11.** Lad  $n$  være det mindste positive heltal så  $\sqrt{n \cdot 261}$  er et helt tal. Da må  $n \cdot 261 = n \cdot 29 \cdot 3^2$  være et kvadrattal, og altså må 29 være en primfaktor i  $n$  da 29 skal indgå i en lige potens i primfaktoropløsningen af  $n \cdot 29 \cdot 3^2$ . For  $n = 29$  er  $\sqrt{n \cdot 261} = 3 \cdot 29$ , dvs.  $n = 29$  er det mindste positive heltal så  $\sqrt{n \cdot 261}$  er et helt tal.

**Opgave 1.1.12.** Antag at  $p$  er et primtal, og at  $p \mid ab$ . Hvis et af tallene  $a$  og  $b$  er  $\pm 1$  eller 0, er udsagnet oplagt. Antag derfor at  $|a|, |b| > 1$ . Antag desuden i første omgang at  $a$  og  $b$  er positive. Primfaktoropløsningen af  $ab$  er netop primfaktoropløsningen af  $a$  gange primfaktoropløsningen af  $b$  da primfaktoropløsningen er entydig. Da  $p$  indgår i primfaktoropløsningen af  $ab$ , må  $p$  derfor også indgå i primfaktoropløsningen af  $a$  eller primfaktoropløsningen af  $b$ . Dermed må  $p \mid a$  eller  $p \mid b$ . Beviset kører på helt samme måde hvis et eller begge af tallene  $a$  og  $b$  er negative.

Udsagnet gælder ikke altid hvis  $p$  ikke er et primtal. Fx går 6 op i  $4 \cdot 9$ , men hverken i 4 eller 9.

**Opgave 1.1.13.** Kun  $10982 \cdot 505$  er delelig med 10 da det er det eneste af tallene der indeholder  $2 \cdot 5$  i sin primfaktoropløsning. Kun  $5025 \cdot 2092$  er delelig med 100 da det er det eneste af tallene der indeholder  $2^2 \cdot 5^2$  i sin primfaktoropløsning.

**Opgave 1.1.14.** Blandt tre på hinanden følgende heltal findes altid mindst et som er deleligt med 2, og et som er deleligt med 3. Dermed er produktet af dem deleligt med  $2 \cdot 3 = 6$ . Blandt fem på hinanden følgende heltal er der altid mindst et der er deleligt med 3, mindst et der er deleligt med  $4 = 2^2$ , og et der er deleligt med 5. Dermed er produktet af dem deleligt med  $3 \cdot 2^2 \cdot 5 = 60$ .

**Opgave 1.1.15.** Da  $a + b = 2002$ , er  $b = 2002 - a$ . Derfor er  $ab = a(2002 - a) = 2002a - a^2$ . Hvis 2002 skal gå op i  $ab$ , skal 2002 derfor også gå op i  $a^2$ . Vi betragter nu primfaktoropløsningen af 2002, som er  $2002 = 2 \cdot 7 \cdot 11 \cdot 13$ . Dermed skal hver af primfaktorerne 2, 7, 11 og 13 gå op i  $a^2$ , og derfor også i  $a$  ifølge sætning 1.1.5. Men hvis 2, 7, 11 og 13 går op i  $a$ , så må  $2 \cdot 7 \cdot 11 \cdot 13 = 2002$  også



gå op i  $a$  ifølge korollar 1.1.4. Men det er umuligt da  $0 < a < 2002$  fordi  $a$  og  $b$  er positive heltal så  $a + b = 2002$ . Altså kan 2002 aldrig gå op i  $ab$ .

**Opgave 1.2.1.** Ved at omskrive fås

$$53 = x^6 - y^2 = (x^3 + y)(x^3 - y).$$

Da 53 er et primtal, må  $x^3 + y = 53$  og  $x^3 - y = 1$ . Dermed er  $x = 3$  og  $y = 26$  eneste løsning.

**Opgave 1.2.2.** Tallet  $m^3 - m$  er deleligt med 6 for alle hele tal  $m$  da

$$m^3 - m = m(m^2 - 1) = m(m - 1)(m + 1)$$

viser at  $m^3 - m$  er et produkt af tre på hinanden følgende hele tal, og 2 og 3 hver især går op i mindst et af de tre tal.

**Opgave 1.2.3.** Kald den ukendte katete  $a$  og hypotenusen  $c$ . Da er

$$2^2 \cdot 997^2 = 1994^2 = c^2 - a^2 = (c + a)(c - a).$$

Da  $c + a$  og  $c - a$  har samme paritet (dvs. de enten begge er lige eller ulige), må de begge være lige. Vi har derfor

$$997^2 = \frac{c + a}{2} \cdot \frac{c - a}{2},$$

hvor 997 er et primtal. Heraf ses at  $\frac{c+a}{2} = 997^2$  og  $\frac{c-a}{2} = 1$ . Dette giver  $c = 1 + 997^2 = 994010$ .

**Opgave 1.2.4.** Omskriv sammenhængen mellem  $p$ ,  $q$  og  $r$  til

$$p = r^2 - q^2 = (r + q)(r - q).$$

For at vise at 6 går op i  $pqr$ , viser vi at 2 og 3 hver især går op i mindst et af tallene  $p$ ,  $q$  og  $r$ , og dermed i deres produkt. Hvis hverken  $q$  eller  $r$  er lige, er de begge ulige, og så er  $r + q$  lige, og altså  $p = (r + q)(r - q)$  lige. Altså er mindst et af tallene  $p$ ,  $q$  og  $r$  deleligt med 2. Hvis hverken  $q$  eller  $r$  er deleligt med 3, da har de hver især rest 1 eller 2 ved division med 3. Hvis de har forskellig rest, er  $r + q$  deleligt med 3, og hvis de har samme rest, er  $r - q$  deleligt med 3. I begge

tilfælde er  $p$  deleligt med 3. Dermed er mindst et af tallene  $p$ ,  $q$  og  $r$  deleligt med 3. Samlet giver dette at deres produkt  $pqr$  er deleligt med 6.

**Opgave 1.2.5.** Da

$$a^2 + b^2 + 9ab = (a - b)^2 + 11ab,$$

er  $(a - b)^2$  deleligt med 11, og da 11 er et primtal, må  $a - b$  også være deleligt med 11. Altså er  $a^2 - b^2 = (a + b)(a - b)$  deleligt med 11.

**Opgave 1.2.6.** Lad  $n = a^2 + b^2$  og  $m = c^2 + d^2$ . Vi skal nu vise at produktet  $nm$  også er en sum af to kvadrattal, og det gør vi ved at omskrive vha. af kvadrat-sætninger.

$$\begin{aligned} nm &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (ac + bd)^2 - 2abcd + (ad - bc)^2 + 2abcd \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

**Opgave 1.2.7.** For alle  $n > 1$  viser omskrivningen

$$n^4 + 4 = (n^2 + 2)^2 - (2n)^2 = (n^2 + 2n + 2)(n^2 - 2n + 2).$$

at  $n^4 + 4$  ikke er et primtal. For  $n = 1$  er  $n^4 + 4 = 5$  et primtal.

**Opgave 1.2.8.** Først omskriver vi således:

$$\begin{aligned} 2x^2y^2 + 16x^2 + y^2 &= 448 \\ 2x^2(y^2 + 8) + y^2 + 8 &= 456 \\ (2x^2 + 1)(y^2 + 8) &= 2^3 \cdot 3 \cdot 19. \end{aligned}$$

Da  $2x^2 + 1$  er ulige, må  $2x^2 + 1$  være lig med 1, 3, 19 eller 57. Af dette ser man at  $x = 0, 1, 3$ . Ved at efterprøve disse muligheder får man følgende løsninger (1, 12) og (3, 4).

**Opgave 1.2.9.** Da  $xy + 3y = y(x + 3)$  og  $x^2 + 2x = (x + 3)(x - 1) + 3$ , kan ligningen omskrives til

$$1994 = (x + 3)(x - 1) - y(x + 3) = (x + 3)(x - 1 - y).$$

De eneste faktoriseringer af tallet 1994 er  $1994 \cdot 1$  og  $997 \cdot 2$ , og da  $x + 3$  er den største af faktorerne, får vi derfor løsninger  $(x, y) = (1991, 1989)$  og  $(x, y) = (994, 991)$ .

**Opgave 1.3.1.** Det følger af korollar 1.1.4 at enhver positiv divisor i  $n$  er på formen

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

hvor  $\beta_i$  er et af tallene  $0, 1, \dots, \alpha_i$ . Dermed har  $n$  i alt  $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_m)$  forskellige positive divisorer ifølge multiplikationsprincippet.

**Opgave 1.3.2.** Antag at  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  har et ulige antal positive divisorer, og altså at  $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_m)$  er ulige. Da er  $1 + \alpha_i$  ulige og  $\alpha_i$  lige for alle  $i = 1, 2, \dots, m$ . Dette viser at  $n$  er et kvadrattal. Omvendt har alle kvadrattal også et ulige antal positive divisorer. De hele tal som har et ulige antal positive divisorer, er derfor netop kvadrattallene.

**Opgave 1.3.3.** 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 fem positive 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 størst mulige  $n$  med den ønskede egenskab er derfor  $n = 3^4 = 81$  da  $5^4 > 500$ .

**Opgave 1.3.4.** Tal med netop syv divisorer må ifølge sætning 1.3.1 være på formen  $p^6$ , hvor  $p$  er et primtal. Et sådant tal er derfor altid et kubiktal da  $p^6 = (p^2)^3$ , og produktet af sådanne tal er derfor også et kubiktal.

**Opgave 1.3.5.** Da  $n$  skal være delelig med  $1001 = 7 \cdot 11 \cdot 13$ , må både 7, 11 og 13 indgå i primfaktoropløsningen af  $n$ . Sæt

$$n = 7^{\alpha_1} \cdot 11^{\alpha_2} \cdot 13^{\alpha_3} \cdot p_4^{\alpha_4} \dots p_s^{\alpha_s}, \quad \alpha_i \geq 1, s \geq 3$$

Antallet af divisorer i  $n$  er netop  $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1)$ , og dermed er

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_s + 1) = 1001 = 7 \cdot 11 \cdot 13.$$

Af denne ligning ses at  $s \leq 3$ , og dermed at  $s = 3$  og  $n = 7^{\alpha_1} \cdot 11^{\alpha_2} \cdot 13^{\alpha_3}$ . Nu er

$$(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) = 7 \cdot 11 \cdot 13,$$

og dvs. at  $\alpha_1, \alpha_2$  og  $\alpha_3$  er 6, 10 og 12 i en eller anden rækkefølge. De mulige værdier af  $n$  er altså  $7^6 \cdot 11^{10} \cdot 13^{12}$ ,  $7^6 \cdot 11^{12} \cdot 13^{10}$ ,  $7^{10} \cdot 11^6 \cdot 13^{12}$ ,  $7^{10} \cdot 11^{12} \cdot 13^6$ ,  $7^{12} \cdot 11^6 \cdot 13^{10}$  og  $7^{12} \cdot 11^{10} \cdot 13^6$ .

**Opgave 1.4.1.**  $\gcd(12, 45) = 3$ ,  $\gcd(1000, 1205) = 5$ ,  $\gcd(1024, 12) = 4$ ,  $\gcd(88, 90) = 2$  og  $\gcd(1002, 1003) = 1$ .

**Opgave 1.4.2.** Hvis  $d$  er divisor i  $n$  og  $n + 1$ , må  $d$  også være divisor i  $(n + 1) - 1 = 1$ , og altså  $\gcd(n, n + 1) = 1$ . Hvis  $d$  er divisor i  $n$  og  $n + 2$ , må  $d$  også være divisor i  $2 = (n + 2) - n$ . Hvis  $n$  er lige, har vi derfor  $\gcd(n, n + 2) = 2$ , og hvis  $n$  er ulige,  $\gcd(n, n + 2) = 1$ .

**Opgave 1.4.3.** Da  $754 = 2 \cdot 338 + 78$ ,  $338 = 4 \cdot 78 + 26$  og  $78 = 3 \cdot 26 + 0$ , er  $\gcd(754, 338) = 26$ .

**Opgave 1.4.4.** Da  $b$  og  $c$  ikke har nogen fælles primfaktorer, må de fælles divisorer i  $a$  og  $b$  være de samme som de fælles divisorer i  $ac$  og  $b$ . Dermed er  $\gcd(a, b) = \gcd(ac, b)$ .

**Opgave 1.4.5.** Brøken er uforkortelig når største fælles divisor for nævner og tæller er 1. Ifølge sætning 1.4.1 er

$$\begin{aligned} \gcd(n^4 + 3n^2 + 1, n^3 + 2n) &= \gcd(n^4 + 3n^2 + 1 - n(n^3 + 2n), n^3 + 2n) \\ &= \gcd(n^2 + 1, n^3 + 2n) \\ &= \gcd(n^2 + 1, n^3 + 2n - n(n^2 + 1)) = \gcd(n^2 + 1, n) \\ &= \gcd(n^2 + 1 - n \cdot n, n) = \gcd(1, n) = 1. \end{aligned}$$

**Opgave 1.4.6.** Brøken er uforkortelig når største fælles divisor for nævner og tæller er 1. Ifølge sætning 1.4.1 er

$$\begin{aligned} \gcd(m^4 + 3m^3 - 3m^2 + 2m - 2, m - 1) &= \\ \gcd(m^4 + 3m^3 - 3m^2 + 2m - 2 - 3m^2(m - 1) - 2(m - 1), m - 1) &= \\ \gcd(m^4, m - 1). \end{aligned}$$

Da  $m$  og  $m - 1$  er indbyrdes primiske, må  $m^4$  og  $m - 1$  også være indbyrdes primiske, dvs.  $\gcd(m^4, m - 1) = 1$ . Dermed er brøken uforkortelig.



**Opgave 1.4.7.** At  $\frac{3n^2+3n+9}{3n+2}$  er et helt tal, er ensbetydende med at  $3n+2$  går op i  $3n^2+3n+9$ , dvs. at  $\gcd(3n+2, 3n^2+3n+9) = 3n+2$ . Ved at udnytte at  $3n+2$  og 3 er indbyrdes primiske får vi af sætning 1.4.1 og sætning 1.4.2 at

$$\begin{aligned}\gcd(3n+2, 3n^2+3n+9) &= \gcd(3n+2, 3n^2+3n+9 - n(3n+2)) \\ &= \gcd(3n+2, n+9) \\ &= \gcd(3n+2, 3(n+9)) \\ &= \gcd(3n+2, 3n+27) \\ &= \gcd(3n+2, 25).\end{aligned}$$

Altså er  $\frac{3n^2+3n+9}{3n+2}$  er et helt tal, netop når  $3n+2$  er divisor i 25, dvs. netop når  $3n+2$  er blandt tallene  $\pm 1, \pm 5, \pm 25$ . De eneste muligheder er derfor  $n = -9, n = -1$  og  $n = 1$ .

**Opgave 1.4.8.** Først regner vi på  $\gcd(a_n, a_{n+1})$ . Ved at udnytte at  $2n+1$  og 2 er indbyrdes primiske får vi af sætning 1.4.1 og sætning 1.4.2 at

$$\begin{aligned}\gcd(a_n, a_{n+1}) &= \gcd(n^2+500, n^2+2n+1+500) \\ &= \gcd(n^2+500, n^2+2n+1+500 - (n^2+500)) \\ &= \gcd(n^2+500, 2n+1) = \gcd(2(n^2+500), 2n+1) \\ &= \gcd(2n^2+1000, 2n+1) = \gcd(2n^2+1000 - n(2n+1), 2n+1) \\ &= \gcd(1000-n, 2n+1) = \gcd(2(1000-n), 2n+1) \\ &= \gcd(2000-2n, 2n+1) = \gcd(2000-2n+(2n+1), 2n+1) \\ &= \gcd(2001, 2n+1).\end{aligned}$$

Heraf ses at  $\gcd(a_n, a_{n+1})$  altid er divisor i 2001 og dermed højst 2001. Da  $\gcd(a_{1000}, a_{1001}) = 2001$ , er det den mindste værdi for  $N$ .

**Opgave 1.4.9.**  $\text{lcm}(10, 12) = 60$ ,  $\text{lcm}(2 \cdot 3^4 \cdot 7^8, 2^2 \cdot 3^3 \cdot 7^3 \cdot 11) = 2^2 \cdot 3^4 \cdot 7^8 \cdot 11$ ,  $\text{lcm}(13, 17) = 13 \cdot 17 = 221$ .

