MAT1140, H16

MAT 1140 – Innføring i klassisk tallteori

Dette heftet er basert på forelesningsnotater av Karl Egil Aubert som senere er blitt bearbeidet av Erik Alfsen, Tom Lindstrøm, Arne B. Sletsjøe og Erik Bédos. Oppgavene er i stor grad samlet av Torgeir Onstad. I 2016-utgaven har jeg lagt til noen oppgaver, men ellers ikke gjort store endringer.

Blindern 20. august 2016

Tom Lindstrøm

Kapitlene har følgende innhold:

1. Delelighet og Euklids algoritme

Vi lar $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ betegne mengden av hele tall og $\mathbb{N} = \{1, 2, 3, \ldots\}$ mengden av naturlige tall. Det er disse to tallsystemene vi stort sett skal arbeide med i dette heftet.

Delelighet er grunnbegrepet i tallteorien. Vi minner om definisjonen: Dersom a og b er hele tall, sier vi at a *er delelig med* b dersom det finnes et helt tall q slik at

$$a = qb,$$

dvs. slik at $\frac{a}{b} = q$,. Vi sier også at b *går opp i* a, at b *deler* a, at b er en *divisor* av a og at a *er et multiplum av* b. Med symboler skriver vi

$$b \mid a$$

La $b \in \mathbb{N}$. Ved å se for oss alle multiplene av b på talllinja innser vi at et tall $a \in \mathbb{Z}$ må ligge i nøyaktig ett halvåpent intervall av typen $[qb, (q+1)b)$ for en passende $q \in \mathbb{Z}$. Tallet a er derfor på formen

$$a = qb + r \quad \text{der} \quad 0 \leq r < b$$

Vi sier at q er (den ufullstendige) *kvotienten* og at r er *resten* vi får når vi deler a med b. Legg merke til at a er delelig med b hvis og bare hvis $r = 0$.

Vi formulerer denne observasjonen som en setning:

Setning 1.1 Divisjonsalgoritmen. Anta at $a \in \mathbb{Z}$ og $b \in \mathbb{N}$. Da finnes det entydig bestemte tall $q, r \in \mathbb{Z}$ slik at

$$a = qb + r \quad , \quad 0 \leq r < b \tag{1.1}$$

□

Det kan hevdes at argumentet ovenfor ikke er helt rigorøst. Divisjonsalgoritmen kan begrunnes (jf. oppgave 1.11) ved hjelp av det såkalte *velordningsprinsippet for de naturlige tallene* som sier at enhver ikke-tom delmengde av $\mathbb{N}$ har et minste element. (Dette prinsippet er forøvrig ekvivalent med induksjonsprinsippet).

La $m, n \in \mathbb{Z}$. Ethvert heltall som deler både m og n kalles *en felles divisor av* m *og* n. Anta at m og n ikke begge er null. *Den største felles divisoren til* m og n er da det største naturlige tallet som går opp i både m og n; det betegner vi med

$$(m, n)$$

Dersom både m og n er null, er alle tall divisorer i m og n, og det er ikke så godt å vite hvordan man skal definere (m, n). Vi setter $(0, 0) = 0$, selv om det for øyeblikket sikkert ser absurd ut.

Siden 1 går opp i alle tall, vil 1 alltid være en felles divisor. Dersom 1 er den største felles divisoren til m og n, sier vi at m og n er *innbyrdes primiske*.

Vi skal studere egenskaper ved den største felles divisoren. Vi begynner med en definisjon som tilsynelatende ikke har noe med saken å gjøre. La $a, b \in \mathbb{Z}$. Vi sier at et tall $c \in \mathbb{Z}$ er en *lineær kombinasjon* av a og b dersom det finnes tall $s, t \in \mathbb{Z}$ slik at

$$c = sa + tb$$

Mengden av lineære kombinasjoner av a og b skriver vi $I(a, b)$. Vi skal bestemme nøyaktig hvilke tall som er med i $I(a, b)$. Først en enkel observasjon:

1.2 Lemma. Anta at $d \mid a$ og $d \mid b$. Da deler d også alle elementer i $I(a, b)$.

Bevis: Vi kan skrive $a = q_1 d, b = q_2 d$. Dersom $c \in I(a,b)$, finnes det $s, t \in \mathbb{Z}$ slik at

$$c = sa + tb.$$

Kombinerer vi dette, får vi

$$c = sa + tb = sq_1 d + tq_2 d = (sq_1 + tq_2)d$$

som viser at $d \,|\, c$. □

1.3 Lemma. Anta at a og b ikke begge er null. La d være det minste positive tallet i $I(a,b)$. Da består $I(a,b)$ nøyaktig av de tallene som er delelig med d.

Bevis: La oss først vise at dersom $d \,|\, c$, så er $c \in I(a,b)$. Dette er lett; vi vet at det finnes hele tall q, s, t slik at $c = qd$ og $d = sa + tb$. Dermed er

$$c = qd = q(sa + tb) = (qs)a + (qt)b$$

som viser at $c \in I(a,b)$.

Det gjenstår å vise at dersom c ikke er delelig med d, så er c ikke med i $I(a,b)$. Anta for motsigelse at $c \in I(a,b)$; da er

$$c = s'a + t'b \quad \text{for } s', t' \in \mathbb{Z}.$$

Siden c ikke er delelig med d, gir divisjonsalgoritmen

$$c = qd + r$$

der $0 < r < d$. Siden $d \in I(a,b)$, vet vi også at

$$d = sa + tb.$$

Kombinerer vi disse ligningene, får vi

$$\begin{aligned} r &= c - qd = s'a + t'b - q(sa + tb) \\ &= (s' - sq)a + (t' - tq)b \end{aligned}$$

som viser at $r \in I(a,b)$. Men dette er umulig siden $0 < r < d$ og d er det *minste*, positive elementet i $I(a,b)$. □

1.4 Teorem. La $a, b \in \mathbb{Z}$. Mengden $I(a,b)$ består da nøyaktig av de hele tallene som er delelig med (a,b). Med andre ord består $I(a,b)$ av alle de heltallige multiplene av (a,b).

Bevis: Hvis både a og b er null, er påstanden riktig på grunn av vår underlige definisjon av $(0,0)$ (det er faktisk dette som er grunnen til at $(0,0)$ er definert til å være 0). Anta derfor at a og b ikke begge er null. Ifølge lemma 1.3 er det nok å vise at $d = (a,b)$. Siden $a, b \in I(a,b)$, følger det fra det samme lemmaet at d deler både a og b. På den annen side vet vi fra lemma 1.2 at d er delelig med alle felles divisorer til a og b. Det er bare én måte å få oppfylt begge disse kravene på - d må være lik den største felles divisoren (a,b). □

Vi kan trekke et par tilleggskonklusjoner fra argumentene ovenfor:

1.5 Korollar. Største felles divisor til to tall er delelig med alle andre felles divisorer.

Bevis: Følger fra argumentet for teorem 1.4. □

1.6 Korollar. Vi kan skrive ethvert heltall som en lineær kombinasjon av a og b hvis og bare hvis a og b er innbyrdes primiske. □

Teorem 1.4 kan brukes til å si noe om eksistensen av løsninger til såkalte diofantiske ligninger. En *diofantisk ligning* av første grad er en ligning av typen

$$a\,x + b\,y = c$$

der koeffisientene a, b og c er hele tall, og der vi bare er interessert i heltallige løsninger $x, y \in \mathbb{Z}$. Vi antar dessuten at a og b ikke begge er null. Ved litt omtanke følger det direkte av teorem 1.4 at denne ligningen har heltallige løsninger hvis og bare hvis (a, b) deler c.

La oss derfor anta at (a, b) deler c. Hvordan kan vi så finne to hele tall x, y slik at $a\,x + b\,y = c$?

Problemet er at beviset til teorem 1.4 ikke gir oss noen praktisk metode til å finne x og y. Det finnes imidlertid en eldgammel metode som går tilbake til den greske matematikeren Euklid (rundt 300 f.Kr.).

Vi merker oss først at det er nok å finne to hele tall x' og y' slik at

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

Dersom $q \in \mathbb{Z}$ er slik at $c = q(a, b)$, setter vi nemlig $x = qx'$ og $y = qy'$ og får

$$a\,x + b\,y = q(a\,x' + b\,y') = q(a, b) = c$$

som ønsket.

Euklids metode, eller **Euklids algoritme** som den ofte kalles, består av to deler, og den første delen er ikke noe annet enn en litt uvant måte til å bestemme største felles divisor til to tall a og b som ikke begge er null. Vi kan like godt anta at $b \in \mathbb{N}$. Ved divisjonsalgoritmen kan vi da skrive:

$$a = q_1 b + r_1$$

Hvis divisjonen ikke går opp, deler vi b med resten r_1:

$$b = q_2 r_1 + r_2.$$

Hvis divisjonen ikke går opp, deler vi resten r_1 med resten r_2:

$$r_1 = q_3 r_2 + r_3$$

Hvis divisjonen ikke går opp, deler vi resten r_2 med resten r_3:

$$r_2 = q_4 r_3 + r_4$$

Vi fortsetter på denne måten inntil divisjonen går opp (siden hver rest er mindre enn den foregående, må vi til slutt få en rest som er null). Dersom r_n er den siste

resten som ikke er null, har vi nå utført følgende divisjoner

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \quad \vdots \quad \vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

Påstanden er nå at den siste ikke-null resten r_n er den største felles divisoren til a og b.

La oss først vise at r_n deler både a og b. Starter vi nedenfra i ligningene våre, ser vi at $r_n \mid r_{n-1}$. Fra den nest nederste ligningen følger det at $r_n \mid r_{n-2}$. Men hvis $r_n \mid r_{n-1}$ og $r_n \mid r_{n-2}$, så følger det fra den tredje nederste ligningen at $r_n \mid r_{n-3}$. Fortsetter vi oppover i systemet på denne måten, ser vi at r_n må dele alle venstresidene i ligningene, og til slutt får vi at $r_n \mid b$ og $r_n \mid a$.

Dermed vet vi at r_n er en felles divisor, og for å vise at det er den *største* felles divisoren, er det nok å vise at ethvert tall c som deler både a og b også deler r_n. Denne gang begynner vi ovenfra - den øverste ligningen i (1.2) forteller oss at $c \mid r_1$ (fordi c deler både a og b). Men hvis $c \mid b$ og $c \mid r_1$, så forteller den andre linjen oss at $c \mid r_2$. Fortsetter vi på samme måte, ser vi at $c \mid r_3$ osv. Til slutt får vi at $c \mid r_n$, og dermed har vi vist at r_n er den største felles divisoren til a og b. La oss se på et eksempel.

1.7 Eksempel. Finn største felles divisor til 222 og 84. Vi får

$$\begin{aligned} 222 &= 2 \cdot 84 + 54 \\ 84 &= 1 \cdot 54 + 30 \\ 54 &= 1 \cdot 30 + 24 \\ 30 &= 1 \cdot 24 + 6 \\ 24 &= 4 \cdot 6 \end{aligned}$$

som viser at største felles divisor er 6. □

For små tall er Euklids algoritme tungvinn sammenlignet med den vanlige faktoriseringsmetoden (faktoriser begge tallene og plukk ut de felles faktorene), men for store tall er den overlegen siden store tall er tidkrevende å faktorisere.

Vi er nå klare til å gå løs på **andre del av Euklids metode** - den som forteller oss hvordan vi kan skrive største felles divisor som en lineær kombinasjon av de opprinnelige tallene. Det er enklest å illustrere dette med et eksempel, så la oss ta Eksempel 1.7 som utgangspunkt. Vi ønsker altså å skrive 6 som en lineær kombinasjon av 222 og 84. Starter vi med den nest nederste ligningen ser vi at

$$6 = 30 - 1 \cdot 24.$$

Fra den tredje nederste ligningen ser vi at $24 = 54 - 1 \cdot 30$, og setter vi dette inn i uttrykket ovenfor, får vi

$$6 = 30 - 1 \cdot 24 = 30 - 1(54 - 1 \cdot 30) = 2 \cdot 30 - 54$$

(legg merke til at vi bare samler sammen leddene uten å gange ut). Nå ser vi fra den nest øverste ligningen at $30 = 84 - 1 \cdot 54$, og setter vi dette inn i det siste uttrykket ovenfor, får vi

$$6 = 2 \cdot 30 - 54 = 2(84 - 1 \cdot 54) - 54 = 2 \cdot 84 - 3 \cdot 54.$$

Til slutt ser vi fra den øverste ligningen at $54 = 222 - 2 \cdot 84$, så

$$6 = 2 \cdot 84 - 3(222 - 2 \cdot 84) = 8 \cdot 84 - 3 \cdot 222$$

Dermed har vi skrevet 6 som en lineær kombinasjon av 84 og 222;

$$6 = 8 \cdot 84 + (-3) \cdot 222$$

Metoden er helt generell, og går vi tilbake til ligningene i (1.2), ser vi hva som skjer: Den nederste linjen gir oss den største felles divisoren som en lineær kombinasjon $r_n = r_{n-2} - q_n r_{n-1}$ av r_{n-2} og r_{n-1}. Ved å bruke den tredje nederste linjen $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$, kan vi bytte ut r_{n-1} og få r_n som en lineær kombinasjon av r_{n-2} og r_{n-3}:

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) \\ &= (1 + q_n q_{n-1}) r_{n-2} - q_n r_{n-3} \end{aligned}$$

Ved å fortsette på denne måten får vi skrevet r_n som en lineær kombinasjon av stadig større rester, og til slutt ender vi opp med en lineær kombinasjon av a og b.

La oss si at vi egentlig ønsket å finne to hele tall x og y slik at

$$222\,x + 84\,y = 30 \ (= 5 \cdot 6).$$

Siden vi har funnet ut at $6 = 8 \cdot 84 + (-3) \cdot 222$, så vil $x = 5 \cdot (-3) = -15$ og $y = 5 \cdot 8 = 40$ være en løsning.

Metoden ovenfor hjelper oss til å finne én heltallig løsning av ligningen $ax + by = c$ når (a, b) deler c, men det finnes uendelig mange slike løsninger, og av og til har vi bruk for dem alle sammen. Det er en enkel metode for å finne alle de andre løsningene når vi kjenner én, men for å bevise den trenger vi en hjelpesetning.

1.8 Lemma. Anta at a, b er innbyrdes primiske og at a deler bc. Da må a dele c.

Bevis: Siden a og b er innbyrdes primiske, finnes det tall s, t slik at $1 = sa + tb$. Ganger vi denne ligningen med c, får vi $c = sac + tbc$. Siden bc er delelig med a, er $bc = qa$ for en heltallig q. Setter vi dette inn i ligningen, får vi

$$c = sac + tbc = sac + tqa = (sc + tq)a$$

som viser at c er delelig med a. □

Vi er nå klare til å beskrive alle løsninger av lineære diofantiske ligninger.

1.9 Setning. Anta at c er delelig med $d = (a, b)$. Da har ligningen $ax + by = c$ uendelig mange, heltallige løsninger. Hvis (x_0, y_0) er én av dem, er de andre gitt ved

$$x_k = x_0 + k\frac{b}{d}, \quad y_k = y_0 - k\frac{a}{d}$$

der $k \in \mathbb{Z}$.

Bevis: Det er lett å sjekke ved innsetting at (x_k, y_k) virkelig er en løsning:

$$ax_k + by_k = a(x_0 + k\frac{b}{d}) + b(y_0 - k\frac{a}{d}) = ax_0 + by_0 + k\frac{ab}{d} - k\frac{ba}{d} = c + 0 = c$$

For å vise at det ikke finnes flere løsninger, antar vi at (x, y) er en vilkårlig løsning og viser at den må være på formen (x_k, y_k). Setter vi $e = x - x_0$ og $f = y - y_0$, er $x = x_0 + e$ og $y = y_0 + f$. Siden både (x, y) og (x_0, y_0) er løsninger av ligningen, har vi dermed

$$c = ax + by = a(x_0 + e) + b(y_0 + f) = ax_0 + bx_0 + ae + bf = c + ae + bf$$

som gir

$$ae = -bf \tag{1}$$

Siden $d = (a, b)$, kan vi skrive $a = \frac{a}{d} \cdot d$, $b = \frac{b}{d} \cdot d$ der $\frac{a}{d}$ og $\frac{b}{d}$ er innbyrdes primiske heltall. Setter vi dette inn i ligning (1) og forkorter med d, får vi

$$\frac{a}{d} \cdot e = -\frac{b}{d} \cdot f \tag{2}$$

Dette betyr at $\frac{b}{d}$ deler produktet $\frac{a}{d} \cdot e$, og siden $\frac{a}{d}$ og $\frac{b}{d}$ er innbyrdes primiske, betyr det (ifølge lemmaet) at $\frac{b}{d}$ deler e. Følgelig er $e = k\frac{b}{d}$ for et heltall k. Ganger vi ligning (2) med k, får vi

$$k \cdot \frac{a}{d} \cdot e = -k \cdot \frac{b}{d} \cdot f \iff k \cdot \frac{a}{d} \cdot e = -ef \iff f = -k\frac{a}{d}$$

Dette betyr at $x = x_0 + e = x_0 + k\frac{b}{d}$, $y = y_0 + f = y_0 - k\frac{a}{d}$ for en $k \in \mathbb{Z}$, og dermed er setningen bevist. □

Oppgaver.

1.1 Bruk Euklids algoritme til å finne største felles divisor til 297 og 176. Skriv største felles divisor som en lineær kombinasjon av 297 og 176.

1.2 Bruk Euklids algoritme til å finne største felles divisor av 357 og 483, og uttrykk denne som en lineærkombinasjon av de to tallene.

1.3 a) Bruk Euklids algoritme til å finne største felles divisor til 784 og 36. Finnes det hele tall x, y slik at $784x + 36y = 2$?

b) Finn hele tall x, y slik at $784x + 36y = 12$.

1.4 Avgjør om det finnes hele tall x, y slik at

a) $7x + 4y = 1$
b) $9x + 15y = 4$
c) $28x + 7y = -42$

Finn i så fall alle løsningene.

1.5 Kan 21 skrives som en lineær kombinasjon av 455 og 2772? Hvis ja, finn alle slike kombinasjon.

1.6 Vis at dersom a og b er innbyrdes primiske tall som begge deler c, så vil ab også dele c.

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

a) Vis at $(ka, kb) = k(a, b)$ for alle $k \in \mathbb{N}$.

b) Definer hva som menes med minste (ikke-negativt) felles multiplum $[a, b]$ til a og b. (Merk at her har (a, b) eller $[a, b]$ ingenting med koordinater eller intervaller å gjøre!)

c) Vis at $(a, b) \cdot [a, b] = |ab|$.

d) Vis at $[ka, kb] = k[a, b]$ for alle $k \in \mathbb{N}$.

e) Definer største felles divisor (a, b, c) og minste felles multiplum $[a, b, c]$ til a, b og c.

f) Vis at

$$[a, b, c] = \frac{|abc|(a, b, c)}{(a, b)(a, c)(b, c)}$$

1.8 En delmengde I av $\mathbb{Z}$ kalles et *ideal* dersom følgende tre betingelser er oppfylt:

(i) I inneholder et element $a \neq 0$

(ii) Hvis $a, b \in I$, så er $a + b \in I$

(iii) Hvis $a \in I$ og $n \in \mathbb{Z}$, så er $na \in I$.

a) Vis at dersom ikke både a og b er null, så er $I(a, b)$ et ideal.

b) Vis at dersom I er et ideal, så er $0 \in I$ og I inneholder både positive og negative tall.

c) Anta at I er et ideal og at d er det minste positive tallet i I. Vis at

$$I = \{nd \,|\, n \in \mathbb{Z}\}$$

d) Anta at $m_1, m_2, \cdots, m_k \in \mathbb{Z}$ er forskjellig fra 0. Vis at et tall $a \in \mathbb{Z}$ kan skrives på formen

$$a = s_1 m_1 + s_2 m_2 + \cdots + s_k m_k \quad \text{der } s_i \in \mathbb{Z}$$

hvis hvis og bare hvis a er delelig med største felles divisor til $m_1, m_2, \cdots, m_k$.

1.9 Blant tallene $1, 2, 3, \cdots, 2n$ velger man ut $n+1$ vilkårlige tall. Vis at blant disse må det nødvendigvis finnes to tall a og b slik at $a \,|\, b$.
(*Hint*: Skriv de utvalgte tallene på formen $x = 2^k y$ med odde y. Hvor mange forskjellige slike oddetall kan det høyst finnes?).