**Opgave 1.4.10.** Den største potens af  $p_i$  som går op i både  $a$  og  $b$ , er  $p_i^{\min(\alpha_i, \beta_i)}$  for  $i = 1, 2, \dots, n$ . Derfor må deres største fælles divisor være

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \dots p_n^{\min(\alpha_n, \beta_n)}.$$

Ifølge korollar 1.1.4 går  $a$  op i et tal, netop når  $p^{\alpha_i}$  går op i tallet for  $i = 1, 2, \dots, n$ . Tilsvarende for  $b$ . Både  $a$  og  $b$  går derfor op i et tal netop når  $p_i^{\max(\alpha_i, \beta_i)}$  går op i tallet for  $i = 1, 2, \dots, n$ . Derfor må mindste fælles multiplum være

$$\text{lcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \dots p_n^{\max(\alpha_n, \beta_n)}.$$

Da  $\alpha_i \cdot \beta_i = \min(\alpha_i, \beta_i) \cdot \max(\alpha_i, \beta_i)$  for alle  $i = 1, 2, \dots, n$ , fås

$$a \cdot b = \gcd(a, b) \cdot \text{lcm}(a, b)$$

som ønsket.

**Opgave 1.4.11.** Med brug af opgave 1.4.3 fås  $\gcd(754, 338) = 26 = 338 - 4 \cdot 78 = 338 - 4(754 - 2 \cdot 338) = -4 \cdot 754 + 9 \cdot 338$ .

**Opgave 1.4.12.** Tallene på formen  $s \cdot 35 + t \cdot 15$ ,  $s, t \in \mathbb{Z}$ , er netop alle multipla af  $\gcd(35, 15) = 5$ . Vi viser først at alle multipla af 5 kan skrives på denne form: Ifølge Bezouts identitet findes hele tal  $s'$  og  $t'$  så  $5 = \gcd(35, 15) = s' \cdot 35 + t' \cdot 15$ . (De kan også nemt findes, fx  $5 = -2 \cdot 35 + 5 \cdot 15$ ). Dermed kan alle multipla af 5 skrives på formen  $s \cdot 35 + t \cdot 15$ , da

$$5m = m s' \cdot 35 + m t' \cdot 15.$$

Så viser vi at ethvert tal på denne form er et multiplum af 5: Da 5 går op i både 15 og 35, må 5 også gå op i  $s \cdot 35 + t \cdot 15$ ,  $s, t \in \mathbb{Z}$ .

**Opgave 1.4.13.** Vi viser først at alle multipla af  $\gcd(a, b)$  kan skrives på formen  $ax + by$ ,  $x, y \in \mathbb{Z}$ , og der dermed findes  $x, y \in \mathbb{Z}$  der løser ligningen, når  $c$  er et multiplum af  $\gcd(a, b)$ . Ifølge Bezouts identitet findes hele tal  $x'$  og  $y'$  så  $\gcd(a, b) = x'a + y'b$ . Dermed er

$$m \gcd(a, b) = m x' a + m y' b,$$

som ønsket.

Nu vises omvendt at  $c$  er et multiplum af  $\gcd(a, b)$  hvis der findes  $x, y \in \mathbb{Z}$  så  $c = xa + yb$ . Da  $\gcd(a, b)$  går op i både  $a$  og  $b$ , må det også gå op i et  $c$  på formen  $c = xa + yb$ . Dermed er  $c$  et multiplum af  $\gcd(a, b)$ .

**Opgave 1.5.1.** Antag først at  $a$  og  $b$  har samme rest ved division med  $n$ , dvs. at  $a = q_a n + r$  og  $b = q_b n + r$ ,  $0 \leq r < n$ . Da går  $n$  op i  $a - b = (q_a n + r) - (q_b n + r) = (q_a - q_b)n$ , og dermed er  $a \equiv b \pmod{n}$ .

Antag omvendt at  $a \equiv b \pmod{n}$ , dvs. at  $n \mid a - b$ . Lad  $a = q_a n + r_a$  og  $b = q_b n + r_b$ ,  $0 \leq r_a, r_b < n$ . Da ved vi at  $n$  går op i  $a - b = (q_a - q_b)n + (r_a - r_b)$ , og dermed også i  $r_a - r_b$ . Da  $-n < r_a - r_b < n$ , må  $r_a - r_b = 0$ , og altså  $r_a = r_b$  som ønsket.

**Opgave 1.5.2.** At  $a \equiv 0 \pmod{n}$ , betyder at  $n \mid a - 0 = a$ , dvs. at  $n$  går op i  $a$ . Restklassen repræsenteret ved 0 er derfor netop alle multipla af  $n$ .

**Opgave 1.5.3.** At  $a \equiv b \pmod{2}$  betyder at  $2 \mid a - b$ , altså at  $a$  og  $b$  har samme paritet, dvs. at de enten begge er lige, eller begge er ulige.

**Opgave 1.5.4.** a)  $182 \equiv 92 \pmod{18}$  da  $18 \mid 182 - 92 = 90$ . b)  $-43 \equiv 1 \pmod{4}$  da  $4 \mid 1 - (-43) = 44$ . c)  $111 \not\equiv 13 \pmod{11}$  da  $11 \nmid 111 - 13 = 98$ .

**Opgave 1.5.5.** ii) At  $a \equiv b$  og  $c \equiv d \pmod{n}$ , betyder at  $n \mid a - b$  og  $n \mid c - d$ . Dermed må  $n \mid (a - b) - (c - d) = (a - c) - (b - d)$ , og altså  $a - c \equiv b - d \pmod{n}$ .

iv) At  $a \equiv b \pmod{n}$ , betyder at  $n \mid a - b$ . Dermed må  $n \mid c(a - b) = ca - cb$ , og altså  $c \cdot a \equiv c \cdot b \pmod{n}$ .

v) For at vise at  $a \equiv b \pmod{n}$  medfører at  $a^k \equiv b^k \pmod{n}$ , benyttes iii)  $k - 1$  gange.

**Opgave 1.5.6.** Ligningen  $x - 12 \equiv 5 \pmod{11}$  omskrives til  $x \equiv 5 + 12 \equiv 6 \pmod{11}$ . Det er altså netop restklassen repræsenteret ved 6 modulo 11 der løser ligningen, og løsningsmængden er derfor  $\{\dots, -16, -5, 6, 17, 28, \dots\}$ .

**Opgave 1.5.7.** Vi regner modulo 13 ved brug af regnereglerne fra sætning 1.5.1:

$$27^{103} \cdot 17^2 \cdot 5^{14} \equiv 1^{103} \cdot 4^2 \cdot (5^2)^7 \equiv 1 \cdot 3 \cdot (-1)^7 \equiv -3 \equiv 10 \pmod{13}.$$

**Opgave 1.5.8.** Sidste ciffer i et positivt heltal er netop resten ved division med 10, derfor regnes modulo 10:

$$2007^{2007} \equiv 7^{2007} \equiv (7^2)^{1003} \cdot 7 \equiv (-1)^{1003} \cdot 7 \equiv -7 \equiv 3 \pmod{10}.$$

Altså er 3 sidste ciffer i  $2007^{2007}$ .

**Opgave 1.5.9.** Lad  $p$  være et primtal, og antag at  $a \cdot b \equiv 0 \pmod{p}$ . Dette betyder at  $p \mid a \cdot b$ , og altså at  $p \mid a$  eller  $p \mid b$ , hvilket jo netop betyder at  $a \equiv 0$  eller  $b \equiv 0 \pmod{p}$ .

**Opgave 1.5.10.** a) Løsningerne til  $x^2 \equiv 4 \pmod{5}$  er netop restklasserne repræsenteret ved 2 og 3 modulo 5. b) Ligningen  $x^2 \equiv 2 \pmod{5}$  har ingen løsninger. c) Løsningerne til  $x^2 \equiv 1 \pmod{8}$  er netop alle ulige tal. d) Løsningerne til  $x^2 \equiv 0 \pmod{2}$  er netop alle lige tal.

**Opgave 1.5.11.** Ligningen  $x^2 \equiv 1 \pmod{p}$  omskrives til

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

Ifølge nulreglen ved vi nu at  $x + 1 \equiv 0$  eller  $x - 1 \equiv 0 \pmod{p}$ . Dermed er de eneste løsninger restklasserne 1 og  $-1$  modulo  $p$ .

**Opgave 1.5.12.** ii) Vi viser at  $n \equiv t(n) \pmod{9}$ , da dette viser det ønskede:

$$\begin{aligned} n &= a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0 \\ &\equiv a_m \cdot 1^m + a_{m-1} \cdot 1^{m-1} + \dots + a_1 \cdot 1 + a_0 \\ &\equiv a_m + a_{m-1} + \dots + a_1 + a_0 = t(n) \pmod{9}. \end{aligned}$$

iii) Vi viser at  $n$  er kongruent med plus eller minus den alternerende tværsom af  $n$  modulo 11, da det viser det ønskede.

$$\begin{aligned} n &= a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0 \\ &\equiv a_m \cdot (-1)^m + a_{m-1} \cdot (-1)^{m-1} + \dots + a_1 \cdot (-1) + a_0 \\ &\equiv (-1)^m (a_m - a_{m-1} + \dots - (-1)^m a_1 + (-1)^m a_0) \pmod{11}. \end{aligned}$$

**Opgave 1.5.13.** Et tal er deleligt med 18 netop hvis det er lige, og tværsommen er delelig med 9. Et tal er deleligt med 22 netop hvis det er lige, og den alternerende tværsom er delelig med 11.

**Opgave 1.6.1.** De kvadratiske rester modulo 3 er 0 og 1. De kvadratiske rester modulo 4 er 0 og 1. De kvadratiske rester modulo 5 er 0, 1 og 4.

**Opgave 1.6.2.** a) Vi regner modulo 4. Bemærk først at et lige tal i anden har rest 0 ved division med 4, mens et ulige tal i anden har rest 1. Da der er to lige



og to ulige tal blandt fire på hinanden følgende tal, så er summen af kvadraterne af fire på hinanden følgende tal kongruent med 2 modulo 4. Da 2 ikke er kvadratisk rest modulo 4, kan denne sum ikke være et kvadrattal.

b) Vi regner igen modulo 4. De der er 2 eller 3 lige tal og tilsvarende 3 eller 2 ulige tal blandt fem på hinanden følgende tal, er summen af kvadraterne af fem på hinanden følgende tal kongruent med 2 eller 3 modulo 4. Da hverken 2 eller 3 er kvadratiske rester modulo 4, kan denne sum ikke være kvadrattal.

c) Vi regner igen modulo 4. Da der er tre lige og tre ulige tal blandt seks på hinanden følgende tal, er summen af kvadraterne af seks på hinanden følgende tal kongruent med 3 modulo 4, og da 3 ikke er kvadratisk rest modulo 4, kan denne sum ikke være et kvadrattal.

**Opgave 1.6.3.** Hvis vi betragter ligningen  $x^2 + 10 = 5^y$  modulo 4, får vi at  $x^2 + 2 \equiv 1 \pmod{4}$ . Altså er  $x^2 \equiv 3 \pmod{4}$ , og da 3 ikke er kvadratisk rest modulo 4, har ligningen ingen løsninger.

**Opgave 1.6.4.** Hvis vi betragter ligningen  $x^2 - 3y^2 = 17$  modulo 3, får vi at  $x^2 \equiv 2 \pmod{3}$ , og da 2 ikke er kvadratisk rest modulo 3, har ligningen ingen løsninger.

**Opgave 1.6.5.** Produktet af to lige tal er altid deleligt med 4, dvs. produktet af to lige tal lagt til 2006 har rest 2 modulo 4, men 2 er ikke kvadratisk rest modulo 4. Hvis der findes fire tal med den ønskede egenskab, må tre af disse derfor være ulige. Blandt tre ulige tal findes to som har samme rest modulo 4. Produktet af disse to har rest 1 modulo 4, og dermed har produktet lagt til 2006 rest 3 modulo 4, men 3 er ikke kvadratisk rest modulo 4. Derfor findes der ikke fire tal med den ønskede egenskab.

**Opgave 1.6.6.** Hvis  $x^2 + y^2 + z^2 = 2xyz$ , skal enten et eller tre af tallene  $x$ ,  $y$  og  $z$  være lige. Antag at kun et af tallene er lige, fx  $x = 2x_1$ . Da vil  $y^2 + z^2 = 4x_1yz - 4x_1^2 \equiv 0 \pmod{4}$ . Vi ved at et ulige tal i anden har rest 1 modulo 4, og dermed har ligningen i dette tilfælde ingen løsninger. Altså er alle tre tal lige. Ved at sætte  $x = 2x_1$ ,  $y = 2y_1$  og  $z = 2z_1$  får vi  $x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1$ . Ved samme argumentation følger nu at  $x_1$ ,  $y_1$ ,  $z_1$  er lige, og da dette kan gentages, vil  $x$ ,  $y$ ,  $z$  være delelige med  $2^n$  for alle  $n \in \mathbb{N}$ . Dermed er den eneste løsning  $x = y = z = 0$ .

**Opgave 1.6.7.** Lad  $x, y \in \{1, 2, 3, \dots, p-1\}$  og  $x \neq y$ . Antag at  $x^2 \equiv y^2 \pmod{p}$ , hvilket betyder at  $p \mid x^2 - y^2 = (x-y)(x+y)$ . Da  $x \not\equiv y \pmod{p}$ , går  $p$  ikke op i  $x-y$ , og dermed går  $p$  ifølge nulreglen op i  $x+y$ . Da  $x, y \in \{1, 2, \dots, p-1\}$ , må  $x+y = p$ . Af dette følger at tallene  $1^2, 2^2, \dots, (\frac{p-1}{2})^2$  alle har forskellige rester modulo  $p$ , mens  $x^2 \equiv (p-x)^2 \pmod{p}$ . Dvs. blandt tallene  $1^2, 2^2, \dots, (p-1)^2$  er der netop  $\frac{p-1}{2}$  forskellige kvadratiske rester. Ingen af resterne  $1^2, 2^2, \dots, (\frac{p-1}{2})^2$  kan være repræsentant for 0-restklassen ifølge nulreglen. Altså er netop halvdelen af tallene  $1, 2, \dots, p-1$  kvadratiske rester modulo  $p$ .

**Opgave 1.6.8.** Hvis  $m = 1$ , er der ingen løsning. Hvis  $m = 2$ , er  $n = 1$ . Antag at  $m > 2$ . Betragter vi ligningen  $7^n = 3 + 2^m$  modulo 8, får vi  $(-1)^n \equiv 3 \pmod{8}$  hvilket er umuligt. Dermed er den eneste løsning  $m = 2$  og  $n = 1$ .

**Opgave 1.6.9.** Af ligningen  $6(x! + 3) = y^2 + 5$  ses at  $y^2$  er ulige, og dermed at  $y$  også er ulige. Da alle kvadrater af ulige tal har rest 1 ved division med 8, er  $y^2 \equiv 1 \pmod{8}$ . For  $x \geq 4$  er  $6(x! + 3) \equiv 6 \cdot 3 \equiv 2 \pmod{8}$ , mens  $y^2 + 5 \equiv 6 \pmod{8}$ . Der er altså ingen løsninger når  $x \geq 4$ . Nu er det let at tjekke mulighederne  $x = 1, 2, 3$ . Samtlige løsninger er dermed  $(x, y) = (2, 5)$  og  $(x, y) = (3, 7)$ .

**Opgave 1.6.10.** Et tal er deleligt med  $1599 = 39 \cdot 41$  netop hvis det er deleligt med både 39 og 41. Vi regner nu modulo henholdsvis 39 og 41 for at undersøge for hvilke  $n$  tallene 39 og 41 går op i  $S = 46^n + 34^n - 7^n - 5^n$ .

$$S = 46^n + 34^n - 7^n - 5^n \equiv 7^n + (-5)^n - 7^n - 5^n \equiv ((-1)^n - 1)5^n \pmod{39},$$

dvs. at  $S$  er delelig med 39, netop når  $n$  er lige.

$$S = 46^n + 34^n - 7^n - 5^n \equiv 5^n + (-7)^n - 7^n - 5^n \equiv ((-1)^n - 1)7^n \pmod{41},$$

dvs. at  $S$  er delelig med 41 netop når  $n$  er lige. Samlet er  $S$  delelig med 1599 netop når  $n$  er lige.

**Opgave 1.6.11.** Antag at  $n = d_1^2 + d_2^2 + d_3^2 + d_4^2$ . Hvis  $n$  er ulige, er alle divisorer i  $n$  ulige. Altså vil  $d_1^2 + d_2^2 + d_3^2 + d_4^2 \equiv 1 + 1 + 1 + 1 \equiv 0 \pmod{4}$ , hvilket er umuligt.

Hvis  $n$  er lige, vil  $d_1 = 1$  og  $d_2 = 2$ , og dermed  $n \equiv 1 + 0 + d_3^2 + d_4^2 \not\equiv 0 \pmod{4}$ , dvs. at 4 ikke går op i  $n$ . Samlet ser vi at  $d_3 = p$ , og at  $d_4 = 2p$  eller  $d_4 = q$ , hvor  $p$  og  $q$  er ulige primtal. Hvis  $d_4 = q$ , vil  $n \equiv 1 + 2^2 + p^2 + q^2 \equiv 3 \pmod{4}$ , hvilket er umuligt da  $n$  er lige. Dermed er  $n = 1 + 4 + p^2 + 4p^2 = 5p^2 + 5 = 5(p^2 + 1)$ . Af

dette ses at 3 ikke går op i  $n$ . Dermed er  $p = 5$ , og dvs. at  $n = 5(5^2 + 1) = 130$  er det eneste tal der opfylder det ønskede.