1.10 En rikmann sendte sin slave til markedet for å kjøpe sauer og geiter, og sendte med ham 170 drakmer. Slaven kom tilbake med innkjøpte dyr. "Hva var prisene?" spurte rikmannen. "En sau kostet 30 drakmer og en geit 18 drakmer," svarte slaven. "Har du noen penger igjen?" spurte rikmannen. "Nei, jeg handlet for alle sammen," svarte slaven. "Du lyver," sa rikmannen. Og ganske riktig, da de ransaket slaven, fant de 8 drakmer.

a) Hvordan kunne rikmannen vite at slaven løy?

b) Hvor mange sauer og hvor mange geiter hadde slaven kjøpt?

1.11 Gi et bevis for divisjonsalgoritmen (setning 1.1) ved hjelp av velordningsprinsippet for $\mathbb{N}$.

2. Primtall og primtallsfaktorisering.

Et tall p som ikke kan deles på noe mindre tall, kalles et primtall. Mer presist har vi:

2.1 Definisjon. Et naturlig tall $p \geq 2$ som ikke kan deles med andre naturlige tall enn 1 og p, kalles et *primtall*.

Legg merke til at ifølge denne definisjonen er 1 *ikke* et primtall til tross for at det ikke kan deles med noe annet tall. De første primtallene er

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

Fordi de ikke kan spaltes i mindre tall, er primtallene de grunnleggende byggestenene i tallteorien. Alle andre tall kan skrives som produkter av primtall. De fleste vil sikkert kunne finne faktoriseringen

$$666 = 2 \cdot 3 \cdot 3 \cdot 37,$$

men det er nok ikke så mange som har sett et bevis for at en slik faktorisering alltid er mulig, og at den er entydig (når vi ser bort fra faktorenes rekkefølge). Det er disse bevisene vi nå skal se på. Vårt hovedverktøy vil være teorien fra kapittel 1.

Vi begynner med en hjelpesetning som vil være nyttig i mange sammenhenger.

2.2 Setning. Anta at p er et primtall. Dersom a og b er hele tall slik at $p \mid ab$, så må p dele minst ett av tallene a, b.

Bevis: Hvis p ikke deler a, er a og p innbyrdes primiske. Siden p deler produktet ab, må p da dele b ifølge lemma 1.8. □

Legg merke til at setningen er gal dersom p ikke er et primtall; f.eks. deler 4 tallet $12 = 6 \cdot 2$, men 4 deler hverken 6 eller 2.

2.3 Aritmetikkens fundamentalteorem. Ethvert helt tall $a \geq 2$ kan skrives som et produkt

$$a = p_1 p_2 \cdots p_m$$

der alle faktorene $p_1, p_2, \cdots, p_m$ er primtall (vi tillater produkter med bare én faktor, dvs. vi kan godt ha $m = 1$). Denne oppspaltingen er entydig i den forstand at dersom vi har

$$a = q_1 q_2 \cdots q_n$$

der $q_1, q_2, \ldots, q_n$ er primtall, så er $m = n$, og faktorene q_i er de samme som faktorene p_j bortsett fra at rekkefølgen kan være en annen.

Bevis: Dersom ikke alle tall kan skrives som produkter av primtall, må det finnes et minste tall c som ikke kan skrives som et slikt produkt. Siden c ikke kan være et primtall (hvis c er et primtall p_1, ville $c = p_1$ være en primtallsfaktorisering av c med én faktor), så må $c = ab$ der både a og b er mindre enn c. Dermed vil a og b ha primtallsfaktoriseringer

$$a = p_1 p_2 \cdots p_m \quad \text{og} \quad b = q_1 q_2 \cdots q_n$$

som gir

$$c = ab = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n$$

Dette er en primtallsfaktorisering av c, og vi har en selvmotsigelse.

Så var det entydigheten. Dersom ikke alle tall har entydige faktoriseringer, må det finnes et minste tall med to faktoriseringer

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n \tag{2.1}$$

Siden primtallet p_1 går opp i $a = q_1 q_2 \cdots q_n$, må p_1 gå opp i én av faktorene $q_1, q_2, \ldots, q_n$ ifølge Setning 2.2 (denne setningen gjelder også når vi har flere enn to faktorer, se oppgave 3 nedenfor). La oss si at p_1 går opp i q_j. Siden q_j er et primtall, betyr dette at $p_1 = q_j$. Dermed kan vi forkorte i (2.1) og få

$$p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_n.$$

Dette betyr at tallet $b = p_2 p_3 \cdots p_m = q_1 \cdots q_{j-1} q_{j+1} \cdots q_n$ har to forskjellig faktoriseringer, og det er umulig siden $b < a$. □

Det er entydigheten som er den vanskeligste delen av aritmetikkens fundamentalteorem. I mange sammenhenger er den også den nyttigste delen. Som et eksempel skal vi bruke den til å bevise at $\sqrt{2}$ ikke er et rasjonalt tall (dette kan også vises på andre måter, noe du sikkert allerede har sett). I geometrisk form går dette resultatet tilbake til den pythagoreiske skolen i Hellas over 400 år f. Kr.

2.4 Teorem. $\sqrt{2}$ er irrasjonal.

Bevis: Anta at $\sqrt{2} = \frac{m}{n}$ der $m, n \in \mathbb{N}$. Da er

$$2n^2 = m^2$$

Faktoriserer vi $n = p_1 p_2 \cdots p_r$ og $m = q_1 q_2 \cdots q_s$, får vi

$$2p_1^2 p_2^2 \cdots p_r^2 = q_1^2 q_2^2 \cdots q_s^2$$

Dette er to primtallsfaktoriseringer av det samme tallet, og bortsett fra rekkefølgen må de være like. Men det er umulig siden det må være et odde antall 2'ere på venstre side, og like antall på høyre side. Altså har antagelsen om at $\sqrt{2}$ er rasjonal ledet til en motsigelse, og vi kan konkludere med at $\sqrt{2}$ må være irrasjonal. □

Skriver vi opp de første primtallene etter hverandre, ser vi at de blir sjeldnere og sjeldnere etter hvert, og det er naturlig å spørre om de tar slutt et sted. I følge Euklid gjør de ikke det.

2.5 Teorem (Euklid). Det finnes uendelig mange primtall.

Bevis: Anta at det motsatte er sant, altså at det bare finnes et endelig antall primtall, og la $p_1, p_2, \cdots, p_n$ være en opplisting av alle primtallene. Vi skal vise at det må finnes et primtall til, det vil si et primtall p slik at $p \neq p_i$ for alle i, og dermed utlede en motsigelse. La

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Da har N rest 1 når vi deler med p_i for alle i, så $p_i \nmid N$. Men ifølge Aritmetikkens Fundamentalteorem, må N være delelig med et primtall p. Altså er $p \neq p_i$ for alle i og teoremet er bevist. □

La $t \in \mathbb{N}$, $t \geq 2$. Vi sier at to tall $a, b \in \mathbb{Z}$ er *kongruente modulo* t dersom a og b har samme rest når vi deler dem med t. Vi beskriver dette ved $a \equiv b \pmod{t}$. For eksempel er $a \equiv 1 \pmod{2}$ hvis og bare hvis a er et oddetall. Vi skal studere kongruensbegrepet nærmere i neste kapittel.

Primtallene større enn 2 er enten kongruente med 1 (mod 4) eller med 3 (mod 4). F.eks. er 5, 13 og 17 kongruente med 1 (mod 4), mens 3, 7 og 11 er kongruente med 3 (mod 4). Vi skal se senere at primtallene som er kongruente med 1 (mod 4) har en annen oppførsel enn dem som er kongruente med 3 (mod 4). Det kan derfor være interessant å vite om det er uendelig mange av hver type. Det er det, men resultatet er mye enklere å vise for primtall som er kongruente med 3 (mod 4). Dette skyldes at produktet av tall som er kongruente med 1 (mod 4) selv er kongruente med 1 (mod 4) som følgende utregning viser

$$(4n+1)(4m+1) = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1$$

Ved induksjon gjelder resultatet også for mer enn to faktorer. Tar vi produktet av tall som er kongruente med 3 (mod 4), vil det være kongruent med 1 eller 3 avhengig av om produktet har et like eller odde antall faktorer.

2.6 Setning. Det finnes uendelig mange primtall som er kongruente med 3 (mod 4).

Bevis: Idéen er den samme som i Euklids bevis. Anta for motsigelse at det bare finnes endelige mange primtall $p_1, p_2, \cdots, p_n$ som er kongruente med 3 (mod 4). Vi må vise at finnes et primtall $p \equiv 3 \pmod{4}$ som er forskjellig fra alle p_i.

Vi må åpenbart ha med 3 i listen $p_1, p_2, \cdots, p_n$, så la oss si $p_1 = 3$. Vi danner

$$N = 4p_2p_3 \cdots p_n + 3$$

(legg merke til at vi har utelatt $p_1 = 3$ i produktet), og observerer at $p_i \nmid N$ for alle i. På den annen side må minst én av primfaktorene p til N være kongruent med 3 (mod 4): Hvis de alle var kongruente med 1 (mod 4), så ville også $N \equiv 1 \pmod{4}$ etter argumentet ovenfor, og N er åpenbart kongruent med 3 (mod 4). Dermed er $p \equiv 3 \pmod{4}$ og $p \neq p_i$ for alle i, og beviset er komplett. □

Beviset for at det også finnes uendelig mange primtall som er kongruente med 1 (mod 4), følger den samme grunnidéen, men er noe mer komplisert, så vi venter med det til kapittel 5. Vi kan uttrykke disse to resultatene på en litt annen måte - den første sier at den aritmetiske tallfølgen

$$\{4n+3\}_{n\in\mathbb{Z}}$$

inneholder uendelig mange primtall, og den andre sier det samme om tallfølgen

$$\{4n+1\}_{n\in\mathbb{Z}}.$$

Vi kan stille det samme spørsmålet mer generelt - gitt to hele tall a, b, når vil den aritmetiske tallfølgen

$$\{an + b\}_{n\in\mathbb{Z}}$$

inneholde uendelig mange primtall?

Dersom a og b har en felles faktor d, så vil også $an + b$ være delelig med d, så i dette tilfellet inneholder følgen høyst ett primtall (nemlig d). Hvis a og b ikke har felles faktorer, sier et berømt teorem av den tyske matematikeren Peter Gustav Lejeune Dirichlet (1805-1859) at følgen $\{an+b\}_{n\in\mathbb{Z}}$ inneholder uendelig mange primtall. Dirichlets bevis var en sensasjon da det kom i 1839; det benyttet helt nye metoder fra den matematiske fysikken (Fourier-rekker) som de færreste hadde forestilt seg skulle ha noe med tallteori å gjøre. Selv i dag er bevisene for Dirichlets teorem for vanskelige (og lange) til at vi kan ta med et her.

Man kan stille andre typer spørsmål om primtallenes fordeling. Lar vi f.eks.

$$\pi(x) = \text{antall primtall som er mindre eller lik } x,$$

så hadde allerede Legendre og Gauss kommet frem til at $\pi(x)$ vokser omtrent som $\frac{x}{\log x}$ ved å studere et stort tallmateriale. (Med $\log x$ menes her den naturlige logaritmen til x).
Den russiske matematikeren P.L. Tsjebysjev (1821-1894) viste i 1852 at

$$0.9\,\frac{x}{\log x} \leq \pi(x) \leq 1.11\,\frac{x}{\log x}$$

for alle $x \geq 30$.
I 1896 klarte den franske matematikeren Jacques Hadamard (1865-1963) og den belgiske matematikeren Charles de la Vallée Poussin (1866-1962) uavhengig av hverandre å vise hovedresultatet i denne delen av tallteorien:

Primtallsatsen.

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

Det opprinnelige beviset for primtallsatsen benytter teknikker fra kompleks funksjonsteori, og for mange var det en stor overraskelse da den norske matematikeren Atle Selberg (1917-2007) i 1948 la frem et bevis som kun benyttet tallteoretiske metoder (i matematisk sjargong kalles dette et "elementært" bevis - men det betyr ikke at det er lett!).

Oppgaver

2.1 La $a, b \in \mathbb{Z}$, $|a|, |b| \geq 2$.

a) La $p_1, p_2, \ldots, p_n$ være samtlige primfaktorer som forekommer i a eller i b. Da kan vi skrive $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ med alle $\alpha_i \geq 0$ og $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$ med alle $\beta_i \geq 0$. Forklar at da er

$$(a, b) = p_1^{\mu_2} p_2^{\mu_2} \cdots p_n^{\mu_n} \ , \ \mu_i = \min\{\alpha_i, \beta_i\}$$

$$[a, b] = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n} \ , \ \lambda_i = \max\{\alpha_i, \beta_i\}$$

(Husk at $[a, b]$ betegner minste felles multiplum til a og b).

b) Faktoriser 172 og 36, og bestem (172,36) og [172,36].

2.2 Anta at $k^2 = ab$, der $k, a, b \in \mathbb{N}$ og $(a, b) = 1$. Vis at a og b er kvadrattall.

2.3 Vis følgende påstand ved induksjon på n: Dersom p er et primtall og $p|a_1a_2 \cdots a_n$, så må p dele minst én av faktorene $a_1, a_2, \cdots, a_n$.

2.4 Anta at $n \in \mathbb{N}$ ikke er et kvadrattall. Vis at $\sqrt{n}$ er irrasjonal.

2.5 Husk her at $\log_a b$ er definert ved $a^{\log_a b} = b$ når $a > 1, b > 0$.

a) Vis at $\log_2 5$ er irrasjonal.
b) La a og b være naturlige tall større enn 1, og anta at det ene tallet har en primfaktor som ikke forekommer i det andre. Vis at $\log_a b$ er irrasjonal.

2.6 La n være et vilkårlig naturlig tall.

a) Vis at det fins en sekvens av n naturlige tall (i rekkefølge) som ikke inneholder noe primtall. (*Hint*: Start med $(n + 1)! + 2$).
b) Vis at det fins et primtall p slik at $n < p \leq n! + 1$.

2.7 I Setning 2.6 viste vi at det fins uendelig mange primtall som er kongruente med 3 (mod 4). Vi skal se senere (i kapittel 5) at det også fins uendelig mange primtall som er kongruente med 1 (mod 4). Her bes du om å sjekke noen andre tilfeller av Dirichlets generelle resultat.

a) Vis at det finnes uendelig mange primtall som er kongruente med 2 (mod 3). *Å bevise at det fins uendelig mange primtall som er kongruente med 1 (mod 3) er atskillig vanskeligere.*
b) Vis at det finnes uendelig mange primtall som er kongruente med 5 (mod 6).
c) Forklar hvorfor det bare fins endelig mange primtall som er kongruente med 2, 3 eller 4 (mod 6).

2.8 La $a, n \in \mathbb{N}$ og $n > 1$. Vis at dersom $a^n - 1$ er et primtall, så må $a = 2$, og n må være et primtall.

2.9 Fermat-tallene defineres ved $F_n = 2^{2^n} + 1$ for $n = 0, 1, 2, 3, \cdots$

a) Vis at to forskjellige Fermat-tall er innbyrdes primiske. (*Hint*: La F_n og F_{n+k} være de to tallene, og sett $x = 2^{2^n}$. Vis først at $F_n|(F_{n+k} - 2)$.)
b) Vis at for enhver $n \in \mathbb{N}$ fins det minst n primtall mindre enn F_n.
c) Bruk b) til å vise at det fins uendelig mange primtall.

2.10

a) Vis at for alle tall $a, n \in \mathbb{N}$ er

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$$

Vis at hvis $a^n - 1$ er et primtall, så er $a = 2$.
b) Vis at hvis $2^n - 1$ er et primtall, så er n et primtall.

3. Kongruensregning

I dette kapitlet lar vi t være et naturlig tall større enn 1. Vi minner om at to tall $a, b \in \mathbb{Z}$ kalles *kongruente modulo* t dersom a og b har samme rest når vi deler disse med t, og at vi beskriver dette ved $a \equiv b \pmod{t}$.

Dersom vi deler et helt tall med t, har vi t mulige rester: $0, 1, 2, \cdots, t-1$. Samler vi sammen de tallene som gir samme rest, m.a.o. de tallene som er kongruente modulo t med hverandre, får vi mengdene

$$\begin{aligned}
\bar{0} &= \{\cdots, -2t, -t, 0, t, 2t, 3t, \cdots\} \\
\bar{1} &= \{\cdots, -2t+1, -t+1, 1, t+1, 2t+1, 3t+1, \cdots\} \\
\bar{2} &= \{\cdots, -2t+2, -t+2, 2, t+2, 2t+2, 3t+2, \cdots\} \\
&\vdots \quad \vdots \qquad \vdots \qquad \vdots \\
\bar{r} &= \{\cdots, -2t+r, -t+r, r, t+r, 2t+r, 3t+r, \cdots\} \\
&\vdots \quad \vdots \qquad \vdots \qquad \vdots \\
\overline{t-1} &= \{\cdots, -2t-1, -t-1, -1, t-1, 2t-1, 3t-1, \cdots\}
\end{aligned}$$

Mengdene $\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{t-1}$ kalles *restklasser modulo* t, og mengden

$$\mathbb{Z}/(t) = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{t-1}\}$$

kalles *restklasseringen modulo* t. Vi har altså at a og b er kongruente modulo t hvis og bare hvis a og b tilhører samme restklasse modulo t. Vi legger også merke til at $a \equiv b \pmod{t}$ hvis og bare hvis $a - b$ er delelig med t.

Hvorfor $\mathbb{Z}/(t)$ kalles en ring, forstår vi dersom vi tenker oss tallinjen som en line som vi kan kveile opp. Kveiler vi slik at hver løkke får lengde t, vil elementene i samme restklasse havne på samme sted på sirkelen.

For et vilkårlig helt tall c lar vi $\bar{c}$ betegne restklassen som c tilhører (tidligere har vi bare brukt denne skrivemåten for $c = 0, 1, \cdots, t-1$). Vi har da at

$$a \equiv b \pmod{t} \Leftrightarrow a \text{ og } b \text{ gir samme rest når vi deler med } t \Leftrightarrow t \mid (a-b) \Leftrightarrow \bar{a} = \bar{b}$$

Selv om disse formuleringene er logisk ekvivalente, leder de tankene i ulike retninger, og det er derfor nyttig å kunne veksle mellom dem.

Som vi snart skal se eksempler på, er restklasser et av de viktigste verktøyene i tallteorien. Grunnen til at de er så nyttige, ligger i følgende enkle setning.

3.1 Setning. Anta $a_1 \equiv a_2 \pmod{t}$ og $b_1 \equiv b_2 \pmod{t}$. Da er

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{t} \text{ og } a_1 b_1 \equiv a_2 b_2 \pmod{t}$$

Bevis: Siden $a_1 \equiv a_2 \pmod{t}$ og $b_1 \equiv b_2 \pmod{t}$, finnes det hele tall m og n slik at $a_1 = a_2 + mt$ og $b_1 = b_2 + nt$. Dermed er

$$a_1 + b_1 = (a_2 + mt) + (b_2 + nt) = a_2 + b_2 + (m+n)t$$

som viser at $a_1 + b_1 \equiv a_2 + b_2 \pmod{t}$. Tilsvarende er

$$a_1 b_1 = (a_2 + mt)(b_2 + nt) = a_2 b_2 + (a_2 n + b_2 m + mnt)t$$

som viser at $a_1 b_1 \equiv a_2 b_2 \pmod{t}$. □

Bemerkning: Ved induksjon kan vi utvide disse reglene til flere enn to ledd/ faktorer.

På grunn av setningen ovenfor kan vi definere addisjon og multiplikasjon av restklasser.

3.2 Definisjon. Dersom $\bar{a}, \bar{b} \in \mathbb{Z}/(t)$ er to restklasser, definerer vi deres sum og produkt ved

$$\bar{a} + \bar{b} = \overline{a+b}$$
$$\bar{a}\bar{b} = \overline{ab}$$

For å addere (multiplisere) restklassene $\bar{a}$ og $\bar{b}$, adderer (multipliserer) vi altså tallene a og b, og tar så restklassen til resultatet.