**Opgave 1.6.12.** Hvis vi betragter ligningen  $19x^3 - 84y^2 = 1984$  modulo 7, skal  $x$  opfylde at  $5x^3 \equiv 3 \pmod{7}$ , dvs. at  $x^3 \equiv 3 \cdot 3 \equiv 2 \pmod{7}$ , men 2 er ikke kubisk rest modulo 7. Dermed har ligningen ingen heltallige løsninger. (Man finder samtlige kubiske rester modulo 7 ved at se på resterne af  $0^3, 1^3, 2^3, 3^3, 4^3, 5^3, 6^3$ ).

**Opgave 1.6.13.** For  $n = m = 1$  er  $k = 14$ . Antag at der findes et  $k < 14$  med den ønskede egenskab.

Hvis  $n$  er ulige, er  $k = 19^n - 5^m \equiv (-1)^n - 5 \equiv 4 \pmod{10}$ . Sidste ciffer i  $k$  er derfor 4, dvs.  $k = 4$ . Men  $19^n - 5^m \equiv 1 - 2^m \pmod{3}$  har aldrig rest 1 modulo 3, dvs. dette er ikke muligt.

Hvis  $n$  er lige, er  $k = 19^n - 5^m \equiv (-1)^n - 5 \equiv 6 \pmod{10}$ . Sidste ciffer i  $k$  er derfor 6, dvs.  $k = 6$ . Men  $19^n - 5^m \equiv 3^n - 1 \equiv 0 \pmod{4}$ , dvs.  $k = 6$  er ikke muligt.

Dermed er  $k = 14$  det mindste  $k$  på denne form.

**Opgave 1.7.1.** Resultatet følger af sætning 1.7.1.

**Opgave 1.7.2.** Lad  $d$  være divisor i  $n$ , og sæt  $n = dn'$ . Ifølge sætning 1.7.1 i) er

$$a^n - b^n = (a^d)^{n'} - (b^d)^{n'} = (a^d - b^d)((a^d)^{n'-1} + (a^d)^{n'-2}b^d + \dots + (b^d)^{n'-1}).$$

Altså går  $a^d - b^d$  op i  $a^n - b^n$ .

**Opgave 1.7.3.** Antag at  $a^n - 1$  er et primtal. Vi udnytter at

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a + 1),$$

til at indse at  $a = 2$ . Hvis  $n$  har en ikke-triviel divisor  $d$ , ved vi fra opgave 1.7.2 at  $a^n - 1$  er delelig med  $a^d - 1$ , hvilket viser at  $a^n - 1$  ikke er et primtal da  $1 < a^d - 1 < a^n - 1$ . Dermed må  $n$  være et primtal hvis  $a^n - 1$  er et primtal.

**Opgave 1.7.4.** Da

$$n^3 + 100 = n^3 + 10^3 - 900 = (n + 10)(n^2 - 10n + 100) - 900,$$

går  $n + 10$  op i  $n^3 + 100$  netop når  $n + 10$  går op i 900. Det største  $n$  så  $n^3 + 100$  er delelig med  $n + 10$ , er derfor  $n = 890$ .

**Opgave 1.7.5.** Summen af samtlige positive divisorer i  $n$  er lig med

$$(1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \dots (1 + p_r + p_r^2 + \dots + p_r^{\alpha_r})$$

da hver divisor netop svarer til et led når man ganger alle parenteserne sammen. Vha. omskrivningen i sætning 1.7.1 i) giver dette det ønskede.

**Opgave 1.7.6.** Bemærk først at hvis  $a + b$  er delelig med  $n$ , da er  $b \equiv -a \pmod{n}$  og dermed

$$a^{n-1} - a^{n-2}b + \dots - ab^{n-2} + b^{n-1} \equiv na^{n-1} \equiv 0 \pmod{n}.$$

Altså er  $a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \dots - ab^{n-2} + b^{n-1})$  delelig med  $n^2$  da begge parenteser er delelige med  $n$ . Dette medfører at

$$1^n + 2^n + \dots + n^n = (1^n + (n-1)^n) + (2^n + (n-2)^n) + \dots + \left(\left(\frac{n-1}{2}\right)^n + \left(\frac{n+1}{2}\right)^n\right) + (n^n)$$

er delelig med  $n^2$ .

**Opgave 1.7.7.** Vi ved at  $v_p(a - 1) > 0$ . Dette betyder at  $a - 1$  er delelig med  $p$ , og altså  $a \equiv 1 \pmod{p}$ . Ifølge sætning 1.7.1 er

$$a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \dots + 1).$$

Nu undersøger vi den sidste faktor modulo  $p$ :

$$a^{k-1} + a^{k-2} + \dots + 1 \equiv 1 + 1 + \dots + 1 = k \not\equiv 0 \pmod{p}.$$

Da  $k$  ikke er delelig med  $p$ , er

$$v_p(a^k - 1) = v_p(a - 1) + v_p(a^{k-1} + a^{k-2} + \dots + 1) = v_p(a - 1),$$

som ønsket.

**Opgave 1.7.8.** Først faktoriseres  $3^{1024} - 1 = 3^{2^{10}} - 1$  vha. sætning 1.7.1.

$$3^{2^{10}} - 1 = (3 - 1)(3 + 1)(3^2 + 1)(3^{2^2} + 1) \dots (3^{2^9} + 1).$$



Da  $3^m \equiv 1 \pmod{4}$  for lige  $m$ , er alle parenteser på nær  $(3+1)$  delelig med 2, men ikke med 4. Dermed er  $v_2(3^{1024} - 1) = 12$ .

**Opgave 1.7.9.** Antag at  $m$  er et ulige positivt tal som ikke er delelig med 5. Ved at faktorisere får vi

$$a^n = 2^m + 3^m = (2+3)(2^{m-1} - 2^{m-2} \cdot 3 + \dots - 2 \cdot 3^{m-2} + 3^{m-1}).$$

Dette viser at 5 går op i  $a$ . Hvis  $n > 1$ , skal 5 også gå op i

$$2^{m-1} - 2^{m-2} \cdot 3 + \dots - 2 \cdot 3^{m-2} + 3^{m-1}.$$

Men da  $2 \equiv -3 \pmod{5}$ , er

$$\begin{aligned} 2^{m-1} - 2^{m-2} \cdot 3 + \dots - 2 \cdot 3^{m-2} + 3^{m-1} &\equiv 2^{m-1} + 2^{m-1} + \dots + 2^{m-1} \\ &= m2^{m-1} \\ &\not\equiv 0 \pmod{5}, \end{aligned}$$

Dermed er  $n = 1$ .

**Opgave 1.7.10.** Lad  $d = \gcd(a, b)$ , og sæt  $a = da'$  og  $b = db'$ .

Først viser vi at  $m^d - 1$  går op i  $\gcd(m^a - 1, m^b - 1)$ : Vi ved fra opgave 1.7.2 at  $m^d - 1$  går op i både  $m^a - 1$  og  $m^b - 1$ , og dermed også i  $\gcd(m^a - 1, m^b - 1)$ .

Derefter viser vi at  $\gcd(m^a - 1, m^b - 1)$  går op i  $m^d - 1$ . Sæt  $n = \gcd(m^a - 1, m^b - 1)$ . Da er  $m^a \equiv 1 \pmod{n}$  og  $m^b \equiv 1 \pmod{n}$ . Ifølge Bezouts identitet findes hele tal  $s$  og  $t$  så  $d = sa + tb$ . Da  $d \leq a$  og  $d \leq b$ , må netop en af  $s$  og  $t$  være positiv. Antag uden tab af generalitet at  $s$  er positiv. Da er  $d - tb = sa$  og altså

$$m^d \equiv m^d \cdot (m^b)^{-t} \equiv m^{d-bt} \equiv m^{as} \equiv (m^a)^s \equiv 1 \pmod{n}.$$

Dermed må  $n$  gå op i  $m^d - 1$ , hvilket samlet viser at  $\gcd(m^a - 1, m^b - 1) = m^{\gcd(a,b)} - 1$ .

**Opgave 1.7.11.** Lad  $n$  være et positivt heltal,  $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$  og  $N_{n,k}$  tallet med  $2^n$  cifre som alle er  $k$ . Ved at faktorisere  $N_{n,k}$  vha. sætning 1.7.1 fås

$$N_{n,k} = k \cdot \frac{10^{2^n} - 1}{10 - 1} = k(10^{2^0} + 1)(10^{2^1} + 1)(10^{2^2} + 1) \cdots (10^{2^{n-1}} + 1).$$

Hvis  $n_1 < n_2$ , må  $10^{2^{n_1}} + 1$  gå op i

$$10^{2^{n_2}} - 1 = (10 - 1)(10^{2^0} + 1)(10^{2^1} + 1)(10^{2^2} + 1) \cdots (10^{2^{n_2-1}} + 1).$$

Dermed må  $\gcd(10^{2^{n_1}} + 1, 10^{2^{n_2}} + 1)$  gå op i  $\gcd(10^{2^{n_2}} - 1, 10^{2^{n_2}} + 1) = 1$ . De  $n$  faktorer  $10^{2^i} + 1$ ,  $i = 0, 1, 2, \dots, n-1$ , i faktoriseringen af  $N_{n,k}$  er derfor parvis indbyrdes primiske, dvs. de må hver have en primfaktor der ikke er primfaktor i de andre faktorer. Dette viser at  $N_{n,k}$  har mindst  $n$  forskellige primfaktorer.

**Opgave 1.7.12.** Vi bestemmer  $99^{703}$  modulo  $10^4$  vha. af binomialformlen:

$$99^{703} = (100 - 1)^{703} \equiv \binom{703}{1} 100 - 1 = 70300 - 1 \equiv 299 \pmod{10^4}.$$

Dermed er de fire sidste cifre 0299.

**Opgave 1.7.13.** Vi regner modulo  $b^4$  på udtrykket  $(b^2 + a)^b - a^b$  og udnytter undervejs binomialformlen:

$$(b^2 + a)^b - a^b \equiv \binom{b}{1} b^2 a^{b-1} = b^3 a^{b-1} \pmod{b^4}.$$

Da  $a$  og  $b$  ikke har nogen fælles primfaktorer og  $b > 1$ , er  $a^{b-1}$  ikke delelig med  $b$ . Dette viser at  $(b^2 + a)^b - a^b$  er delelig med  $b^3$ , men ikke med  $b^4$ , dvs. at  $n = 3$ .

**Opgave 1.8.1.**  $\phi(3) = 2$ ,  $\phi(4) = 2$ ,  $\phi(5) = 4$ ,  $\phi(6) = 2$ ,  $\phi(7) = 6$ ,  $\phi(8) = 4$ ,  $\phi(9) = 6$ ,  $\phi(10) = 4$ ,  $\phi(11) = 10$ ,  $\phi(12) = 4$ ,  $\phi(13) = 12$ ,  $\phi(14) = 6$ ,  $\phi(15) = 8$ ,  $\phi(16) = 8$ ,  $\phi(17) = 16$ ,  $\phi(18) = 6$ ,  $\phi(19) = 18$ .

**Opgave 1.8.2.** a) Samtlige primiske restklasser modulo 15 er repræsenteret ved 1, 2, 4, 7, 8, 11, 13, 14. Deres multiplikative inverse ses af følgende:  $1 \cdot 1 \equiv 1 \pmod{15}$ ,  $2 \cdot 8 \equiv 1 \pmod{15}$ ,  $4 \cdot 4 \equiv 1 \pmod{15}$ ,  $7 \cdot 13 \equiv 1 \pmod{15}$ ,  $11 \cdot 11 \equiv 1 \pmod{15}$ ,  $14 \cdot 14 \equiv 1 \pmod{15}$ . b)  $7x + 19 \equiv 36 \Leftrightarrow 7x \equiv 2 \Leftrightarrow x \equiv 13 \cdot 2 \equiv 11 \pmod{15}$ . Løsningen er altså restklassen 11 modulo 15.

**Opgave 1.8.3.** Det følger af sætning 1.5.3

**Opgave 1.8.4.** Det følger af sætning 1.8.3 og 1.8.7.

**Opgave 1.8.5.** Ifølge sætning 1.8.8 er  $\phi(120) = \phi(2^3 \cdot 3 \cdot 5) = 2^2 \cdot 2 \cdot 4 = 32$  og  $\phi(98) = \phi(2 \cdot 7^2) = 7 \cdot 6 = 42$ .

**Opgave 1.8.6.** Lad  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ , og antag at  $\phi(n) = 8$ . Da er

$$8 = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_r^{\alpha_r-1} (p_1-1)(p_2-1)\cdots(p_r-1).$$

Da  $p_i - 1$  skal gå op i 8, må primdivisorerne i  $n$  være blandt primtallene 2, 3 og 5. Dermed kan man nemt tjekke at de eneste muligheder er  $n = 2^4 = 16$ ,  $n = 2^3 \cdot 3 = 24$ ,  $2^2 \cdot 5 = 20$ ,  $n = 3 \cdot 5 = 15$  og  $n = 2 \cdot 3 \cdot 5 = 30$ .

Lad nu  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ , og antag at  $\phi(m) = 14$ . Da er

$$14 = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_r^{\alpha_r-1} (p_1-1)(p_2-1)\cdots(p_r-1).$$

Da  $p_i - 1$  skal gå op i 14, må primdivisorerne i  $m$  være blandt primtallene 2 og 3. Når  $m$  ikke har andre primdivisorer end 2 og/eller 3, er 7 ikke en divisor i  $\phi(m)$ , hvilket er en modstrid. Derfor findes ingen  $m$  så  $\phi(m) = 14$ .

**Opgave 1.8.7.** Lad primfaktoropløsningen af  $n$  være  $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ . Ifølge sætning 1.8.8 er

$$\begin{aligned} \phi(n^\alpha) &= \phi(p_1^{\alpha\alpha_1} p_2^{\alpha\alpha_2} \cdots p_m^{\alpha\alpha_m}) \\ &= p_1^{\alpha\alpha_1-1} (p_1-1) \cdots p_m^{\alpha\alpha_m-1} (p_m-1) \\ &= \left( (p_1^{\alpha_1})^{\alpha-1} \cdots (p_m^{\alpha_m})^{\alpha-1} \right) (p_1^{\alpha_1-1} (p_1-1) \cdots p_m^{\alpha_m-1} (p_m-1)) \\ &= n^{\alpha-1} \phi(n). \end{aligned}$$

**Opgave 1.8.8.** Lad primfaktoropløsningen af  $n$  være  $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ . Vi har tidligere set at summen af samtlige positive divisorer i  $n$  er

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{\alpha_r})$$

Desuden ved vi fra sætning 1.8.7 at  $\phi(ab) = \phi(a) \cdot \phi(b)$  for to indbyrdes pri-

miske hele tal  $a$  og  $b$ , og derfor må

$$\begin{aligned} \sum_{d|n} \phi(d) &= \prod_{i=1}^m \left( 1 + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{\alpha_i}) \right) \\ &= \prod_{i=1}^m \left( 1 + (p_i-1) + (p_i-1)p_i + \cdots + (p_i-1)p_i^{\alpha_i-1} \right) \\ &= \prod_{i=1}^m \left( 1 + (p_i-1) \frac{p_i^{\alpha_i} - 1}{p_i - 1} \right) \\ &= \prod_{i=1}^m p_i^{\alpha_i} = n. \end{aligned}$$

**Opgave 1.9.1.** Hvis  $n$  er et primtal, gælder ifølge Wilsons sætning at

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

dvs. at  $n$  går op i  $(n-1)! + 1$ .

Hvis  $n > 1$  ikke er et primtal, findes et primtal  $p$  som går op i  $n$ , hvor  $p < n$ . Da  $p$  går op i  $(n-1)!$ , kan  $p$  og dermed heller ikke  $n$  gå op i  $(n-1)! + 1$ . Altså er betingelsen kun opfyldt når  $n$  er et primtal eller  $n = 1$ .

**Opgave 1.9.2.** Vi viser indirekte at svaret er nej. Antag at mængden

$$S = \{n, n+1, \dots, n+9\}$$

kan deles i to disjunkte mængder  $S_1$  og  $S_2$  så produkterne  $\pi_1$  og  $\pi_2$  af henholdsvis elementerne i  $S_1$  og  $S_2$  er ens. Blandt ti på hinanden følgende tal kan højst et være deleligt med 11, men hvis et af tallene var deleligt med 11, ville de to produkter ikke være ens. Tallene i  $S$  repræsenterer således restklasserne  $1, 2, \dots, 10$  modulo 11. Ifølge Wilsons sætning gælder nu at

$$\pi_1^2 = \pi_1 \pi_2 \equiv (11-1)! \equiv -1 \pmod{11}.$$

Ved at tjekke kvadratet på alle resterne modulo 11 ses at  $-1$  ikke er kvadratisk rest modulo 11, hvilket viser at det ikke er muligt. (Senere skal vi se at  $-1$  ikke er kvadratisk rest modulo nogen primtal på formen  $4n+3$ ).