Bemerkning: Dersom vi ikke hadde hatt setning 3.1, ville ikke denne definisjonen gitt mening. Da kunne vi nemlig ha plukket ut tall a_1, a_2, b_1, b_2 slik at $\bar{a}_1 = \bar{a}_2, \bar{b}_1 = \bar{b}_2$, men $\overline{a_1 + b_1} \neq \overline{a_2 + b_2}$. Hva skulle vi da ha definert summen av de to restklassene til å være : $\overline{a_1 + b_1}$ eller $\overline{a_2 + b_2}$? Konstruksjoner av denne typen er vanlig i alle deler av matematikken, og matematikere sier gjerne at operasjoner er *veldefinerte* når de ikke avhenger av hvilke representanter vi plukker ut fra restklassene. Operasjoner som ikke er veldefinerte, vil de som regel ikke ha noe med å gjøre.

3.3 Eksempel. La oss regne ut $\bar{5} + \bar{6}$ og $\bar{5} \cdot \bar{6}$ i $\mathbb{Z}/(13)$. Vi har at

$$\bar{5} + \bar{6} = \overline{5+6} = \overline{11} \quad \text{og} \quad \bar{5} \cdot \bar{6} = \overline{5 \cdot 6} = \overline{30}\,.$$

Dette siste svaret er for så vidt riktig, men det er ikke veldig opplysende - det ville ha vært bedre å få oppgitt svaret som restklassen til et tall mellom 0 og 12. Det er lett å ordne; vi deler rett og slett svaret 30 på modulusen 13

$$30 = 2 \cdot 13 + 4,$$

som viser at $30 \equiv 4 \,(\text{mod } 13)$. Altså er

$$\bar{5} \cdot \bar{6} = \bar{4} \quad \text{i } \mathbb{Z}/(13).$$

□

Ved å gå fram på denne måten kan vi lage addisjons- og multiplikasjonstabellen for $\mathbb{Z}/(t)$. Tabellen nedenfor viser addisjon i $\mathbb{Z}/(6)$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

TABELL 1. Addisjon i $\mathbb{Z}/(6)$

Den neste taballen viser multiplikasjon i $\mathbb{Z}/(6)$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

TABELL 2. Multplikasjon i $\mathbb{Z}/(6)$

La oss nå se på noen av de grunnleggende regnereglene for $\mathbb{Z}/(t)$:

3.4 Setning. I $\mathbb{Z}/(t)$ gjelder

(i) $\bar{a}+\bar{b}=\bar{b}+\bar{a}$ og $\bar{a}\bar{b}=\bar{b}\bar{a}$ (kommutative lover)
(ii) $(\bar{a}+\bar{b})+\bar{c}=\bar{a}+(\bar{b}+\bar{c})$ og $(\bar{a}\bar{b})\bar{c}=\bar{a}(\bar{b}\bar{c})$ (assosiative lover)
(iii) $\bar{a}(\bar{b}+\bar{c})=\bar{a}\bar{b}+\bar{a}\bar{c}$ (distributiv lov)
(iv) $\bar{a}+\bar{0}=\bar{a}$ (null-element)
(v) $\bar{a}\cdot\bar{1}=\bar{a}$ (nøytralt element)
(vi) $\bar{a}+\overline{(-a)}=\bar{0}$ (motsatt element)

for alle $\bar{a},\bar{b},\bar{c}\in\mathbb{Z}/(t)$.

Bevis: Alle disse punktene vises på samme måte - vi overfører til tilsvarende egenskaper i $\mathbb{Z}$. La oss ta (iii) som et eksempel:

$$\begin{aligned}
\bar{a}(\bar{b}+\bar{c}) &= \bar{a}(\overline{b+c}) && \text{(def. av addisjon)}\\
&= \overline{a(b+c)} && \text{(def. av multiplikasjon)}\\
&= \overline{ab+ac} && \text{(distributiv lov i } \mathbb{Z})\\
&= \overline{ab}+\overline{ac} && \text{(def. av addisjon)}\\
&= \bar{a}\bar{b}+\bar{a}\bar{c} && \text{(def. av multiplikasjon)}
\end{aligned}$$

□

Bemerkning: Et algebraisk system som tilfredsstiller punktene (i)-(vi) ovenfor, kalles en *kommutativ ring*. Dette er et generelt begrep som omfatter mange interessante eksempler, men det har sitt utspring i restklasseringene $\mathbb{Z}/(t)$.

Regnereglene ovenfor er så like de vi er vant til, at det er lett å tro at regning i $\mathbb{Z}/(t)$ er akkurat som regning i $\mathbb{Z}$. Men ser vi nøyere på multiplikasjonstabellen for $\mathbb{Z}/(6)$ ovenfor, finner vi raskt to brudd på vanlige regler; for det første er produktet $\bar{3}\cdot\bar{2}$ lik null uten at noen av faktorene er lik null, og for det andre er $\bar{4}\cdot\bar{1}=\bar{4}\cdot\bar{4}$ uten at vi kan forkorte og få at $\bar{1}=\bar{4}$. Vi skal se nærmere på disse merkverdighetene om et øyeblikk, men la oss først ta med oss en regel som faktisk gjelder.

3.5 Setning. Dersom $\bar{x}+\bar{a}=\bar{y}+\bar{a}$, så er $\bar{x}=\bar{y}$.

Bevis: Adderer vi $\overline{(-a)}$ på begge sider, får vi

$$(\bar{x}+\bar{a})+\overline{(-a)} = \bar{y}+\bar{a}+\overline{(-a)} \overset{(ii)}{\Rightarrow} \bar{x}+(\bar{a}+\overline{(-a)}) = \bar{y}+(\bar{a}+\overline{(-a)})$$
$$\overset{(vi)}{\Rightarrow} \bar{x}+\bar{0} = \bar{y}+\bar{0} \overset{(iv)}{\Rightarrow} \bar{x} = \bar{y}$$

der romertallene markerer hvilken del av setning 3.4 vi bruker. □

Regninger av denne typen ligner mer på det vi er vant til, dersom vi innfører *subtraksjon* ved å definere

$$\bar{a}-\bar{b} = \bar{a}+\overline{(-b)}$$

(sagt på en annen måte er $\bar{a}-\bar{b} = \overline{a-b}$).

La oss nå vende tilbake til de bruddene på vanlige regneregler som vi oppdaget ovenfor. Vi trenger et par definisjoner.

Et element $\bar{a} \in \mathbb{Z}/(t)$ kalles en *null-divisor* dersom $\bar{a} \neq \bar{0}$ og det finnes et annet element $\bar{b} \neq \bar{0}$ slik at $\bar{a}\cdot\bar{b} = \bar{0}$.

Videre sier vi at *forkortningsregelen gjelder for* $\overline{a}$ (i $\mathbb{Z}/(t)$) dersom følgende holder :

$$\text{hvis } \overline{x},\overline{y} \in \mathbb{Z}/(t) \text{ er slik at } \overline{a}\cdot\overline{x} = \overline{a}\cdot\overline{y}\,, \text{ så er } \overline{x} = \overline{y}.$$

3.6 Setning. La $t \in \mathbb{N}$, $\overline{a} \in \mathbb{Z}/(t), \overline{a} \neq \overline{0}$. Da har vi at

$$(a,t) = 1 \Leftrightarrow \text{ forkortningsregelen gjelder for } \overline{a}$$

og

$$(a,t) \neq 1 \Leftrightarrow \overline{a} \text{ er en null-divisor i } \mathbb{Z}/(t).$$

Spesielt ser vi at hvis t er et primtall, så har $\mathbb{Z}/(t)$ ingen null-divisorer, og forkortningsregelen gjelder for alle elementene i $\mathbb{Z}/(t)$ forskjellige fra null-elementet $\bar{0}$.

Bevis. Anta først at $(a,t) = 1$. Vi skal vise at da gjelder forkortningsregelen for $\overline{a}$ og at $\overline{a}$ ikke er en null-divisor.

Anta derfor at $\overline{x},\overline{y} \in \mathbb{Z}/(t)$ er slik at $\overline{a}\cdot\overline{x} = \overline{a}\cdot\overline{y}$. Da er $\overline{ax} = \overline{ay}$, dvs. at $t \mid (ax-ay) = a(x-y)$. Siden $(a,t) = 1$ får vi fra lemma 1.8 at da må $t \mid (x-y)$, altså at $\overline{x} = \overline{y}$. Dette viser at forkortningsregelen gjelder for $\overline{a}$.

Observer også at hvis $\overline{a}\cdot\overline{b} = \overline{0}$ for en $\overline{b} \in \mathbb{Z}/(t)$, så er $\overline{a}\cdot\overline{b} = \overline{a}\cdot\overline{0}$ siden $\overline{0} = \overline{a}\cdot\overline{0}$. Vi kan nå bruke forkortningsregelen for $\overline{a}$ og konkludere med at $\overline{b} = \overline{0}$. Dette viser at $\overline{a}$ ikke kan være en null-divisor.

Anta så at $(a,t) \neq 1$. Vi skal nå vise at forkortningsregelen ikke gjelder for $\overline{a}$ og at $\overline{a}$ er en null-divisor.

Sett $d = (a,t) > 1$, og velg $k,l \in \mathbb{Z}$ slik at $a = k\cdot d$, $t = l\cdot d$.

Da er $0 < l < t$, så $\overline{l} \neq \overline{0}$. Videre er

$$\overline{a}\cdot\overline{l} = \overline{kd}\cdot\overline{l} = \overline{kdl} = \overline{kt} = \overline{0} = \overline{a}\cdot\overline{0}.$$

Altså er $\overline{a}\cdot\overline{l} = \overline{a}\cdot\overline{0}$ samtidig som $\overline{l} \neq \overline{0}$. Dette viser at forkortningsregelen ikke gjelder for $\overline{a}$. Videre har vi at $\overline{a}\cdot\overline{l} = \overline{0}$, som betyr at $\overline{a}$ er en null-divisor.

Tilsammen har vi dermed vist at begge ekvivalensene holder. Vi ser også at hvis t er et primtall, så er $(a,t)=1$ for alle $\overline{a}\neq\overline{0}$ (siden det siste betyr at t ikke deler a), og den siste påstanden følger da fra det vi allerede har vist. □

3.7 Eksempel. Vi skal nå se på et enkelt eksempel på bruk av restklasser. Husk at tverrsummen til et tall er summen av sifrene - tverrsummen til 734 er altså 7+3+4=14. En gammel regel sier at et tall er delelig med 3 hvis og bare hvis tverrsummen til tallet er delelig med 3.

For å bevise dette la oss anta at tallet er $a_n a_{n-1}a_{n-2}\cdots a_1a_0$, der a'ene angir sifrene. Siden vi (implisitt) bruker 10-tallssystemet, betyr det at tallet er lik

$$a_n\cdot 10^n + a_{n-1}10^{n-1}+\cdots+a_1 10+a_0.$$

Bruker vi at $\overline{10}=\bar{1}$ i $\mathbb{Z}/(3)$, får vi

$$\begin{aligned}&\overline{a_n\cdot 10^n + a_{n-1}10^{n-1}+\cdots+a_1\cdot 10+a_0} = \\ &= \bar{a}_n\cdot\bar{1}^n+\bar{a}_{n-1}\cdot\bar{1}^{n-1}+\cdots+\bar{a}_1\bar{1}+\bar{a}_0 = \\ &= \overline{a_n+a_{n-1}+\cdots+a_1+a_0}\end{aligned}$$

som viser at tallet og tverrsummen tilhører samme restklasse i $\mathbb{Z}/(3)$, og derfor gir samme rest når de deles med 3. □

Vi skal nå studere hvordan vi kan løse lineære ligninger $\bar{a}\cdot\bar{x}=\bar{b}$ i $\mathbb{Z}/(t)$. Vi begynner med hovedresultatet.

3.8 Teorem. Ligningen $\bar{a}\cdot\bar{x}=\bar{b}$ har en løsning i $\mathbb{Z}/(t)$ hvis og bare hvis $(a,t)\,|\,b$.

Bevis: Anta $(a,t)\,|\,b$. Ifølge teorem 1.4 finnes det hele tall x,y slik at

$$b=xa+yt$$

Tar vi restklasser, får vi

$$\bar{b}=\overline{xa+yt}=\bar{x}\cdot\bar{a}+\bar{y}\cdot\bar{t}=\bar{x}\cdot\bar{a}$$

og ligningen er løst.

Anta omvendt at ligningen har en løsning $\bar{x}$. Da er $\bar{b}=\bar{a}\cdot\bar{x}$ som betyr at

$$b=xa+yt\quad\text{for en } y\in\mathbb{Z}$$

Dermed har vi skrevet b som en linear kombinasjon av a og t, og ifølge teorem 1.4 er da b delelig med (a,t). □

Legg merke til at dersom $(a,t)=1$, så følger det fra teorem 3.8 at ligningen $\bar{a}\bar{x}=\bar{b}$ alltid en løsning. I dette tilfelle er løsningen entydig: Dersom både $\bar{x}$ og $\bar{y}$ er løsninger, så må $\bar{a}\bar{x}=\bar{a}\bar{y}$, og dermed $\bar{x}=\bar{y}$ ifølge setning 3.6. Dersom $1\neq(a,t)\,|\,\ b$ vil ligningen ha flere løsninger, og vi kan bruke setning 1.9 til å finne dem.

3.9 Korollar. Anta at $d=(a,t)$ og at $d|b$. Da har ligningen $\bar{a}\bar{x}=\bar{b}$ nøyaktig d forskjellige løsninger i $\mathbb{Z}/(t)$. Dersom vi har én løsning $\overline{x}_0$, er alle løsningene gitt ved $\bar{x}=\overline{x_0+k\frac{t}{d}}$, der $k=0,1,2,\ldots,d-1$.

Bevis: Vi ser fra beviset for teoremet at $\bar{x}$ er en løsning av $\bar{a}\bar{x} = \bar{b}$ hvis og bare hvis det finnes en $y \in \mathbb{Z}$ slik at $ax + yt = b$. Ifølge setning 1.9 finnes det en slik y hvis og bare hvis $x = x_0 + k\frac{t}{d}$ for en $k \in \mathbb{Z}$. Følgelig er løsningene til ligningen vår gitt ved $\bar{x} = \overline{x_0 + k\frac{t}{d}}$ der $k \in \mathbb{Z}$, men bare de k første ($k = 0, 1, 2, \ldots, d-1$) av disse er forskjellige (sjekk dette selv!) □

Innebygget i beviset ovenfor ligger det en metode til å løse ligningen. Vi viser den gjennom et eksempel.

3.10 Eksempel. Vi skal løse ligningen $\overline{9}\,\bar{x} = \bar{6}$ i $\mathbb{Z}/(24)$. Siden $d = (9, 24) = 3$ og 6 er delelig med 3, har ligningen $d = 3$ forskjellige løsninger. Vi bruker først Euklids metode på koeffisienten 9 og modulusen 24:

$$\begin{aligned} 24 &= 2 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 \end{aligned}$$

Dermed kan vi skrive

$$3 = 9 - 6 = 9 - (24 - 2 \cdot 9) = 3 \cdot 9 - 24$$

som ganget med 2 gir

$$6 = 6 \cdot 9 - 2 \cdot 24$$

Dette viser at $\bar{x}_0 = \bar{6}$ er en løsning av ligningen. De andre er gitt ved (legg merke til at $\frac{t}{d} = \frac{24}{3} = 8$):

$$\bar{x}_1 = \overline{x_0 + 1 \cdot \frac{24}{3}} = \bar{6} + \bar{8} = \overline{14}$$

og

$$\bar{x}_2 = \overline{x_0 + 2 \cdot \frac{24}{3}} = \bar{6} + \overline{16} = \overline{22}$$

□

La oss ta med et eksempel til.

3.11 Eksempel. Vi skal løse ligningen $\overline{11}\,\bar{x} = \bar{3}$ i $\mathbb{Z}/(37)$. Siden 37 er et primtall er $(11, 37) = 1$, så vi vet at ligningen har en entydig løsning. Vi bruker nå først Euklids algoritme på koeffisienten 11 og modulusen 37:

$$\begin{aligned} 37 &= 3 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 \end{aligned}$$

Dermed kan vi skrive

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 = 4 - 1(11 - 2 \cdot 4) = 3 \cdot 4 - 11 \\ &= 3(37 - 3 \cdot 11) - 11 = 3 \cdot 37 - 10 \cdot 11. \end{aligned}$$

Multipliserer vi med 3, får vi

$$3 = 9 \cdot 37 - 30 \cdot 11$$

som gir

$$\bar{3} = \bar{9} \cdot \overline{37} + \overline{(-30)} \cdot \overline{11} = \overline{(-30)} \cdot \overline{11}.$$

Siden $\overline{-30} = \overline{-30 + 37} = \bar{7}$, ser vi at $\bar{x} = \bar{7}$.

Legg forøvrig merke til at vi i dette tilfellet kunne ha forenklet regningene ved å stoppe etter linje 2 i Euklids algoritme. Det ville ha gitt oss

$$3 = 11 - 2 \cdot 4 = 11 - 2(37 - 3 \cdot 11) = -2 \cdot 37 + 7 \cdot 11,$$

det vil si

$$\bar{3} = \overline{(-2)} \cdot \overline{37} + \bar{7} \cdot \overline{11} = \bar{7} \cdot \overline{11}.$$

□

Et viktig spesialtilfelle av ligningen $\bar{a}\bar{x} = \bar{b}$ får vi ved å sette $\bar{b} = \bar{1}$. Fra teorem 3.8 og den etterfølgende kommentaren ser vi at ligningen $\bar{a}\bar{x} = \bar{1}$ har en løsning hvis og bare hvis $(a, t) = 1$, og at denne løsningen da er entydig. Vi kaller denne løsningen den *(multiplikative) inversen til* $\bar{a}$ og betegnes med $\bar{a}^{-1}$.

Vi har altså at når $(a, t) = 1$, så er $\bar{a}^{-1}$ det entydige bestemte elementet i $\mathbb{Z}/(t)$ som er slik at

$$\bar{a}^{-1} \cdot \bar{a} = \bar{1}.$$

Hvis t er et primtall, har vi spesielt at ethvert element $a \in \mathbb{Z}/(t)$ som ikke er lik $\bar{0}$ har en invers. For dem som kan litt algebra, betyr denne egenskapen at når t er et primtall, er $\mathbb{Z}(t)$ ikke bare en ring, men det som kalles en *kropp*.

3.12 Setning. Anta at $(a, t) = 1$. Da er den entydige løsningen til $\bar{a}\bar{x} = \bar{b}$ i $\mathbb{Z}/(t)$ gitt ved $\bar{x} = \bar{a}^{-1}\bar{b}$.

Bevis: At ligningen har en entydig løsning har vi allerede sett. Ved å multiplisere ligningen $\bar{a}\bar{x} = \bar{b}$ med $\bar{a}^{-1}$ og bruke regnereglene i setning 3.4 får vi:

$$\bar{a}^{-1}(\bar{a}\bar{x}) = \bar{a}^{-1}\bar{b} \;\Rightarrow\; (\bar{a}^{-1}\bar{a})\bar{x} = \bar{a}^{-1}\bar{b} \Rightarrow\; \bar{1} \cdot \bar{x} = \bar{a}^{-1}\bar{b} \;\Rightarrow\; \bar{x} = \bar{a}^{-1}\bar{b}.$$

□

3.13 Eksempel. Vi kan også løse ligningen $\overline{11}\bar{x} = \bar{3}$ i $\mathbb{Z}/(37)$ fra forrige eksempel slik:

Siden $(-10) \cdot 11 = -110 = 1 - 3 \cdot 37$, så er $\overline{11}^{-1} = \overline{-10}$ i $\mathbb{Z}/37$. (Merk: vi fant ut at $1 = 3 \cdot 37 - 10 \cdot 11$ i forrige eksempel ved Euklids algoritme; men noen ganger kan man lett "se" hva inversen skal være). Derfor er løsningen til ligningen gitt ved

$$\bar{x} = \overline{11}^{-1} \cdot \bar{3} = \overline{-10} \cdot \bar{3} = \overline{-30} = \bar{7}.$$

□

3.14 Eksempel. Vi tar med til slutt et annet eksempel på bruk av kongruensregning (som spesielt interesserte anbefales å utforske på egenhånd; det er ikke pensumsrelevant). Alle som bor i Norge har et 11-sifret personnummer. Personnummeret består av et 6-sifret fødselsnummer, et 3-sifret individnummer og 2 kontrollsiffer. La $(a_1, \ldots, a_9)$ være de 9 første sifrene.