**Opgave 1.9.3.** Antag at  $p$  er et primtal på formen  $p = 4n + 1$ . Ifølge Wilsons sætning gælder

$$\begin{aligned} -1 &\equiv (p-1)! = 1 \cdot 2 \cdots 2n \cdot (2n+1) \cdots (p-2) \cdot (p-1) \\ &\equiv 1 \cdot 2 \cdots 2n \cdot (-2n) \cdots (-2) \cdot (-1) \\ &\equiv (-1)^{2n} ((2n)!)^2 = ((2n)!)^2 \pmod{p}. \end{aligned}$$

Dvs. at  $((2n)!)^2 \equiv -1 \pmod{p}$ , og altså at  $-1$  er kvadratisk rest modulo  $p$ .

**Opgave 1.10.1.** Hvis  $a$  ikke er primisk med  $p$ , er  $a \equiv 0 \pmod{p}$ , og da er  $a \equiv 0 \equiv a^p$ . Hvis  $a$  er primisk med  $p$ , siger Fermats lille sætning at  $a^{p-1} \equiv 1 \pmod{p}$ , og dermed er  $a^p \equiv a \pmod{p}$ .

**Opgave 1.10.2.** Bemærk først at  $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ , og at  $p = 2, 3, 5, 7, 13$  opfylder at  $p-1 \mid 12$ . Ifølge Fermats lille sætning ved vi at

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

hvis  $a$  er primisk med  $p$ . I dette tilfælde vil yderligere  $a^{13} \equiv a \pmod{p}$  da vi ved at  $p-1 \mid 12$ . Hvis  $a$  ikke er primisk med  $p$ , vil  $a^{13} \equiv 0 \equiv a \pmod{p}$ . Samlet er  $a^{13} - a$  delelig med primtallene 2, 3, 5, 7, 13 og dermed også med 2730 som er produktet af dem.

**Opgave 1.10.3.** Ifølge sætning 1.8.3 er  $\phi(32) = \phi(2^5) = 2^4 = 16$ . Da 17 er primisk med 32, gælder ifølge Eulers sætning at  $17^{16} \equiv 1 \pmod{32}$ . Altså er

$$17^{1601} = 17 \cdot (17^{16})^{100} \equiv 17 \cdot 1^{100} \equiv 17 \pmod{32}.$$

**Opgave 1.10.4.** Antag uden tab af generalitet at  $a \geq b$ . Da  $a \equiv b \pmod{\phi(n)}$ , er  $a = q \cdot \phi(n) + b$  for et ikke-negativt heltal  $q$ . Ifølge Eulers sætning er  $m^{\phi(n)} \equiv 1 \pmod{n}$ , og dermed

$$m^a = m^{q \cdot \phi(n) + b} = (m^{\phi(n)})^q \cdot m^b \equiv 1^q \cdot m^b = m^b \pmod{n}.$$

**Opgave 1.10.5.** Bemærk først at  $x_1 + x_2 + \cdots + x_k = 1492 \equiv 1 \pmod{7}$ . Ifølge korollar 1.10.3 er  $x^7 \equiv x \pmod{7}$  for alle hele tal  $x$ . Dermed er

$$x_1^7 + x_2^7 + \cdots + x_k^7 \equiv x_1 + x_2 + \cdots + x_k \equiv 1 \pmod{7}.$$

Altså findes der ikke hele tal med sum 1492 så  $x_1^7 + x_2^7 + \cdots + x_k^7 = 70707$ , da  $70707 \equiv 0 \pmod{7}$ .

**Opgave 1.10.6.** Da  $\phi(100) = \phi(2^2) \cdot \phi(5^2) = 40$ , og 3, 97 og 13 alle er primiske med 100, kan vi reducere eksponenterne modulo 40.

$$\begin{aligned} 3^{214} \cdot 97^{828} \cdot 13^{521} &\equiv 3^{14} \cdot (-3)^{28} \cdot 13 \\ &\equiv 3^{14} \cdot (-1)^{28} \cdot 3^{28} \cdot 13 \\ &\equiv (-1)^{28} \cdot 3^{42} \cdot 13 \\ &\equiv 3^2 \cdot 13 \equiv 17 \pmod{100}. \end{aligned}$$

De to sidste cifre i  $3^{214} \cdot 97^{828} \cdot 13^{521}$  er derfor 17.

**Opgave 1.10.7.** Da  $\phi(10) = 4$  og  $\gcd(10, 7) = 1$ , ønsker vi at udregne eksponenten modulo 4. Vi ved at  $7^x \equiv (-1)^x \pmod{4}$  har rest 3 modulo 4 når  $x$  er ulige, dvs. at

$$\underbrace{7^{7^{7^{\cdots 7}}}}_{1000} \equiv 7^3 \equiv 3 \pmod{10}.$$

Dermed er sidste ciffer 3.

**Opgave 1.10.8.** Da  $\phi(1000) = \phi(2^3) \cdot \phi(5^3) = 2^2 \cdot 5^2 \cdot 4 = 400$  og  $\gcd(4007, 1000) = 1$ , bestemmer vi først  $4003^{4001} \pmod{400}$  så vi kan udnytte Eulers sætning til at reducere eksponenten i  $4007^{4003^{4001}} \pmod{1000}$ . Da  $\gcd(4003, 400) = 1$ ,  $\phi(400) = 160$  og  $4001 \equiv 1 \pmod{160}$ , følger det af Eulers sætning at

$$4003^{4001} \equiv 3 \pmod{400}.$$

Ved at benytte Eulers sætning igen får vi

$$4007^{4003^{4001}} \equiv 7^3 = 343 \pmod{1000}.$$

De tre sidste cifre i  $4007^{4003^{4001}}$  er altså 343.

**Opgave 1.10.9.** For at bestemme de sidste tre cifre i  $N = 2003^{2002^{2001}}$  ønsker vi at udregne  $N$  modulo 1000, dvs. at vi er interesserede i at udregne eksponenten  $2002^{2001} \pmod{\phi(1000)}$  da  $\gcd(2003, 1000) = 1$ . Lad  $r$  være resten af

$2002^{2001}$  modulo  $\phi(100) = 400$ , dvs. at  $0 \leq r < 400$  og  $r \equiv 2002^{2001} \equiv 2^{2001} \pmod{400}$ . Problemet er nu at  $\gcd(2, 400) = 2$ , dvs. de er ikke indbyrdes primiske, og vi udregner derfor i første omgang  $r$  modulo  $2^4$  og modulo  $5^2$  hver for sig. Da  $\phi(5^2) = 20$ , er

$$r \equiv 2^{2001} \equiv 2 \pmod{5^2} \text{ og } r \equiv 2^{2001} \equiv 0 \pmod{2^4}.$$

Altså er  $r = k \cdot 2^4$ , hvor  $0 \leq k < 5^2$  og  $2^4 k \equiv 2 \pmod{5^2}$ . Den inverse til 2 modulo 25 er 13, og derfor er

$$k \equiv 2 \cdot 13^4 \equiv 13^3 \equiv 22 \pmod{5^2}.$$

Derfor må  $k = 22$ , og dermed  $r = 2^4 \cdot 22$ . Altså er  $2002^{2001} \equiv 2^4 \cdot 22 = 352 \pmod{400}$ . Vi er nu klar til at udregne  $N$  modulo 1000.

$$\begin{aligned} N &\equiv 3^{2002^{2001}} \equiv 3^{352} \equiv 9^{176} = (10-1)^{176} \\ &\equiv \binom{176}{2} 10^2 - \binom{176}{1} 10 + 1 \equiv 241 \pmod{1000}. \end{aligned}$$

De tre sidste cifre i  $N$  er dermed 241.

**Opgave 1.10.10.** Lad  $m$  være et positivt heltal som hverken har 2 eller 5 som primfaktor. Da det om lidt viser sig at der er nogle særlige problemer omkring primfaktoren 3, sætter vi  $m' = 3^2 m$ . Lad yderligere  $q \in \mathbb{N}$ . Fordi  $\gcd(m', 10) = 1$ , ved vi fra Eulers sætning at

$$10^{q \cdot \phi(m')} = (10^{\phi(m')})^q \equiv 1 \pmod{m'}.$$

Dermed går  $m'$  op i

$$10^{q \cdot \phi(m')} - 1 = 3^2 \cdot \underbrace{1111111 \dots 111}_{q \cdot \phi(m')}.$$

Da  $m' = 3^2 m$ , går  $m$  op i

$$n_q = \underbrace{1111111 \dots 111}_{q \cdot \phi(m')}$$

for alle  $q \in \mathbb{N}$ . Der findes altså uendeligt mange tal  $n_q$  med den ønskede egenskab.

**Opgave 1.10.11.** Hvis  $p$  ikke er et primtal, er vi færdige. Antag derfor at  $p$  er et primtal. Vi skal nu vise at  $q$  ikke er et primtal for at vise at mindst et af tallene  $p$  og  $q$  ikke er primtal.

Af  $p = n + k^n$  fås  $n = p - k^n$  og  $k^n - 1 = p - n - 1$ , og samlet at

$$q = n k^{k^n - 1} + 1 = (p - k^n) k^{p - n - 1} + 1.$$

Fordi  $k$  er primisk med  $p$ , ved vi ifølge Fermats lille sætning at

$$q = (p - k^n) k^{p - n - 1} + 1 \equiv -k^{p-1} + 1 \equiv -1 + 1 \equiv 0 \pmod{p}.$$

Da  $k, n \geq 2$ , kan man nemt vise ved induktion efter  $n$  at  $k^n - 1 > n$ . Altså er  $q = n k^{k^n - 1} + 1 > n + k^{k^n - 1} > n + k^n = p$ . Heraf følger at  $q$  ikke er et primtal.

**Opgave 1.11.1.** Da  $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5, 2^6 \equiv 1 \pmod{9}$  er  $\text{ord}_9(2) = 6$ .

Da  $3^1 \equiv 3, 3^2 \equiv 1 \pmod{8}$  er  $\text{ord}_8(3) = 2$ .

Da  $7^1 \equiv 7, 7^2 \equiv 9, 7^3 \equiv 3, 7^4 \equiv 1 \pmod{10}$ , er  $\text{ord}_{10}(7) = 4$ .

**Opgave 1.11.2.** Lad  $m = \text{ord}_n(a)$ . Et positivt helt tal  $k$  kan skrives som  $q \cdot m + r$ , hvor  $0 \leq r < m$ . Dermed er

$$a^k = a^{q \cdot m + r} = (a^m)^q \cdot a^r \equiv a^r \pmod{n}.$$

Bemærk at  $a^r \equiv 1 \pmod{n}$  hvis og kun hvis  $r = 0$ , da  $0 \leq r < m$ , og  $m$  er det mindste positive hele tal så  $a^m \equiv 1 \pmod{n}$ . Altså er  $a^k \equiv 1 \pmod{n}$  hvis og kun hvis  $r = 0$ , dvs. hvis og kun hvis ordenen  $m$  er divisor i  $k$ .

Ifølge Eulers sætning er  $a^{\phi(n)} \equiv 1 \pmod{n}$ , og dermed er ordenen  $m$  divisor i  $\phi(n)$ .

**Opgave 1.11.3.** Hvis  $a^m \equiv 1 \pmod{n}$  og  $a^k \equiv 1 \pmod{n}$ , så ved vi fra sætning 1.11.1 at  $\text{ord}_n(a)$  går op i både  $m$  og  $k$  og dermed i  $\gcd(m, k)$ , Altså er

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



**Opgave 1.11.4.** Da  $q$  går op i  $2^p - 1$ , er  $2^p \equiv 1 \pmod{q}$ . Ifølge sætning 1.11.1 er  $\text{ord}_q(2)$  divisor i  $p$ , og da  $p$  er et primtal, må  $\text{ord}_q(2) = p$ . Af Fermats lille sætning følger at  $2^{q-1} \equiv 1 \pmod{q}$ , og dermed at  $p$  går op i  $q-1$ . Da  $q-1$  er lige, må  $q-1 = 2pk$  for et positivt heltal  $k$ , dvs. at  $q = 2pk + 1$ .

**Opgave 1.11.5.** Lad  $p$  være en ulige primfaktor i  $a^{2^n} + 1$ . Da  $p > 2$ , er

$$a^{2^n} \equiv -1 \not\equiv 1 \pmod{p} \text{ og } a^{2^{n+1}} = (a^{2^n})^2 \equiv 1 \pmod{p}.$$

Dette viser at ordenen  $d$  af  $a$  modulo  $p$  er divisor i  $2^{n+1}$ , men ikke i  $2^n$ , og dermed at  $d = 2^{n+1}$ . Altså må  $2^{n+1}$  gå op i  $\phi(p) = p-1$ .

**Opgave 1.11.6.** Antag at der findes et helt tal  $n$  større end 1 så  $2^n - 1$  er delelig med  $n$ , og lad  $p$  være den mindste primfaktor i  $n$ . Bemærk at  $p$  er ulige da  $p$  også er divisor i  $2^n - 1$ . Lad desuden  $d = \text{ord}_p(2)$ . Nu ved vi at  $d > 1$  og yderligere at  $d$  er divisor i  $\phi(p) = p-1$  og dermed mindre end  $p$ . Men da  $2^n \equiv 1 \pmod{p}$ , går  $d$  også op i  $n$  i modstrid med at  $p$  var den mindste primfaktor i  $n$ .

**Opgave 1.11.7.** Lad  $d$  være ordenen af  $q$  modulo  $p$ . Fordi  $p \mid q^r + 1$  og  $p > 2$ , må

$$q^r \equiv -1 \not\equiv 1 \pmod{p} \text{ og } q^{2r} \equiv (-1)^2 \equiv 1 \pmod{p}.$$

Dette viser at  $d$  er divisor i  $2r$ , men ikke i  $r$ , og da  $r$  er et primtal, må  $d = 2$  eller  $d = 2r$ .

Hvis  $d = 2r$ , da vil  $2r$  gå op i  $\phi(p) = p-1$ . Hvis  $d = 2$ , er  $q^2 \equiv 1 \pmod{p}$ , dvs. at  $p$  går op i  $q^2 - 1$ . Altså gælder enten at  $2r \mid p-1$  eller at  $p \mid q^2 - 1$ .

**Opgave 1.11.8.** Bemærk først at hverken 2 eller 5 går op i  $(5^p - 2^p)(5^q - 2^q)$ . Dermed er  $p$  og  $q$  forskellige fra 2 og 5. Ifølge Fermats lille sætning er  $5^p \equiv 5 \pmod{p}$ , og  $2^p \equiv 2 \pmod{p}$ . Altså er  $5^p - 2^p \equiv 5 - 2 = 3 \pmod{p}$ . Tilsvarende er  $5^q - 2^q \equiv 3 \pmod{q}$ . Dermed har vi at hvis  $p \mid 5^p - 2^p$ , er  $p = 3$ , og hvis  $q \mid 5^q - 2^q$ , er  $q = 3$ . En mulig løsning er  $p = 3$ , og  $q = 3$ .

Antag nu at  $p = 3$ , mens  $q \neq 3$ . Da vil  $q \mid 5^3 - 2^3 = 125 - 8 = 117 = 3^2 \cdot 13$ , dvs.  $q = 13$ . Tilsvarende får vi hvis  $q = 3$  og  $p \neq 3$ , at  $p = 13$ .

Antag til slut at hverken  $p$  eller  $q$  er 3. Da må  $p \mid 5^q - 2^q$  og  $q \mid 5^p - 2^p$ . Antag uden tab af generalitet at  $p \geq q$  så  $\text{gcd}(p, q-1) = 1$ . Da  $5^p \equiv 2^p \pmod{q}$ ,

er  $(5 \cdot 2^{-1})^p \equiv 1 \pmod{q}$ . Dermed er ordenen af  $5 \cdot 2^{-1}$  modulo  $q$  divisor i  $\text{gcd}(p, q-1) = 1$ , dvs. ordenen er 1. Men dette betyder at  $5 \cdot 2^{-1} \equiv 1 \pmod{q}$ , og dermed  $5 \equiv 5 \cdot 2^{-1} \cdot 2 \equiv 2 \pmod{q}$ , hvilket betyder at  $q = 3$  i modstrid med antagelsen. Altså er der ingen løsninger i dette tilfælde.

Samtligte løsninger  $(p, q)$  er  $(3, 3)$ ,  $(3, 13)$ ,  $(13, 3)$ .

**Opgave 1.11.9.** Lad  $f_n = 2^{2^n} + 1$ , og antag at  $f_n$  går op i  $3^{(f_n-1)/2} + 1 = 3^{2^{2^n-1}} + 1$ . Da er  $3^{2^{2^n-1}} \equiv -1 \pmod{k}$ , mens

$$3^{2^{2^n}} = (3^{2^{2^n-1}})^2 \equiv (-1)^2 \equiv 1 \pmod{f_n}.$$

Altså er  $\text{ord}_{f_n}(3)$  divisor i  $2^{2^n}$ , men ikke i  $2^{2^n-1}$ . Dette viser at  $\text{ord}_{f_n}(3) = 2^{2^n} = f_n - 1$ . Vi ved desuden ifølge Eulers sætning at  $\text{ord}_{f_n}(3) = f_n - 1$  skal gå op i  $\phi(f_n)$ , og dermed specielt at  $\text{ord}_{f_n}(3) \leq \phi(f_n)$ . Men hvis  $f_n$  ikke er et primtal, så er  $\phi(f_n) < f_n - 1$ . Altså må  $f_n$  være et primtal.

**Opgave 1.11.10.** Ved at indsætte ses at de eneste løsninger for  $x = 1$  er  $(1, p)$ , hvor  $p$  er et primtal, og at eneste løsning for  $x = 2$  eller  $p < 3$  er  $(2, 2)$ .

Antag nu at  $x, p \geq 3$ , og at  $x^{p-1}$  går op i  $(p-1)^x + 1$ . Da  $p$  er ulige, er  $(p-1)^x + 1$  ulige, og dermed er  $x$  også ulige. Lad  $q$  være den mindste primfaktor i  $x$ . Da er  $q$  også ulige, og  $\text{gcd}(x, q-1) = 1$ .

Da  $q$  går op i  $(p-1)^x + 1$ , må

$$(p-1)^x \equiv -1 \pmod{q} \text{ og } (p-1)^{2x} \equiv 1 \pmod{q}.$$

Lad  $d = \text{ord}_q(p-1)$ . Ovenstående viser at  $d > 1$ , og at  $d$  går op i  $\text{gcd}(2x, q-1) = 2$ , og altså  $d = 2$ . Nu er

$$p-1 \not\equiv 1 \pmod{q} \text{ og } (p-1)^2 \equiv 1 \pmod{q}.$$

Da  $q$  er et primtal, viser dette ifølge sætning 1.5.3 at  $p-1 \equiv -1 \pmod{q}$ , og altså at  $p = q$ . Vi ved nu at  $p \mid x$ ,  $x$  er ulige og  $x \leq 2p$ . Dermed er  $x = p$ , når  $x, p \geq 3$ .

Ifølge antagelsen går  $x^{p-1}$  op i  $(p-1)^x + 1$ , og derfor må

$$p^{p-1} \mid (p-1)^p + 1 = p^2 \cdot \left( p^{p-2} - \binom{p}{1} p^{p-3} + \dots - \binom{p}{p-2} + 1 \right).$$

Parentesen på højresiden er ikke delelig med  $p$  da alle led på nær det sidste er delelige med  $p$ , og derfor må  $p^{p-1} \mid p^2$  og dermed  $p \leq 3$ . Det er nemt at tjekke at  $(3, 3)$  er en løsning.

Samtlige løsninger er derfor  $(1, p)$ ,  $(2, 2)$  og  $(3, 3)$ , hvor  $p$  er et vilkårligt primtal.

**Opgave 1.12.1.** Følgen er selvfølgelig ikke periodisk, men regner vi modulo 4, er følgen periodisk fra et vist trin. Her får vi  $1, 1, 2, 3, 3, 2, 3, 3, 2, 3, 3, \dots$ , dvs. at følgen er periodisk fra  $n = 3$  med perioden  $2, 3, 3$ . Da 2 og 3 ikke er kvadratiske rester modulo 4, er  $a_n$  ikke et kvadrattal for noget  $n > 2$ .

**Opgave 1.12.2.** Lad  $k$  være et fast helt tal, og lad  $a_n$  betegne resten ved division af  $F_n$  med  $k$ . Da der kun er  $k^2$  par af restklasser modulo  $k$ , må der findes to ens par  $(a_i, a_{i+1})$  og  $(a_j, a_{j+1})$ ,  $0 \leq i < j$ . Det er klart ud fra definitionen af Fibonaccitalene at følgen  $a_0, a_1, a_2, \dots$  dermed er periodisk fra et vist trin. Da  $a_{n-1}$  kan bestemmes ud fra  $a_n$  og  $a_{n+1}$  ( $a_{n-1} \equiv a_{n+1} - a_n \pmod{k}$ ), er følgen desuden periodisk fra starten. Lad  $m$  være længden af perioden. Da har  $a_0 = 0$  og  $a_m$  samme rest modulo  $k$ , dvs. at  $F_m$  er delelig med  $k$ .

**Opgave 1.12.3.** Bemærk først at hvis  $a_n$  er et kvadrattal, har  $a_n$  rest 0 eller 1 modulo 4.

Hvis  $a_0$  har rest 2 eller 3 modulo 4, da har alle de resterende elementer i følgen skiftevis rest 2 og rest 3, og følgen indeholder derfor ingen kvadrattal. Hvis  $a_0$  har rest 0 modulo 4, da har alle de resterende elementer i følgen skiftevis rest 2 og rest 3, og følgen kan derfor højst have  $a_0$  som kvadrattal. Hvis  $a_0$  har rest 1 modulo 4, da har  $a_1$  rest 0, og derefter har alle de resterende elementer rest 2 eller rest 3. Dette viser at det højst er de to første led i følgen der kan være kvadrattal.

Antag at følgen indeholder to kvadrattal  $a_0$  og  $a_1$ . Da er  $a_0 = s^2$ , hvor  $s$  er ulige, og  $a_1 = s^{10} + 487 = t^2$ . Lad  $t = s^5 + r$ . Da er  $t^2 = (s^5 + r)^2 = s^{10} + 2s^5r + r^2$ , og dermed  $2s^5r + r^2 = 487$ . Hvis  $s = 1$ , er  $r(2 + r) = 487$  hvilket er umuligt. Hvis  $s = 3$ , er  $486r + r^2 = 487$ , og dermed  $r = 1$ . Hvis  $s > 3$ , har ligningen ingen løsninger. Dermed er  $m = a_0 = 9$  den værdi af  $m$  for hvilken følgen indeholder flest kvadrattal.

**Opgave 1.12.4.** Lad  $A_n = \{a_1, a_2, \dots, a_n\}$ . Mængden  $A_n$  består af  $n$  forskellige tal da de har forskellige rester modulo  $n$ . Bemærk desuden at hvis  $a_i, a_j \in A_n$ , da må  $k = |a_i - a_j| < n$ , for ellers vil  $a_i, a_j \in A_k$  og  $a_i \equiv a_j \pmod{k}$ .

Vi har nu at forskellen mellem det største og det mindste tal i  $A_n$  er mindre end  $n$ , og derfor må  $A_n$  indeholde  $n$  på hinanden følgende tal. Da følgen indeholder uendeligt mange både positive og negative tal, må alle hele tal forekomme mindst en gang. Samlet giver dette at alle heltal netop optræder en gang i følgen.

Et eksempel på en mulig følge:  $0, -1, 1, -2, 2, \dots$

**Opgave 1.12.5.** Vi betragter i stedet følgen  $y_n = 2x_n - 1$ . Da er

$$y_n = 2(2x_{n-1}x_{n-2} - x_{n-1} - x_{n-2} + 1) - 1 = 4x_{n-1}x_{n-2} - 2x_{n-1} - 2x_{n-2} + 1 \\ = (2x_{n-1} - 1)(2x_{n-2} - 1) = y_{n-1}y_{n-2} \text{ når } n > 1.$$

Bemærk at  $y_1 = 3$ ,  $y_2 = 3y_0$  og  $y_3 = y_1y_2 = 3^2y_0$ . Ved induktion ses let at  $y_{3n} = 3^{2s}y_0^t$ , hvor  $s$  og  $t$  er positive heltal. Dermed er  $y_{3n}$  et kvadrattal for alle  $n \geq 1$  præcis når  $y_0$  er et kvadrattal. Da  $y_0 = 2a - 1$ , fås det ønskede resultat netop når  $a = \frac{(2m-1)^2+1}{2}$ ,  $m = 1, 2, 3, \dots$

**Opgave 1.12.6.** Vi betragter i stedet følgen  $y_n = x_n - 1$ . Da er

$$y_n = x_n - 1 = 2(y_{n-1} + 1) - 4(y_{n-2} + 1) + 3 - 1 = 2y_{n-1} - 4y_{n-2}$$

for alle  $n > 2$ . Dette kan vi anvende endnu engang og få

$$y_n = 2(2y_{n-2} - 4y_{n-3}) - 4y_{n-2} = -8y_{n-3}.$$

Nu kan vi finde  $x_{2011} - 1$ :

$$x_{2011} - 1 = y_{2011} = -8y_{2008} = \dots = (-8)^{670}y_1 = 2^{2011}.$$

Altså er  $k = 2011$ .

**Opgave 1.12.7.** Antag at følgen er periodisk fra et vist trin. Betragt det største hele tal  $m$  så  $2^m$  går op i alle elementer i følgen. Sæt  $b_k = \frac{a_k}{2^m}$ . Følgen  $b_1, b_2, \dots$  opfylder samme rekursionsformel som  $a_1, a_2, \dots$  da 2015 er ulige, og vi ved at følgen indeholder mindst ét ulige tal. Betragt nu følgen  $b_1, b_2, \dots$  modulo 2. Da 2015 er ulige, må  $b_{k+1} \equiv b_k + b_{k-1} \pmod{2}$ . Da vi yderligere ved at der findes mindst ét ulige element i følgen, må den modulo 2 være  $\dots, 1, 1, 0, 1, 1, 0, 1, 1, 0, \dots$  Dette viser at periodelængden for  $b_1, b_2, \dots$  modulo 2 er 3, og dermed at periodelængden for  $a_1, a_2, \dots$  er delelig med 3.



**Opgave 1.12.8.** Bemærk først at

$$\begin{aligned} a_{2000} &\geq 2a_{1000} \geq 2^2 a_{500} \geq 2^3 a_{250} \geq 2^4 a_{125} \\ &\geq 2^5 a_{25} \geq 2^6 a_5 \geq 2^7 a_1 \geq 2^7 = 128. \end{aligned}$$

Betragt følgen  $a_1 = 1$  og  $a_n = 2^{\alpha_1 + \alpha_2 + \dots + \alpha_k}$  for  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ . Denne følge opfylder den ønskede betingelse, og da  $2000 = 2^4 \cdot 5^3$ , er  $a_{2000} = 128$ . Dermed er 128 den mindst mulige værdi af  $a_{2000}$ .

**Opgave 1.13.1.** Samtlige løsninger er  $x = 63 + k \cdot 114$ ,  $k \in \mathbb{Z}$ .

**Opgave 1.13.2.** Først vælger vi  $n$  forskellige primtal  $p_1, p_2, \dots, p_n$ . Ifølge den kinesiske restklassesætning har følgende kongruenssystem en løsning:

$$\begin{aligned} x+1 &\equiv 0 \pmod{p_1^1} \\ x+2 &\equiv 0 \pmod{p_2^2} \\ &\vdots \\ x+n &\equiv 0 \pmod{p_n^n}. \end{aligned}$$

Hvis  $x$  er en løsning, da er  $x+1, x+2, \dots, x+n$  på hinanden følgende hele tal så tal nummer  $i$  er delelig med en  $i$ 'te potens af et helt tal større end 1.

**Opgave 1.13.3.** Vælg  $nm$  forskellige primtal  $p_{11}, \dots, p_{1m}, p_{21}, \dots, p_{2m}, \dots, p_{nm}$ . Sæt  $q_j = p_{j1} p_{j2} \dots p_{jm}$  for  $j = 1, 2, \dots, n$ . Da er  $q_1, q_2, \dots, q_n$  indbyrdes primiske. Den kinesiske restklassesætning giver da at der findes et positivt heltal  $x$  som er løsning til kongruenssystemet

$$x+1 \equiv 0 \pmod{q_1}, \quad x+2 \equiv 0 \pmod{q_2}, \quad \dots, \quad x+n \equiv 0 \pmod{q_n}.$$

De  $n$  på hinanden følgende tal  $x+1, x+2, \dots, x+n$  er nu delelige med mindst  $m$  forskellige primtal hver.

**Opgave 1.13.4.** Vi viser at følgen eksisterer ved at vise hvordan man konstruerer det næste element ud fra de foregående. Vælg først  $a_1$  fuldstændigt frit.

Antag nu at  $a_1, a_2, \dots, a_m$  opfylder at summen af vilkårlige  $n$  på hinanden følgende elementer er delelig med  $n^2$  for alle  $n \leq m$ . Vi ønsker at konstruere  $a_{m+1}$ , så  $a_1 + a_2 + \dots + a_m + a_{m+1}$  er delelig med  $n^2$ , dvs. så

$$a_{m+1} \equiv -(a_{m-n+2} + \dots + a_m) \pmod{n^2} \quad \dagger$$

for alle  $n \leq m+1$ .

Lad  $p_1, \dots, p_k$  være samtlige primtal mindre end eller lig med  $m+1$ , og lad  $\alpha_i$  være det største hele tal så  $p_i^{\alpha_i} \leq m+1$ . Lad yderligere  $a_{m+1}$  være en løsning til følgende kongruenssystem:

$$\begin{aligned} x &\equiv -(a_{m-p_1^{\alpha_1+2}} + \dots + a_m) \pmod{p_1^{2\alpha_1}} \\ &\vdots \\ x &\equiv -(a_{m-p_k^{\alpha_k+2}} + \dots + a_m) \pmod{p_k^{2\alpha_k}}. \end{aligned}$$

Vi ønsker nu at vise at  $a_{m+1}$  opfylder  $\dagger$  for alle  $n \leq m+1$  da det giver det ønskede.

Først viser vi at  $a_{m+1}$  opfylder  $\dagger$  for alle  $n = p_i^{\beta_i}$ ,  $i = 1, 2, \dots, k$  og  $\beta_i = 1, \dots, \alpha_i - 1$ . Vi ved at summen af

$$a_{m-p_i^{\alpha_i+2}}, \dots, a_{m+1}$$

er delelig med  $p_i^{2\alpha_i}$  og dermed også med  $p_i^{2\beta_i}$ . Hvis vi grupperer elementerne i  $p_i^{\alpha_i - \beta_i}$  grupper med  $p_i^{\beta_i}$  på hinanden følgende elementer i hver, ved vi om samtlige grupper på nær den sidste, at summen af elementerne i gruppen er delelig med  $p_i^{2\beta_i}$  pga. konstruktionen af  $a_1, a_2, \dots, a_m$ . Men da summen af samtlige elementer i alle grupperne er delelig med  $p_i^{2\beta_i}$ , må summen af elementerne i den sidste gruppe også være det. Vi har hermed vist at  $\dagger$  er opfyldt for alle  $n = p_i^{\beta_i}$ ,  $i = 1, 2, \dots, k$  og  $\beta_i = 1, \dots, \alpha_i - 1$ . Per konstruktion af  $a_{m+1}$  ved vi desuden at  $\dagger$  er opfyldt for alle  $n = p_i^{\alpha_i}$ ,  $i = 1, 2, \dots, k$ .

Nu ønsker vi at vise at  $\dagger$  er sand for alle  $n \leq m+1$ . Da  $n$  er et produkt af primtalspotenser  $p_i^{\beta_i}$ ,  $i = 1, 2, \dots, k$  og  $\beta_i = 1, \dots, \alpha_i$ , er det nok at vise at hvis  $\dagger$  er sand for  $n = n_1$  og  $n = n_2$  med  $n_1 n_2 \leq m+1$  og  $\gcd(n_1, n_2) = 1$ , da er  $\dagger$  også sand for  $n = n_1 n_2$ . Antag at  $\dagger$  er sand for  $n = n_1$  og  $n = n_2$  med  $n_1 n_2 \leq m+1$  og  $\gcd(n_1, n_2) = 1$ . Da summen af  $n_1$  på hinanden følgende elementer er delelig med  $n_1^2$ , må summen af  $n = n_1 n_2$  på hinanden følgende elementer også være delelig med  $n_1^2$ . Tilsvarende gælder for  $n_2$ . Da  $\gcd(n_1, n_2) = 1$  gælder altså at summen af  $n_1 n_2$  på hinanden følgende elementer er delelig med  $n^2 = n_1^2 n_2^2$  hvilket netop var hvad vi skulle vise.