Det tiende sifferet er gitt ved $a_{10} = \overline{(-a)}$ i $\mathbb{Z}/(11)$ hvor a er beregnet ved skalarproduktet

$$a = (3, 7, 6, 1, 8, 9, 4, 5, 2) \cdot (a_1, \ldots, a_9)$$

Det siste sifferet er gitt på tilsvarende måte ved at $a_{11} = \overline{(-b)}$ i $\mathbb{Z}/(11)$ hvor

$$b = (5, 4, 3, 2, 7, 6, 5, 4, 3, 2) \cdot (a_1, \ldots, a_{10})$$

Anta nå at vi har oppgitt et 11-sifret personnummer hvor det er en feil i ett av de 9 første sifferene. La (A, B) være de to kontrollsifrene. La (A', B') være de beregnede kontrollsifrene (bruk algoritmene gitt over). Sett $\alpha \equiv A' - A \ (mod\, 11)$ og $\beta \equiv B' - B + 2\alpha \ (mod\, 11)$. En feil x i siffer i gir en verdi på $\alpha = \bar{x} \cdot \bar{F}_i$ hvor $F = (3, 7, 6, 1, 8, 9, 4, 5, 2)$ er vektene som beregner a_{10} og en verdi på $\beta = \bar{x} \cdot \bar{G}_i$ hvor $G = (5, 4, 3, 2, 7, 6, 5, 4, 3, 2)$ beregner a_{11}. Løser vi ut x av disse to ligningene og setter uttrykkene lik hverandre får vi

$$\beta \bar{G}_i^{-1} = \alpha \bar{F}_i^{-1}$$

eller

$$\alpha^{-1}\beta = \bar{F}_i^{-1}\bar{G}_i$$

Vi kaller høyresiden for H og beregner den for hver i. Dette gir

$$H = (H_1, \ldots, H_9) = (\bar{9}, \bar{10}, \bar{6}, \bar{2}, \bar{5}, \bar{8}, \bar{4}, \bar{3}, \bar{7})$$

Dermed kan vi finne ut hvilken i feilen sitter i. Deretter bruker vi funksjonen

$$\bar{F}^{-1} = (\bar{F}_1^{-1}, \ldots, \bar{F}_9^{-1}) = (\bar{4}, \bar{8}, \bar{2}, \bar{1}, \bar{7}, \bar{5}, \bar{3}, \bar{9}, \bar{6})$$

som kombinert med formelen $\bar{x} = \alpha \cdot \bar{F}_i^{\,-1}$ gir oss avviket. Vi skal illustrere hele prossessen med et konkret eksempel. Anta at vi har fått oppgitt personnummeret 260482-08697. Vi skal sjekke nummeret for feil og (forhåpentligvis) rette feilen (hvis det bare er en). De beregnede kontrollsifferene (fra de gitte 9) er $1, 3$. Det gir $\alpha = \bar{8}$ og $\beta = \bar{20} = \bar{9}$ og dermed $\alpha^{-1} = \bar{7}$ og $H = \bar{63} = \bar{8}$ Dette gir oss $i = 6$ i henhold til lista over. Størrelsen på feilen er gitt ved $\bar{x} = \bar{8} \cdot \bar{5} = \bar{7}$. Siden observert siffer er $A' = 2$ får vi $\bar{2} - \bar{A} = \bar{7}$ eller $A = 6$. Korrekt fødselsnummer er derfor 260486-08697. □

Oppgaver

3.1 Lag en addisjonstabell og en multiplikasjonstabell for $\mathbb{Z}/(7)$.

3.2 Løs ligningen $\overline{27} \cdot \bar{x} = \bar{5}$ i $\mathbb{Z}/(31)$.

3.3 Finn de inverse elementene til

a) $\overline{49}$ i $\mathbb{Z}/(61)$

b) alle elementene i $\mathbb{Z}/(11)$, bortsett fra $\bar{0}$.

3.4 Løs ligningen $\overline{770} \cdot \bar{x} = \bar{7}$ i $\mathbb{Z}/(1173)$. Finnes det mer enn en løsning?

3.5

a) Bruk Euklids algoritme til å finne største felles divisor til 784 og 36.
b) Finnes det hele tall x, y slik at $784x + 36y = 2$?
c) Finn hele tall x, y slik at $784x + 36y = 12$.

3.6

a) Skriv 8 som en lineærkombinasjon av 120 og 256.
b) Finn alle løsninger til $\overline{120}\overline{x} = \overline{8}$ i $\mathbb{Z}/(256)$.

3.7 Finn alle løsningene til $\overline{35}\,\bar{x} = \bar{7}$ i $\mathbb{Z}/(49)$.

3.8

a) Skriv 2 som en lineærkombinasjon av 110 og 48.
b) Finn alle løsninger av

$$\overline{48} \cdot \bar{x} = \bar{2} \quad \text{i } \mathbb{Z}/(110)$$

3.9

a) Skriv 1 som en lineærkombinasjon av 19 og 11 og bruk resultatet til å finne $\overline{11}^{-1}$ i $\mathbb{Z}/(19)$.
b) Løs ligningssystemet

$$\begin{aligned} \overline{2} \cdot \overline{x} + \overline{y} &= \overline{2} \\ \overline{7} \cdot \overline{x} - \overline{2} \cdot \overline{y} &= \overline{4} \end{aligned}$$

i $\mathbb{Z}/(19)$.

3.10

a) Vis at hvis n er odde, så er $n^2 \equiv 1 \pmod 4$, og hvis n er like, så er $n^2 \equiv 0 \pmod 4$.
b) Vis at en sum $m^2 + n^2$ aldri kan være kongruent med 3 (mod 4).

3.11 Vis at dersom $7 \mid (a^2 + b^2)$, så må både $7 \mid a$ og $7 \mid b$.
(*Hint*: Betrakt a^2 og b^2 modulo 7).

3.12 Bevis noen av punktene i setning 3.4.

3.13

a) Vis at 9 deler et tall hvis og bare hvis det deler tverrsummen.
b) Den *alternerende tverrsummen* til et naturlig tall n er definert som

$$\alpha_0 - \alpha_1 + \alpha_2 - \alpha_3 + \cdots + (-1)^k \alpha_k$$

der $n = \alpha_k \alpha_{k-1} \alpha_{k-2} \cdots \alpha_1 \alpha_0$ er tallet skrevet i titallsystemet. Vis at 11 deler n hvis og bare hvis 11 deler den alternerende tverrsummen.
c) Undersøk om 778431276659113 er delelig med 3, 9 eller 11.

3.14 Vis at ligningen $3x^2 + 2 = y^2$ ikke har noen heltallige løsninger x, y.
(*Hint*: Vurder de mulige verdiene y kan ha modulo 3).

3.15

a) Vis at kvadratet av et oddetall er kongruent med 1 modulo 8.
b) Vis at ingen heltall $k \equiv 7 \pmod 8$ kan skrives som en sum av tre kvadrattall.

3.16 Sjekk den siste påstanden i beviset for korollar 3.9, nemlig at løsningene for $k = 0, 1, \ldots, d-1$ er de eneste ulike løsningene ligningen har.

3.17 I denne oppgaven er $m_1, m_2, \ldots, m_r$ relativt primiske, naturlige tall (m_i og m_j har altså ingen felles faktorer når $i \neq j$). Vi skal vise at for alle hele tall

$a_1, a_2, \ldots, a_r$, finnes det et helt tall x slik at

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

(dette kalles *kinesisk restteorem*).

a) La $M = m_1 m_2 \ldots m_r$ og sett $M_i = \frac{M}{m_i}$. Vis at $M_i \equiv 0 \pmod{m_j}$ når $i \neq j$.

b) Vis at for hver i har kongruensen

$$M_i y_i = 1 \pmod{m_i}$$

en løsning.

c) La y_i være som i b) og vis at

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + \cdots a_r y_y M_r$$

tilfredsstiller alle kongruensene $x = a_i \pmod{m_1}$ i begynnelsen av oppġaven.

d) Finn et helt tall x slik at

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

4. Fermats lille teorem, Eulers teorem og Wilsons teorem

De regnereglene vi hittil har sett på i $\mathbb{Z}/(t)$, er regler som restklasseringen har arvet fra $\mathbb{Z}$. Men det finnes også nye regneregler i $\mathbb{Z}/(t)$ som ikke har noen motsvarighet i $\mathbb{Z}$. En av de enkleste og nyttigste av disse reglene kalles gjerne "Fermats lille teorem". Det forutsetter at modulusen t er et primtall, og for å markere det skal vi skrive $\mathbb{Z}/(p)$ istedenfor $\mathbb{Z}/(t)$.

4.1 Fermats Lille Teorem: Anta at p er et primtall og at $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$. Da er

$$\bar{a}^{p-1} = \bar{1}$$

Bevis: $\mathbb{Z}/(p)$ består av $p-1$ ikke-null elementer: $\bar{1}, \bar{2}, \cdots, \overline{(p-1)}$. Multipliserer vi hvert av disse elementene med $\bar{a}$, får vi også $p-1$ ikke-null elementer

$$\bar{a}\bar{1}, \bar{a}\bar{2}, \cdots, \bar{a}\overline{(p-1)},$$

og siden forkortningsregelen gjelder, må disse være forskjellige. De to mengdene

$$\{\bar{1}, \bar{2}, \cdots, \overline{p-1}\} \quad \text{og} \quad \{\bar{a}\bar{1}, \bar{a}\bar{2}, \cdots, \bar{a}\overline{(p-1)}\}$$

må derfor ha de samme elementene (bortsett fra at rekkefølgen kan være en annen). Multipliserer vi sammen, får vi

$$\begin{aligned}&\bar{1} \cdot \bar{2} \cdot \cdots \cdot \overline{(p-1)} = (\bar{a} \cdot \bar{1}) \cdot (\bar{a} \cdot \bar{2}) \cdot \cdots \cdot (\bar{a}(\overline{p-1})) = \\ &= \bar{a}^{p-1} \cdot \bar{1} \cdot \bar{2} \cdot \cdots \cdot \overline{(p-1)}\end{aligned}$$

Vi forkorter med $\bar{1} \cdot \bar{2} \cdot \cdots \cdot \overline{(p-1)}$ og får teoremet. □

Forutsetningen om at $\bar{a} \neq \bar{0}$ i Fermats lille teorem kan av og til være litt brysom, og det kan da være bedre å bruke en følgesetning:

4.2 Korollar. Dersom p er et primtall, er

$$\bar{a}^p = \bar{a}$$

for alle $\bar{a} \in \mathbb{Z}/(p)$.