**Opgave 1.14.1.** Af ligningen ses at  $2bc + ac = ba$ . Da  $a$  er ulige, må  $a \mid bc$ ,  $b \mid ac$  og  $c \mid ab$ . Dermed findes positive heltal  $u, v$  og  $w$ , så  $au = bc$ ,  $bv = ac$

og  $c w = a b$ . Af dette får vi  $a b \cdot a c = c w \cdot b v$ , dvs.  $a^2 = v w$ . Tilsvarende for  $b$  og  $c$ , så vi samlet har

$$a^2 = v w, \quad b^2 = u w, \quad c^2 = u v. \quad \dagger$$

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

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

**Opgave 1.14.2.** Sæt  $d = \gcd(x, y)$ ,  $x = d \cdot x_1$  og  $y = d \cdot y_1$ . Ved at gange igennem med  $x^2 \cdot y^2 \cdot 1997$  og dividere med  $d^2$  fås

$$1997 \cdot 13 \cdot y_1^2 + 1997 \cdot 1999 \cdot x_1^2 = x_1^2 \cdot y_1^2 \cdot d^2 \cdot z.$$

Dette viser at  $x_1^2 \mid 1997 \cdot 13$  og  $y_1^2 \mid 1997 \cdot 1999$ , og da 13, 1997 og 1999 er primtal, må  $x_1 = y_1 = 1$ . Nu er

$$z \cdot d^2 = 1997 \cdot (13 + 1999) = 1997 \cdot 2012 = 2^2 \cdot 503 \cdot 1997.$$

Dette giver mulighederne  $d = 1$  og  $d = 2$ , og altså løsningerne  $(x, y, z) = (1, 1, 2^2 \cdot 503 \cdot 1997)$  og  $(x, y, z) = (2, 2, 503 \cdot 1997)$ .

**Opgave 1.14.3.** 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 1.14.4.** Hvis  $m^n + 1$  er et kvadrattal, findes et positivt heltal  $x$  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 positive heltal  $a$  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 1.14.5.** 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 positive heltal  $a$  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 1.14.6.** Ved at tjekke  $n = 1, 2, 3, 4, 5$  indses at blandt disse opfylder kun  $n = 5$  det ønskede. Vi viser indirekte at der ikke er flere  $n$  der opfylder betingelsen.

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

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

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

$$m^2 \geq (2^{n-2} - 1)^2 = 2^{2n-4} - 2^{n-1} + 1 = 2^{n-1}(2^{n-3} - 1) + 1 > n2^{n-1} + 1 = m^2$$

da  $2^{n-3} - 1 > n$  når  $n \geq 6$ . Men dette er en modstrid.

**Opgave 1.14.7.** 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

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

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  $(4, -23)$ .

**Opgave 1.14.8.** Sæt  $m = dn + r$ ,  $0 \leq r < n$ , for et ikke-negativt heltal  $d$ . Da er

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

Da  $n > r$ , er der ingen positive heltal  $m, n > 2$  som opfylder betingelserne.

**Opgave 1.14.9.** Antag modsat at det ikke er sandt, og lad  $s'$  og  $t'$  være de to positive heltal med den mindste sum for hvilke det ikke er sandt. Bemærk at både  $s'$  og  $t'$  må være større end 1, og at  $s' \neq t'$ . Antag uden tab af generalitet at  $s' > t'$ . Nu er

$$\begin{aligned} 1 &\neq \gcd\left(\sum_{i=0}^{s'-1} (-1)^i x^i, \sum_{i=0}^{t'-1} (-1)^i x^i\right) \\ &= \gcd\left(\sum_{i=0}^{s'-1} (-1)^i x^i - (-1)^{s'-t'} x^{s'-t'} \sum_{i=0}^{t'-1} (-1)^i x^i, \sum_{i=0}^{t'-1} (-1)^i x^i\right) \\ &= \gcd\left(\sum_{i=0}^{s'-t'-1} (-1)^i x^i, \sum_{i=0}^{t'-1} (-1)^i x^i\right). \end{aligned}$$

Dermed er  $t'$  og  $s' - t'$  endnu et par af indbyrdes primiske positive heltal for hvilke det ikke er sandt, nu med sum  $s'$  i modstrid med minimaliteten af  $s' + t'$ . Dette viser lemmaet.

**Opgave 1.14.10.** Først viser vi første del af sætningen:

$$\gcd(a^m + 1, a^n + 1) = \begin{cases} a^d + 1 & \text{hvis både } n' \text{ og } m' \text{ er ulige,} \\ 2 & \text{hvis enten } n' \text{ eller } m' \text{ er lige, og } a \text{ er ulige,} \\ 1 & \text{hvis enten } n' \text{ eller } m' \text{ er lige, og } a \text{ er lige.} \end{cases}$$

Antag at både  $n'$  og  $m'$  er ulige. Da er

$$a^n + 1 = (a^d + 1)((a^d)^{n'-1} - (a^d)^{n'-2} + \dots - a^d + 1),$$

$$a^m + 1 = (a^d + 1)((a^d)^{m'-1} - (a^d)^{m'-2} + \dots - a^d + 1).$$

Ifølge lemma 1.14.2 ved vi nu at

$$\gcd\left(\frac{(a^d)^{n'} + 1}{a^d + 1}, \frac{(a^d)^{m'} + 1}{a^d + 1}\right) = 1,$$

og altså at  $\gcd(a^n + 1, a^m + 1) = a^d + 1$ .

Antag nu at enten  $n'$  eller  $m'$  er lige, og lad det uden tab af generalitet være  $m'$ . Da

$$(a^d)^{n'} = a^n \equiv -1 \pmod{\gcd(a^n + 1, a^m + 1)} \text{ og}$$

$$(a^d)^{m'} = a^m \equiv -1 \pmod{\gcd(a^n + 1, a^m + 1)},$$

er

$$a^{dn'm'} = ((a^d)^{n'})^{m'} \equiv (-1)^{m'} = 1 \pmod{\gcd(a^n + 1, a^m + 1)},$$

$$a^{dn'm'} = ((a^d)^{m'})^{n'} \equiv (-1)^{n'} = -1 \pmod{\gcd(a^n + 1, a^m + 1)}.$$

Dermed er  $\gcd(a^n + 1, a^m + 1)$  lig med 1 eller 2, og det er nemt at se at  $\gcd(a^n + 1, a^m + 1) = 1$  når  $a$  er lige, og  $\gcd(a^n + 1, a^m + 1) = 2$  når  $a$  er ulige.

Nu viser vi det vi mangler af anden del af sætningen, nemlig at

$$\gcd(a^m - 1, a^n + 1) = a^d + 1 \text{ hvis } m' \text{ er lige.}$$

Antag at  $m'$  er lige, og sæt  $m' = 2^k u$ , hvor  $u$  er ulige. Da er

$$a^m - 1 = (a^{du})^{2^k} - 1 \\ = (a^{du} - 1)(a^{du} + 1)((a^{du})^2 + 1)((a^{du})^{2^2} + 1) \cdots ((a^{du})^{2^{k-1}} + 1)$$

ifølge sætning 1.7.1. Vi ved fra første del af sætning 1.14.1 at når  $j \geq 1$  er  $\gcd(a^{dn^j} + 1, a^{du^{2^j}} + 1)$  lig med 1 eller 2 afhængig af om  $a$  er lige eller ulige, og desuden at  $\gcd(a^{dn^j} + 1, a^{du} + 1) = a^d + 1$  da  $\gcd(n^j, u) = 1$  og både  $n^j$  og  $u$  er ulige. Den del af sætningen vi allerede har vist, giver at  $\gcd(a^{dn^j} + 1, a^{du} - 1) = \gcd((a^d)^{n^j} + 1, (a^d)^u - 1)$  er 1 eller 2 afhængig af om  $a$  er lige eller ulige. Da

$$a^n + 1 = (a^d + 1)((a^d)^{n'-1} - (a^d)^{n'-2} + \cdots + 1),$$

hvor sidste faktor er ulige uanset pariteten af  $a$ , kan vi samlet konkludere at  $\gcd(a^m - 1, a^n + 1) = a^d + 1$ .

**Opgave 1.14.11.** Det følger af sætning 1.14.1 at

$$\gcd(f_n, f_m) = \gcd(2^{2^n} + 1, 2^{2^m} + 1) = 1$$

når  $n \neq m$ .

**Opgave 1.14.12.** Det følger af sætning 1.14.1 at

$$\gcd(f_n, 2^{f_n} - 2) = \gcd(2^{2^n} + 1, 2^{2^{2^n} + 1} - 2) = \gcd(2^{2^n} + 1, 2^{2^{2^n}} - 1) = 2^{2^n} + 1 = f_n.$$

**Opgave 1.15.1.** Sæt  $v_p(a) = k$  og  $v_p(b) = m$ , og antag uden tab af generalitet at  $k \geq m$ . Dermed er  $a = p^k u$  og  $b = p^m v$ , hvor  $u$  og  $v$  er hele tal som er primiske med  $p$ . Da  $u$  og  $v$  er primiske med  $p$ , ved vi også at  $\gcd(u, v)$  og  $\text{lcm}(u, v)$  er primiske med  $p$ .

1) Da  $ab = p^{k+m} uv$ , er  $v_p(ab) = k + m = v_p(a) + v_p(b)$ .

2) Da

$$\gcd(a, b) = \gcd(p^k u, p^m v) = p^m \cdot \gcd(u, v)$$

fordi  $k \geq m$ , er

$$v_p(\gcd(a, b)) = m = \min(v_p(a), v_p(b)).$$

3) Da

$$\text{lcm}(a, b) = \text{lcm}(p^k u, p^m v) = p^k \cdot \text{lcm}(u, v)$$

fordi  $k \geq m$ , er

$$v_p(\text{lcm}(a, b)) = k = \max(v_p(a), v_p(b)).$$

4) Da  $a + b = p^m(u + p^{k-m}v)$ , er

$$v_p(a + b) \geq m = \min(v_p(a), v_p(b)).$$

5) Hvis  $v_p(a) > v_p(b)$ , dvs.  $k > m$ , er  $a + b = p^m(u + p^{k-m}v)$ , hvor  $u + p^{k-m}v$  ikke er delelig med  $p$ , og dermed er  $v_p(a + b) = m = v_p(b)$ .

**Opgave 1.15.2.** Antag for modstrid at  $b$  ikke er en  $n$ 'te potens af et heltal. Da findes en primdivisor  $p$  i  $b$  så  $n$  ikke går op i  $v_p(b)$ . Dermed ved vi at  $v_p(b) \neq v_p(a_k^n)$  for ethvert  $a_k$ , og ifølge sætning 1.15.1, 5), betyder det at

$$v_p(b - a_k^n) = \min(v_p(b), v_p(a_k^n)) \leq v_p(b).$$

Hvis vi vælger et  $k$  med  $v_p(k) > v_p(b)$ , betyder det at  $k$  ikke går op i  $b - a_k^n$ , hvilket er en modstrid. Dermed må  $b = A^n$  for et helt tal  $A$ .

**Opgave 1.15.3.** Vi skal bestemme alle  $n$  hvor  $v_2(n!) \geq n - 1$ . Ifølge sætning 1.15.2 er det netop de  $n$  hvor

$$n - 1 \leq v_2(n!) = n - s_2(n),$$

dvs. alle  $n$  hvor  $1 \geq s_2(n)$ . Dette er tilfældet netop når  $n$  er en potens af 2, dvs.  $2^{n-1}$  går op i  $n!$  netop når  $n$  er en potens af 2.

**Opgave 1.15.4.** Først viser vi 2). Lad  $p$  være et primtal, og lad  $a$  og  $b$  være to hele tal som er primiske med  $p$ . Antag yderligere at  $p \mid a + b$ , og at  $n$  er ulige. Ifølge LTE (sætning 1.15.3), 1), er

$$v_p(a^n + b^n) = v_p(a^n - (-b)^n) = v_p(a - (-b)) + v_p(n) = v_p(a + b) + v_p(n).$$

Nu viser vi 3). Antag at  $a$  og  $b$  er ulige, og at  $n$  er ulige. Fra sætning 1.15.1 ved vi at

$$v_2(a^n - b^n) = v_2(a - b) + v_2(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}) = v_2(a - b)$$



da  $a^{n-1} + a^{n-2}b + \dots + b^{n-1}$  er ulige fordi  $a$ ,  $b$  og  $n$  er ulige.

Nu viser vi 4) ved induktion efter  $v_2(n)$ . Antag først at  $v_2(n) = 1$ , dvs. at  $n = 2n'$ , hvor  $n'$  er ulige. Ved at benytte LTE (sætning 1.15.3), 3), fås

$$\begin{aligned} v_2(a^n - b^n) &= v_2((a^2)^{n'} - (b^2)^{n'}) = v_2(a^2 - b^2) \\ &= v_2(a - b) + v_2(a + b) = v_2(a - b) + v_2(a + b) + v_2(n) - 1. \end{aligned}$$

Antag nu at 4) er sand for positive hele tal  $n$  med  $v_2(n) = N$  for et positivt heltal  $N$ . Betragt  $n$  hvor  $v_2(n) = N + 1$ , og sæt  $n = 2^{N+1}n'$ . Nu er

$$\begin{aligned} v_2(a^n - b^n) &= v_2((a^2)^{2^N n'} - (b^2)^{2^N n'}) \\ &= v_2(a^2 - b^2) + v_2(a^2 + b^2) + v_2(2^N n') - 1 \\ &= v_2(a - b) + v_2(a + b) + 1 + N - 1 \\ &= v_2(a - b) + v_2(a + b) + v_2(n) - 1, \end{aligned}$$

da  $a^2 + b^2$  er delelig med 2, men ikke med 4. Hermed er induktionen fuldført.

**Opgave 1.15.5.** Ved at sætte  $a = -1$  ses at  $n$  må være lige. Lad  $n = 2m$  for et helt tal  $m$ . Ifølge LTE (sætning 1.15.3), 3), har vi

$$v_2(a^n - 1) = v_2(a - 1) + v_2(a + 1) + v_2(n) - 1 = v_2(a^2 - 1) + v_2(m),$$

dvs. vi skal bestemme alle positive heltal  $n$  så  $v_2(a^2 - 1) + v_2(m) \geq 2017$  for alle ulige tal  $a$ . Når  $a = 3$ , må  $v_2(m) \geq 2014$ , og det er også en tilstrækkelig betingelse da  $v_2(a^2 - 1) = v_2(a - 1) + v_2(a + 1) \geq 3$ . Dermed er svaret alle positive  $n$  med  $v_2(n) \geq 2015$ , dvs. alle tal på formen  $n = 2^{2015} \cdot n'$ , hvor  $n'$  er et positivt heltal.

**Opgave 1.15.6.** Antag at  $p$  er et primtal,  $p > 2025$ , og at  $v_p(a + b) = 1$  og  $v_p(a^{2025} + b^{2025}) > 1$ . Først ser vi på tilfældet hvor  $a$  og  $b$  er primiske med  $p$ . Ifølge LTE (sætning 1.15.3), 2), er

$$v_p(a^{2025} + b^{2025}) = v_p(a + b) + v_p(2025) = 1,$$

hvilket er umuligt. Altså må  $p$  gå op i enten  $a$  eller  $b$ , og dermed i dem begge, dvs.  $v_p(a^{2025} + b^{2025}) \geq 2025$ .

**Opgave 1.15.7.** Tallet  $n$  må være ordenen af 2025 modulo  $2^{1000}$ . Da  $\gcd(2025, 2^{1000}) = 1$ , findes ordenen af 2025 modulo  $2^{1000}$ , og den er divisor i  $\phi(2^{1000}) = 2^{999}$ . Altså er  $n$  en potens af 2. Sæt  $n = 2^m$ . Ifølge LTE (sætning 1.15.3), 4), er

$$\begin{aligned} v_2(2025^{2^m} - 1) &= v_2(2025^{2^m} - 1^{2^m}) = v_2(2025 - 1) + v_2(2025 + 1) + v_2(2^m) - 1 \\ &= v_2(2024) + v_2(2026) + m - 1 = v_2(2^3 \cdot 253) + 1 + m - 1 = 3 + m. \end{aligned}$$

Det mindste positive heltal  $n$  så  $2^{1000}$  går op i  $2025^n - 1$  er altså  $n = 2^{997}$ .

**Opgave 1.15.8.** Det er oplagt at  $n = 1$  er en løsning. Antag derfor at  $n > 1$ , og at  $n^2$  går op i  $2^n + 1$ . Lad  $p$  være den mindste primdivisor i  $n$ , og bemærk at  $p$  er ulige da  $p$  går op i  $2^n + 1$ . Vi ved at  $2^n \equiv -1 \pmod{p}$ , hvilket viser at  $2^{2n} \equiv 1 \pmod{p}$ , og altså at  $\text{ord}_p(2)$  er divisor i  $\gcd(2n, p - 1)$ . Fordi  $p$  er mindste primdivisor i  $n$ , må  $\gcd(n, p - 1) = 1$ , dvs.  $\text{ord}_p(2) \leq 2$ . Dermed er  $2^2 \equiv 1 \pmod{p}$ , og vi kan slutte at  $p = 3$ . Sæt  $v_3(n) = k$ . Af LTE (sætning 1.15.3), 2), fås

$$v_3(2^n + 1) = v_3(2 + 1) + v_3(n) = 1 + k.$$

Da  $n^2$  går op i  $2^n + 1$ , er  $2k = v_3(n^2) \leq 1 + k$ , dvs.  $k = 1$ . Ved indsættelse ses at  $n = 3$  er en løsning. Sæt nu  $n = 3n'$ , hvor  $n'$  er et helt tal større end 1 som er primisk med 3. Lad  $q$  være mindste primdivisor i  $n'$ . Vi ved at  $q > 3$ , og at  $2^{3n'} \equiv -1 \pmod{q}$ , dvs. specielt at  $8^{2n'} \equiv 1 \pmod{q}$ . Det betyder at  $\text{ord}_q(8)$  er divisor i  $\gcd(2n', q - 1)$ , og da  $q$  er mindste primdivisor i  $n'$ , må  $\text{ord}_q(8) \leq 2$ . Altså ved vi at  $q$  går op i  $8^2 - 1 = 63$ , dvs.  $q = 7$ . Men  $2^n + 1 = (2^3)^{n'} + 1 \equiv 2 \pmod{7}$ , hvilket er en modstrid. Dermed er  $n = 1$  og  $n = 3$  de eneste løsninger.

**Opgave 1.15.9.** I stedet for kun at vise at der findes et positivt heltal  $n$  med præcis  $N = 2000$  forskellige primdivisorer, så  $n$  går op i  $n^2 + 1$ , viser vi følgende mere generelle udsagn, som også dækker  $N = 2000$ : For ethvert positivt heltal  $N$  findes et positivt ulige tal  $n$  med præcis  $N$  forskellige primdivisorer som opfylder at  $n$  går op i  $2^n + 1$ . Dette viser vi ved induktion efter  $N$ .

For  $N = 1$  har  $n = 3$  den ønskede egenskab. Lad nu  $n$  være et positivt ulige tal med præcis  $N$  forskellige primdivisorer som opfylder at  $n$  går op i  $2^n + 1$ . Lad yderligere  $p$  være en fast primfaktor i  $2^n + 1$ . For ethvert positivt heltal  $k$  gælder ifølge LTE (sætning 1.15.3), 2), at  $v_p(2^{np^k} + 1) = v_p(2^n + 1) + k$ , og for

enhver primfaktor  $q$  i  $2^n + 1$ ,  $q \neq p$ , følger det af LTE (sætning 1.15.3), 2), at  $v_q(2^{np^k} + 1) = v_q(2^n + 1)$ . Dermed må  $2^{np^k} + 1 = p^k(2^n + 1)u$  hvor  $u$  er primisk med  $2^n + 1$ . Hvis vi vælger  $k$  tilstrækkelig stor, må  $u > 1$ , hvilket betyder at  $2^{np^k} + 1$  har en primfaktor  $p_0$  som ikke går op i  $2^n + 1$  og dermed heller ikke i  $n$ .

Sæt  $m = p_0 n p^k$ . Nu har  $m$  i alt  $N + 1$  forskellige ulige primfaktorer. For enhver primfaktor  $q$  i  $2^n + 1$ , dvs. specielt alle primfaktorer i  $n$ , giver LTE (sætning 1.15.3), 2), at

$$v_q(2^m + 1) = v_q(2^n + 1) + v_q(p^k p_0) \geq v_q(n) + v_q(p^k p_0) = v_q(m).$$

Og for  $p_0$  giver LTE (sætning 1.15.3), 2), at

$$v_{p_0}(2^m + 1) = v_{p_0}(2^{np^k} + 1) + 1 \geq 1 = v_{p_0}(m).$$

Dermed må  $v_q(2^m + 1) \geq v_q(m)$  for enhver primdivisor  $q$  i  $m$ , dvs.  $m$  må gå op i  $2^m + 1$ . Dette afslutter induktionen.

**Opgave 1.16.1.** Antag at  $a^2 + b^2 = n$ , og lad  $n = p_1 p_2 \dots p_s$ . Da er  $a^2 + b^2 \equiv 0 \pmod{p_i}$  for alle  $i = 1, 2, \dots, s$ . Ifølge sætning 1.16.1 må  $p_i$  gå op i både  $a$  og  $b$ , dvs. at  $n$  går op i  $a$  og  $b$  hvilket er en modstrid.

**Opgave 1.16.2.** Antag at  $n^2 + 3 = m^3$ . Hvis man betragter ligningen modulo 8, ser man ved at gennemgå de mulige restklasser for  $n$  og  $m$  at  $n$  må være lige samt at  $m$  har rest 3 modulo 4. Ifølge antagelsen er

$$n^2 + 2^2 = m^3 + 1 = (m + 1)(m^2 - m + 1).$$

Desuden er  $m^2 - m + 1 \equiv 3^2 - 3 + 1 \equiv 3 \pmod{4}$ , dvs. at der findes en primfaktor  $p$  i  $m^2 - m + 1$  som har rest 3 modulo 4. Dermed er  $n^2 + 2^2 \equiv 0 \pmod{p}$ , og ifølge sætning 1.16.1 må  $p$  gå op i 2. Dette er en modstrid, og dermed er antagelsen forkert.

**Opgave 1.16.3.** Fra korollar 1.16.2 ved vi at primtal på formen  $p = 4n + 3$  ikke kan skrives som sum af to kvadrattal. Vi mangler derfor blot at vise at primtal på formen  $p = 4n + 1$  altid kan skrives som sum af to kvadrattal.

Lad  $p = 4n + 1$ . Vi ved at der findes et helt tal  $z$  så  $z^2 + 1 \equiv 0 \pmod{p}$ . Da  $\gcd(z, p) = 1$ , findes ifølge Thues sætning hele tal  $x$  og  $y$ , hvor  $0 < x < \sqrt{p}$  og  $0 < y < \sqrt{p}$ , så

$$zy \equiv x \pmod{p} \quad \text{eller} \quad zy \equiv -x \pmod{p}.$$

Da  $z^2 + 1 \equiv 0 \pmod{p}$ , må  $(yz)^2 + y^2 \equiv 0 \pmod{p}$ , og dermed

$$x^2 + y^2 \equiv 0 \pmod{p}.$$

Da  $0 < x^2 + y^2 < 2p$ , må  $x^2 + y^2 = p$ .

**Opgave 1.16.4.** Bemærk først at alle kvadrattal kan skrives som sum af to kvadrater da 0 er et kvadrattal. Hvis to tal kan skrives som sum af to kvadrattal, da kan deres produkt også ifølge opgave 1.2.6. Tallet 2, alle primtal på formen  $4m + 1$  samt alle kvadrater kan skrives som sum af to kvadrater, og dermed kan alle positive heltal, hvor primtal på formen  $4n + 3$  indgår i en lige potens i primfaktoropløsningen, også skrives som sum af to kvadrater.

Antag at  $n = a^2 + b^2$ , og at primfaktoropløsningen for  $n$  indeholder et primtal  $q$  på formen  $4n + 3$ . Da  $q$  går op i en sum af to kvadrater, vil  $q$  ifølge sætning 1.16.1 gå op i både  $a$  og  $b$ . Dermed vil  $q^2$  gå op i  $a^2 + b^2 = n$ . Vi reducerer nu  $n, a^2$  og  $b^2$  med  $q^2$  og får  $a_1^2 + b_1^2 = n_1$ . Hvis  $n_1$  er delelig med  $q$ , kan vi gentage proceduren en gang til og se at  $q^2$  vil gå op i  $n_1$ . På denne måde indses at  $q$  indgår i primfaktoropløsningen for  $n$  i en lige potens.

**Opgave 1.17.1.** Blandt tre på hinanden følgende ulige tal vil det ene være deleligt med 3, og da de alle tre skal være primtal, må det ene primtal i et sæt trillingepriamtal være 3. Dermed er der kun et sæt trillingepriamtal, og det er 3, 5 og 7.

**Opgave 1.17.2.** For  $n = 1$  er  $\binom{2n}{n} = 2$  ikke et kvadrattal. For  $n > 1$  findes ifølge Bertrands postulat et primtal  $p$  så  $n < p < 2n$ . Da

$$\binom{2n}{n} = \frac{(2n)(2n-1)(2n-2)\cdots(n+1)}{n!},$$

må  $p$  gå op netop én gang i tælleren, men ikke i nævneren. Binomialkoefficienten  $\binom{2n}{n}$  er derfor delelig med  $p$ , men ikke med  $p^2$ , hvilket viser at  $\binom{2n}{n}$  ikke kan være et kvadrattal.

**Opgave 1.17.3.** Vi viser det ved stærk induktion efter  $n$ . Det er oplagt sandt for  $n = 1, 2, 3$  da  $1 + 2 = 3$ ,  $3 + 4 = 7$  og  $5 + 6 = 11$ . Antag at  $N > 3$ , og at påstanden er sand for alle  $n < N$ . Ifølge Bertrands postulat findes et primtal  $p$ ,  $2N < p <$



$4N - 2$ , dvs.  $p = 2N + r$ , hvor  $0 < r < 2N - 2$ . Desuden må  $r$  være ulige da  $p$  er ulige. Dermed kan tallene  $r, r + 1, \dots, 2N$  parres så parrenes sum er  $p$ :

$$p = (2N) + (r) = (2N - 1) + (r + 1) = \dots = \frac{2N + r + 1}{2} + \frac{2N + r - 1}{2}.$$

Ifølge induktionsantagelsen ved vi yderligere at tallene  $1, 2, 3, \dots, r - 1$  kan parres så parrenes sum er primtal. Dette afslutter induktionen.

**Opgave 1.17.4.** Primtal på formen  $4n + 3$ : Antag at der kun findes endeligt mange primtal på formen  $4n + 3$ , og kald disse  $p_1, p_2, \dots, p_r$ , hvor  $p_1 = 3$ . Betragt tallet

$$N = 4p_2p_3p_4 \cdots p_r + 3.$$

Primtallet  $p_1 = 3$  kan ikke være divisor i  $N$  da det ikke går op i  $4p_2p_3p_4 \cdots p_r$ . Primtallene  $p_2, p_3, \dots, p_r$  kan heller ikke være divisorer i  $N$  da de går op i  $4p_2p_3p_4 \cdots p_r$ , men ikke i 3. Da  $N \equiv 3 \pmod{4}$ , kan  $N$  ikke kun have primfaktorer på formen  $4n + 1$ , og  $N$  har derfor en primfaktor på formen  $q = 4n + 3$ , men dette er en modstrid.

Primtal på formen  $6n + 5$ : Bemærk først at alle primtal på nær 2 og 3 er på formen  $6n + 1$  eller  $6n + 5$ . Antag at der kun findes endeligt mange primtal på formen  $6n + 5$ , og kald disse  $p_1, p_2, \dots, p_r$ , hvor  $p_1 = 5$ . Betragt tallet

$$N = 6p_2p_3p_4 \cdots p_r + 5.$$

Primtallet 5 kan ikke være divisor i  $N$ , da 5 ikke går op i  $6p_2p_3p_4 \cdots p_r$ . Primtallene  $p_2, p_3, \dots, p_r$  kan heller ikke være divisorer i  $N$  da de går op i  $6p_2p_3p_4 \cdots p_r$ , men ikke i 5. Da  $N \equiv 5 \pmod{6}$ , kan  $N$  ikke kun have primfaktorer på formen  $6n + 1$ , og  $N$  har derfor en primfaktor på formen  $q = 6n + 5$ , men dette er en modstrid.

Primtal på formen  $2^k n + 1$ , hvor  $k \geq 1$ : Antag at der kun findes endeligt mange primtal på formen  $2^k n + 1$ , og kald disse  $p_1, p_2, \dots, p_r$ . Betragt tallet

$$N = (2p_1p_2p_3 \cdots p_r)^{2^{k-1}} + 1,$$

og lad  $q$  være en primfaktor i  $N$ . Sæt  $x = 2p_1p_2 \cdots p_r$ . Da  $x^{2^{k-1}} \equiv -1 \pmod{q}$ , er  $x^{2^k} \equiv 1 \pmod{q}$ , og dermed må  $\text{ord}_q(x) = 2^k$ . Dette betyder at  $2^k$  går op

i  $\phi(q) = q - 1$ , og altså er  $q$  på formen  $2^k n + 1$ . Dette er i modstrid med at ingen af primtallene  $p_1, p_2, \dots, p_r$  går op i  $N$ . Altså findes der uendeligt mange primtal på formen  $2^k n + 1$ .

**Opgave 1.18.1.** Da  $i^2 \equiv (p - i)^2 \pmod{p}$  og  $1^2, 2^2, \dots, (\frac{p-1}{2})^2$  er  $\frac{p-1}{2}$  forskellige kvadratiske rester (det sidste skyldes at  $a^2 \equiv b^2 \pmod{p}$  medfører at  $p$  går op i  $(a + b)(a - b)$ ), er netop halvdelen af tallene  $1, 2, 3, \dots, p - 1$  kvadratiske rester modulo  $p$ . Dette giver det ønskede.

**Opgave 1.18.2.** Hvis  $p \equiv 3 \pmod{4}$ , er

$$\begin{aligned} 2^{\frac{p-1}{2}} \left( \frac{p-1}{2} \right)! &\equiv 2 \cdot 4 \cdot 6 \cdots (p-1) \\ &\equiv 2 \cdot 4 \cdot 6 \cdots \left( \frac{p-3}{2} \right) \cdot \left( -\frac{p-1}{2} \right) \cdots (-5) \cdot (-3) \cdot (-1) \\ &\equiv (-1)^{\frac{p+1}{4}} \left( \frac{p-1}{2} \right)! \pmod{p} \end{aligned}$$

Ifølge Eulers kriterium gælder nu at

$$\left( \frac{2}{p} \right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} \pmod{p}.$$

Dermed er  $\left( \frac{2}{p} \right) = 1$  når  $p \equiv 7 \pmod{8}$ , og  $\left( \frac{2}{p} \right) = -1$  når  $p \equiv 3 \pmod{8}$ .

**Opgave 1.18.3.** Antag at  $a$  er kvadratisk rest modulo  $b$ . Da findes et  $x$  så  $x^2 \equiv a \pmod{b}$ , og dermed også  $x^2 \equiv a \pmod{p_i^{\alpha_i}}$  for alle  $i = 1, 2, \dots, n$ . Altså er  $a$  også kvadratisk rest modulo  $p_i^{\alpha_i}$  for alle  $i = 1, 2, \dots, n$ .

Antag omvendt at  $a$  er kvadratisk rest modulo  $p_i^{\alpha_i}$  for alle  $i = 1, 2, \dots, n$ , dvs. at der findes et  $x_i$  så  $x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$  for alle  $i = 1, 2, \dots, n$ . Ifølge den kinesiske restklasser sætning findes en løsning  $x$  til kongruenssystemet

$$x \equiv x_i \pmod{p_i^{\alpha_i}}, \text{ for alle } i = 1, 2, \dots, n.$$

Dermed er  $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$  for alle  $i = 1, 2, \dots, n$ , og altså  $x^2 \equiv a \pmod{b}$ .

**Opgave 1.18.4.** Lad  $n = 2m + 1$  og  $p$  en primdivisor i  $2^n - 1$ . Da er  $2^{2m+1} \equiv 1 \pmod{p}$ , og altså  $2 \equiv ((2^{-1})^m)^2 \pmod{p}$ . Dette viser at 2 er kvadratisk rest modulo  $p$ , og altså at  $p \equiv \pm 1 \pmod{8}$  ifølge korollar 1.18.3.

**Opgave 1.18.5.** Hvis  $p$  er primdivisor i  $x^2 + 2y^2$ , er  $x^2 + 2y^2 \equiv 0 \pmod{p}$ . Da vi ved at  $x$  og  $y$  er indbyrdes primiske, må de begge være primiske med  $p$ , og dermed har  $y$  en multiplikativ invers  $y^{-1}$  modulo  $p$ . Altså er  $(y^{-1}x)^2 \equiv -2 \pmod{p}$ , hvilket viser at  $-2$  er kvadratisk rest modulo  $p$ . Ifølge korollar 1.18.2 er

$$1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right).$$

Derfor giver korollar 1.18.3 at  $p \equiv 1$  eller  $p \equiv 3 \pmod{8}$ .

**Opgave 1.18.6.** Antag at  $p$  er et primtal,  $p \equiv 3 \pmod{4}$ , samt at  $2p+1$  er divisor i  $M_p = 2^p - 1$ . Da  $2^p \equiv 1 \pmod{2p+1}$ , og  $p$  er et primtal, er  $p$  ordenen af 2 modulo  $2p+1$ . Ifølge Euler-Fermat er  $p$  da divisor i  $\phi(2p+1)$ . Vi ved yderligere at  $\phi(2p+1) \leq 2p$ , dvs.  $\phi(2p+1) = p$  eller  $\phi(2p+1) = 2p$ . Ifølge formelen for Eulers phi-funktion, er  $\phi(n)$  kun et primtal hvis både  $n$  og  $n-1$  er primtal, så vi kan udelukke  $\phi(2p+1) = p$ . Dermed må  $\phi(2p+1) = 2p$ , hvilket ifølge formelen for Eulers phi-funktion giver at  $2p+1$  er et primtal.

Antag omvendt at  $p$  er et primtal,  $p \equiv 3 \pmod{4}$  samt at  $q = 2p+1$  er et primtal. Da  $q \equiv 7 \pmod{8}$ , kan vi ifølge Eulers kriterium og korollar 1.18.3 slutte at

$$2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) = 1 \pmod{q},$$

og altså at primtallet  $q = 2p+1$  går op i  $2^{\frac{q-1}{2}} - 1 = 2^p - 1 = M_p$ .

**Opgave 1.18.7.** For Sophie Germain-primtallene  $p = 23$  og  $p = 83$  viser kriteriet fra opgave 1.18.6 at  $2p+1$  er divisor i  $M_p$ , og dermed at  $M_p$  ikke er et primtal.

**Opgave 1.18.8.** Hvis  $p \equiv \pm 1 \pmod{8}$ , da er 2 kvadratisk rest modulo  $p$  ifølge korollar 1.18.3. Dermed findes et  $x$  så  $2 \equiv x^2 \pmod{p}$  og altså  $16 = 2^4 \equiv x^8 \pmod{p}$ .

Hvis  $p \equiv 3 \pmod{8}$ , da er  $-2$  kvadratisk rest modulo  $p$  ifølge korollar 1.18.3 og korollar 1.18.2. Dermed findes et  $x$  så  $-2 \equiv x^2 \pmod{p}$  og altså  $16 = (-2)^4 \equiv x^8 \pmod{p}$ .

Hvis  $p \equiv 5 \pmod{8}$ , da er  $p = 8n+5$ . Ifølge Fermats lille sætning er  $2^{8n+4} \equiv 1 \pmod{p}$ , og dermed  $16 = 2^4 \equiv ((2^{-1})^n)^8 \pmod{p}$ , hvor  $2^{-1}$  er den multiplikative inverse til 2 modulo  $p$ .

**Opgave 1.18.9.** Antag at  $p$  er primfaktor i  $f_n = 2^{2^n} + 1$ . Da er  $2^{2^n} \equiv -1 \pmod{p}$  og  $2^{2^{n+1}} \equiv 1 \pmod{p}$ . Dette viser at ordenen af 2 modulo  $p$  er divisor i  $2^{n+1}$ , men ikke i  $2^n$ , dvs. ordenen er  $2^{n+1}$ . Dermed er  $2^{n+1}$  divisor i  $p-1$ , og altså  $p \equiv 1 \pmod{2^{n+1}}$ . Specielt er  $p \equiv 1 \pmod{8}$ , dvs. 2 er kvadratisk rest modulo  $p$ . Ifølge Eulers kriterium har vi dermed at

$$1 = \left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p}.$$

Dette viser at  $2^{n+1}$ , som er ordenen af 2 modulo  $p$ , går op i  $\frac{p-1}{2}$ , og altså at  $2^{n+2}$  går op i  $p-1$ .

**Opgave 1.18.10.** Antag at  $x$  og  $y$  er indbyrdes primiske, og at  $p$  er en primdivisor i  $N = ax^2 + bxy + cy^2$ , hvor  $p$  ikke går op i  $abc$ . Da  $x$  og  $y$  er indbyrdes primiske, går  $p$  ikke op i nogen af dem da  $p$  går op i begge to eller ingen af dem fordi  $\gcd(p, abc) = 1$ . Sæt  $D = b^2 - 4ac$ . Da er

$$0 \equiv 4aN = (2ax + by)^2 - Dy^2 \pmod{p}.$$

Da  $p$  ikke går op i  $y$ , har  $y$  en invers  $y^{-1}$  modulo  $p$ . Dermed er

$$D \equiv (y^{-1}(2ax + by))^2 \pmod{p},$$

og  $D$  er altså kvadratisk rest modulo  $p$ .

**Opgave 1.18.11.** Ifølge den kvadratiske reciprocitetssætning og korollar 1.18.2 og 1.18.3 er

$$\left(\frac{37}{2003}\right) = \left(\frac{2003}{37}\right) = \left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

$$\left(\frac{143}{2003}\right) = \left(\frac{11}{2003}\right) \left(\frac{13}{2003}\right) = -\left(\frac{2003}{11}\right) \left(\frac{2003}{13}\right) = -\left(\frac{1}{11}\right) \left(\frac{1}{13}\right) = -1.$$

Altså er hverken 37 eller 143 kvadratiske rester modulo 2003.



**Opgave 1.18.12.** Den eneste primiske kvadratiske rest modulo 3 er 1, og de primiske kvadratiske rester modulo 5 er 1 og 4. Ifølge den kvadratiske reciprocitetssætning har vi derfor at

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = \begin{cases} 1 \cdot 1 = 1 & \text{hvis } p \equiv 1 \pmod{12} \\ -1 \cdot (-1) = 1 & \text{hvis } p \equiv -1 \pmod{12} \\ 1 \cdot (-1) = -1 & \text{hvis } p \equiv 5 \pmod{12} \\ -1 \cdot 1 = -1 & \text{hvis } p \equiv -5 \pmod{12} \end{cases}$$

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & \text{hvis } p \equiv \pm 1 \pmod{5} \\ -1 & \text{hvis } p \equiv \pm 2 \pmod{5} \end{cases}$$

**Opgave 1.18.13.** Antag at  $(x, y)$  opfylder ligningen. Da er  $11x^2 \equiv 7 \pmod{151}$ , hvilket er ækvivalent med at  $(11x)^2 \equiv 7 \cdot 11 \pmod{151}$ . Nu undersøger vi om  $7 \cdot 11$  er kvadratisk rest modulo 151, som er et primtal. Ifølge den kvadratiske reciprocitetssætning og korollar 1.18.2 og 1.18.3 er

$$\left(\frac{7 \cdot 11}{151}\right) = \left(\frac{7}{151}\right) \left(\frac{11}{151}\right) = \left(\frac{151}{7}\right) \left(\frac{151}{11}\right) = \left(\frac{4}{7}\right) \left(\frac{8}{11}\right) = 1 \cdot \left(\frac{2}{11}\right) \left(\frac{4}{11}\right) = -1.$$

Da  $7 \cdot 11$  ikke er kvadratisk rest modulo 151, har vi opnået en modstrid og dermed vist at ligningen ikke har nogen løsninger.

**Opgave 1.18.14.** Antag at  $a^2 - ab + b^2 = c^2$ , og lad  $p$  være en primdivisor i  $c$ . Ifølge sætning 1.18.5 er  $D = (-1)^2 - 4 \cdot 1 \cdot 1 = -3$  dermed kvadratisk rest modulo  $p$ . Altså er

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right).$$

Ifølge korollar 1.18.3 og opgave 1.18.12 viser dette at  $p \equiv 1 \pmod{6}$ .

**Opgave 1.18.15.** Antag at  $p = 2^n + 1$ ,  $n > 1$ , er et primtal. Da  $p$  er et primtal, må  $n$  være lige, for hvis  $n$  er ulige, er  $p$  delelig med 3. Dermed er  $p = 4^m + 1 \equiv 2 \pmod{3}$  og altså ikke kvadratisk rest modulo 3. Ifølge den kvadratiske reciprocitetssætning og Eulers kriterium er

$$-1 = \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = \left(\frac{3}{p}\right) \equiv 3^{\frac{p-1}{2}} \pmod{p}.$$

Altså går  $p$  op i  $3^{\frac{p-1}{2}} + 1$ .

**Opgave 1.18.16.** Bemærk først at  $2007 = 3^2 \cdot 223$ . Lad  $k$  være et positivt heltal, og antag at der findes et heltal  $a$  så

$$k^3 + 3k^2a + 3ka^2 = (k+a)^3 - a^3 \equiv 0 \pmod{3^2 \cdot 223} \quad \dagger$$

Hvis vi regner modulo 3, ses at  $k \equiv 0 \pmod{3}$ . Sæt  $k = 3m$ . Da er  $\dagger$  ensbetydende med

$$3^2 m(3m^2 + 3ma + a^2) \equiv 0 \pmod{3^2 \cdot 223}$$

Hvis 223 går op i  $m$ , er ligningen sand for alle  $a$ . Antag derfor at 223 ikke går op i  $m$ , og lad  $m^{-1}$  være den inverse til  $m$  modulo 223. Da er  $\dagger$  ensbetydende med at

$$\begin{aligned} 3m^2 + 3ma + a^2 &\equiv 0 \pmod{223} \Leftrightarrow \\ 3 + 3am^{-1} + (am^{-1})^2 &\equiv 0 \pmod{223} \Leftrightarrow \\ 3 - 220am^{-1} + (am^{-1})^2 &\equiv 0 \pmod{223} \Leftrightarrow \\ (am^{-1} - 110)^2 - 55 &\equiv 0 \pmod{223} \end{aligned}$$

Ifølge den kvadratiske reciprocitetssætning er

$$\begin{aligned} \left(\frac{55}{223}\right) &= \left(\frac{5}{223}\right) \left(\frac{11}{223}\right) = \left(\frac{223}{5}\right) \left(-\left(\frac{223}{11}\right)\right) \\ &= -\left(\frac{3}{5}\right) \left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1. \end{aligned}$$

Dermed findes altså et helt tal  $x$  så  $x^2 \equiv 55 \pmod{223}$ . Når  $am^{-1} - 110 \equiv x \pmod{223}$ , hvilket er ensbetydende med at  $a \equiv (x + 110)m \pmod{223}$ , er  $\dagger$  opfyldt. Hvis 3 går op i  $k$ , findes derfor et heltal  $a$  så  $(k+a)^3 - a^3 \equiv 0 \pmod{2007}$ .

**Opgave 1.18.17.** Antag at  $a$  er et positivt heltal som ikke er et kvadrattal, og at  $a$  er kvadratisk rest modulo alle primtal. Lad  $m$  være det største hele tal så  $m^2$  går op i  $a$ , og sæt  $a = m^2b$ . Da er  $b$  kvadratfrit. Da  $a$  er kvadratisk rest modulo alle primtal, er  $b$  pr. konstruktion også kvadratisk rest modulo

alle primtal. Antag først at  $b = 2$ . Da er  $b$  ikke kvadratisk rest modulo  $p = 5$ , modstrid. Dermed er  $b > 2$ .

Hvis  $b$  er lige, sættes  $b = 2b'$ , og hvis  $b$  er ulige, sættes  $b = b'$ . Bemærk at  $b'$  også er kvadratisk, og primfaktoropløsningen af  $b'$  derfor kan skrives som

$$b' = p_1 p_2 \cdots p_n,$$

hvor  $p_i$ 'erne er forskellige ulige primtal.

Lad  $c$  være et helt tal så  $\left(\frac{c}{p_n}\right) = -1$ . Vi ønsker at finde et primtal der opfylder at

$$\begin{aligned} p &\equiv 1 \pmod{8} \\ p &\equiv 1 \pmod{p_i}, \quad i = 1, \dots, n-1 \\ p &\equiv c \pmod{p_n}. \end{aligned}$$

Ifølge den kinesiske restklassesætning udgør samtlige løsninger til kongruenssystemet netop en restklasse modulo  $8b'$ . Da denne restklasse er primisk med  $8b'$ , findes ifølge Dirichlets sætning et primtal blandt repræsentanterne for restklassen. Derfor er det muligt at vælge et primtal  $p$  der opfylder kongruenssystemet. Da 2 er kvadratisk rest modulo  $p$  fordi  $p \equiv 1 \pmod{8}$ , er

$$\left(\frac{b}{p}\right) = \left(\frac{b'}{p}\right) = \prod_{i=1}^n \left(\frac{p_i}{p}\right) = \prod_{i=1}^n \left(\frac{p}{p_i}\right) = \left(\prod_{i=1}^{n-1} \left(\frac{1}{p_i}\right)\right) \cdot \left(\frac{c}{p_n}\right) = -1$$

hvilket er en modstrid.

**Opgave 1.18.18** For  $n = 3$  og  $n = 4$  ved vi at  $f_n$  er et primtal, og vi kan derfor antage at  $n \geq 5$ . Lad nu

$$f_n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$$

være primfaktoropløsningen af  $f_n$ .

Vi ved fra opgave 1.18.9 at  $p_i \equiv 1 \pmod{2^{n+2}}$  for alle  $i = 1, 2, \dots, m$ . Vælg  $x_1, x_2, \dots, x_m$  så  $p_i = 2^{n+2}x_i + 1$ . For at vise at der findes en primdivisor i  $f_n$  som er større end  $2^{n+4}(n+2)$ , mangler vi nu blot at vise at der findes et  $i$  så

$$x_i \geq 2^2(n+2).$$

Først vurderer vi summen  $k_1 + k_2 + \cdots + k_m$  opad til. Da  $p_i \geq 2^{n+2} + 1$ , er

$$2^{2^n} + 1 \geq (2^{n+2} + 1)^{k_1 + k_2 + \cdots + k_m} \geq 2^{(n+2)(k_1 + k_2 + \cdots + k_m)} + 1.$$

Altså er

$$k_1 + k_2 + \cdots + k_m \leq \frac{2^n}{n+2}.$$

Nu vurderer vi summen  $x_1 k_1 + x_2 k_2 + \cdots + x_m k_m$  nedad til. Ifølge binomialformlen er

$$p_i^{k_i} = (2^{n+2}x_i + 1)^{k_i} \equiv 2^{n+2}x_i k_i + 1 \pmod{2^{2n+4}}.$$

Da  $2^n > 2n + 4$  for  $n \geq 5$ , er  $f_n \equiv 1 \pmod{2^{2n+4}}$ . Dermed er

$$\begin{aligned} 0 &\equiv (2^{n+2}x_1 k_1 + 1)(2^{n+2}x_2 k_2 + 1) \cdots (2^{n+2}x_m k_m + 1) - 1 \\ &\equiv 2^{n+2}x_1 k_1 + 2^{n+2}x_2 k_2 + \cdots + 2^{n+2}x_m k_m \\ &\equiv 2^{n+2}(x_1 k_1 + x_2 k_2 + \cdots + x_m k_m) \pmod{2^{2n+4}}. \end{aligned}$$

Dette viser at

$$0 \equiv x_1 k_1 + x_2 k_2 + \cdots + x_m k_m \pmod{2^{n+2}}.$$

Da alle  $x_i$ 'erne og  $k_i$ 'erne er positive, er

$$x_1 k_1 + x_2 k_2 + \cdots + x_m k_m \geq 2^{n+2}.$$

Sæt  $x_i = \max(x_1, x_2, \dots, x_m)$ . Da er

$$x_i(k_1 + k_2 + \cdots + k_m) \geq 2^{n+2},$$

og dermed

$$x_i \geq \frac{2^{n+2}}{k_1 + k_2 + \cdots + k_m} \geq \frac{2^{n+2}}{\frac{2^n}{n+2}} = 2^2(n+2)$$

som ønsket.



## Stikordsregister

alternerende tværsom, 12  
aritmetikkens fundamentalsætning, 2

Bertrands postulat, 34  
Bezouts identitet, 9  
binomialformlen, 17

delelighed, 1  
delelighedsregler, 1  
den kvadratiske reciprocitetssætning, 37  
Dirichlets sætning, 34  
division med rest, 10  
divisor, 1  
divisor, ægte, 2  
divisor, triviel, 2  
divisorer, antal, 6

Euklids algoritme, 7  
Eulers  $\phi$ -funktion, 18  
Eulers kriterium, 35  
Eulers sætning, 21

faktorisering, 15  
Fermats lille sætning, 21  
Fermattal, 24  
følger, 25

gcd, største fælles divisor, 7  
Goldbachs formodning, 34

indbyrdes primisk, 8  
invers, multiplikativ, 18

kinesisk restklassesætning, 27

kongruens, 10  
kongruens, løsning af, 10  
kongruent modulo, 10  
kvadrarfri, 33  
kvadratisk reciprocitet, 37  
kvadratisk rest, 13  
kvadrattal, 3

lcm, mindste fælles multiplum, 9  
Legendres formel, 30  
Legendresymbolet, 35  
Lifting the exponent lemma (LTE), 31  
LTE, 31

Mersennetal, 23  
mindste fælles multiplum, 9  
modulo, 10  
multiplikativ invers, 18  
multiplum, 1

nulregel modulo primtal, 11

orden af  $a$  modulo  $n$ , 23

$p$ -adisk valuation, 16, 30  
periodisk følge, 25  
primfaktor, 2  
primfaktoropløsning, 2  
primisk, 8  
primisk rest, 17  
primisk restklasse, 17  
primtal, 2  
primtalsætningen, 34

repræsentant for restklasse, 10  
restklasse, 10

sammensat tal, 2  
Sophie Germain-primtal, 36  
største fælles divisor, 7  
sum af to kvadrattal, 33

Thues sætning, 33  
tværsom, 12  
tvillingeprimtal, 34

Wilson's sætning, 20

ægte divisor, 2