Bevis: Dersom $\bar{a} = \bar{0}$, er begge sider i formelen null, og dersom $\bar{a} \neq 0$, multipliserer vi bare formelen i Fermats lille teorem med $\bar{a}$. □

La oss se et enkelt eksempel på hva Fermats teorem kan brukes til:

4.3 Eksempel. Vis at dersom n ikke er delelig med 13, så er $7n^{12}+6$ delelig med 13.

Dersom $13 \not| n$, så er $n^{12} \equiv 1 \pmod{13}$. Altså er

$$7n^{12} + 6 \equiv 7 + 6 \equiv 13 \equiv 0 \pmod{13}$$

□

Det neste eksemplet er av samme type, men en smule mer komplisert.

4.4 Eksempel. Vi skal vise at $20n^7 + 14n^5 + n$ er delelig med 35 for alle n.

Siden $35 = 5 \cdot 7$, er det nok å vise at uttrykket alltid er delelig med 5 og 7. Bruker vi korollar 4.2 med p lik henholdsvis 5 og 7, får vi

$$20n^7 + 14n^5 + n \equiv 0n^7 + 14n + n \equiv 15n \equiv 0 \pmod 5$$
$$20n^7 + 14n^5 + n \equiv 20n + 0n^5 + n \equiv 21n \equiv 0 \pmod 7),$$

som er nøyaktig det vi skulle vise. □

Hva skjer med Fermats lille teorem dersom vi arbeider modulo et sammensatt tall t og ikke modulo et primtall p? Prøver vi å gjenta beviset i dette tilfellet, ser vi fort at det bryter sammen på et par punkter - for det første vil ikke elementene $\bar{a}\bar{1}, \bar{a}\bar{2}, \cdots, \overline{a(t-1)}$ være forskjellige med mindre a og t er innbyrdes primiske (husk setning 3.6), og for det andre kan vi ikke forkorte med $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdot ... \overline{(t-1)}$ i ligningen

$$\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{(t-1)} = \bar{a}^{t-1} \cdot \bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{(t-1)}$$

fordi dette produktet ikke er innbyrdes primisk med t. Disse observasjonene antyder at vi kanskje kan redde resonnementet ved å innskrenke oss til å se på elementer som er innbyrdes primiske med t.

Vi begynner med en definisjon:

4.5 Definisjon. *Eulers ϕ-funksjon* $\phi : \mathbb{N} \to \mathbb{N}$ er gitt ved

$$\phi(t) = \text{antall naturlige tall } n \text{ slik at } n \leq t \text{ og } (n,t) = 1$$

Legg merke til at dersom p er et primtall, så er $\phi(p) = p - 1$.

4.6 Eulers teorem. Anta a og t er innbyrdes primiske. Da er

$$\bar{a}^{\,\phi(t)} = \bar{1} \quad \text{i } \mathbb{Z}/(t)\,.$$

Bevis: La $a_1, a_2, \cdots, a_{\phi(t)}$ være de naturlige tallene mindre enn eller lik t som er innbyrdes primiske med t. Ifølge setning 3.6 er elementene

$$\bar{a}\bar{a}_1, \bar{a}\bar{a}_2, \cdots, \bar{a}\bar{a}_{\phi(t)}$$

også forskjellige, og siden de også må være innbyrdes primiske[1] med t, er mengdene

$$\{\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_{\phi(t)}\} \quad \text{og} \quad \{\bar{a}\bar{a}_1, \bar{a}\bar{a}_2, \cdots, \bar{a}\bar{a}_{\phi(t)}\}$$

like (bortsett fra rekkefølgen på elementene). Multipliserer vi sammen elementene, får vi

$$\bar{a}_1 \cdot \bar{a}_2 \cdots \bar{a}_{\phi(t)} = \bar{a}^{\phi(t)} \cdot \bar{a}_1 \cdot \bar{a}_2 \cdots \bar{a}_{\phi(t)}.$$

[1]Legg merke til at dersom et tall c er innbyrdes primisk med t, vil også alle tall $c' \equiv c \pmod t$ være innbyrdes primiske med t. Det gir derfor mening å si at restklassen $\bar{c}$ er innbyrdes primisk med t.

Siden $a_1 a_2 \cdots a_{\phi(t)}$ er innbyrdes primisk med t, kan vi forkorte og få

$$\bar{a}^{\phi(t)} = \bar{1}.$$

□

Vi skal til slutt se på en annen regneregel som er spesiell for restklasseringer.

4.7 Wilsons Teorem. La p være et primtall. Da er

$$\overline{(p-1)!} = -\bar{1} \quad \text{i } \mathbb{Z}/(p)$$

Bemerkning: Hvorfor i all verden skulle man være interessert i å regne ut $\overline{(p-1)!}$? Siden

$$\overline{(p-1)!} = \bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{(p-1)}$$

er produktet av alle ikke-null elementer i $\mathbb{Z}/(p)$, er det faktisk en størrelse som dukker opp ganske ofte (vi har allerede støtt på den i beviset for Fermats lille teorem).

I beviset for Wilsons teorem bruker vi følgende lemma:

4.8 Lemma. La p være et primtall. Da er $\bar{1}$ og $\overline{-1}$ de eneste restklassene i $\mathbb{Z}/(p)$ som er sine egne inverser (dvs. som er slik at $\bar{x}^{-1} = \bar{x}$).

Bevis: Det er klart at $\bar{1}$ og $\overline{-1}$ er sine egne inverser. Dersom $\bar{x}$ er en annen restklasse som er sin egen invers, må $\bar{x}^2 = \bar{1}$, dvs. $\bar{x}^2 - \bar{1} = \bar{0}$. Faktoriserer vi, får vi

$$(\bar{x} - \bar{1})(\bar{x} + \bar{1}) = \bar{0}.$$

Siden $\mathbb{Z}/(p)$ ikke har null-divisorer, betyr dette at $\bar{x} - \bar{1} = \bar{0}$ eller $\bar{x} + \bar{1} = \bar{0}$, og følgelig er $\bar{x} = \bar{1}$ eller $\bar{x} = -\bar{1} = \overline{-1}$. □

Bevis for Wilsons teorem: For $p = 2$, har vi

$$\overline{(p-1)!} = \bar{1}! = \bar{1} = \overline{-1}.$$

For $p > 2$, kan vi skrive mengden av ikke-null elementer i $\mathbb{Z}/(p)$ som en disjunkt union

$$\{\overline{-1}\} \cup \{\bar{1}\} \cup \{\bar{x}_1, \bar{x}_1^{-1}\} \cup \{\bar{x}_2, \bar{x}_2^{-1}\} \cup \cdots \cup \{\bar{x}_m, \bar{x}_m^{-1}\}$$

der $m = \frac{p-3}{2}$. Multipliserer vi, får vi

$$(\overline{-1}) \cdot (\bar{1})(\bar{x}_1 \cdot \bar{x}_1^{-1})(\bar{x}_2 \cdot \bar{x}_2^{-1}) \cdots (\bar{x}_m \cdot \bar{x}_m^{-1}) = \overline{-1}$$

som viser at produktet av alle ikke-null elementer i $\mathbb{Z}/(p)$ er $\overline{-1}$. Dette produktet kan også skrives

$$\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{(p-1)} = \overline{(p-1)!},$$

og beviset er fullført. □

Oppgaver

4.1 La n være et helt tall.

a) Vis at dersom n ikke er delelig med 5, så er $n^8 + 2n^6 + 3n^2 + 4$ delelig med 5.

b) Vis at $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ er et helt tall.
c) Vis at $5n^7 - 7n^5 + 2n$ er delelig med 35 for alle $n \in \mathbb{N}$.
d) Vis at $n^7 - n$ er delelig med 42 for alle $n \in \mathbb{Z}$.

4.2 Anta at p er et primtall og at k_1, k_2 er to naturlige tall slik at $k_1 k_2 \equiv 1$ modulo $p-1$. Vis at

$$\bar{a}^{k_1 k_2} = \bar{a}$$

for all $\bar{a} \in \mathbb{Z}/(p)$.

4.3 La a være et helt tall. Vis at

$$n \,|\, (a^{13} - a)$$

gjelder for $n = 2, 3, 5, 7, 13$. Hva kan du si når $n = 1, 4, 6, 8, 9, 10, 11, 12$?

4.4 Vis at for ethvert primtall p, bortsett fra 2 og 5, så finnes det et tall på formen 111...1 (dvs. med alle sifrene lik 1) som p går opp i. (*Hint*: Bruk Fermats lille teorem til først å finne tall av typen 999...9).

4.5 Vis at dersom p og q er to ulike primtall, så er $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

4.6 La k, $n \in \mathbb{Z}$ være slik at $0 \leq k \leq n$.
Husk at *n-fakultet* er definert ved $0! = 1$, $1! = 1$, $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$ når $n \geq 2$, og at *binomialkoeffisientene* er definert ved $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

a) Vis at $\binom{n}{0} = \binom{n}{n} = 1$ og at $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ for alle $0 < k < n$.
b) Bevis ved induksjon *binomialformelen*:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

c) La $r \in \mathbb{N}$. Vis at $a \equiv b \pmod{r^n}$ medfører at $a^r \equiv b^r \pmod{r^{n+1}}$ (*Hint*: Sett $a = b + tr^n$ og beregn a^r ved hjelp av binomialformelen).
d) La p være et primtall. Vis formelen $n^p \equiv n \pmod{p}$ for alle $n \in \mathbb{N}$ ved induksjon.
e) Bruk d) til å vise Fermats lille teorem.

4.7 Beregn $\phi(n)$ for $n = 1, 2, 3, \cdots, 24$.

4.8

a) Vis at dersom p er et primtall og $n \in \mathbb{N}$, så er $\phi(p^n) = p^{n-1}(p-1)$.
b) Vis at dersom $m, n \in \mathbb{N}$ og $(m, n) = 1$, så er $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.
c) Finn $\phi(4851)$.
d) Dersom $n \in \mathbb{N}, n \geq 2$, har primtallsfaktorisering $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, hva er $\phi(n)$?

4.9 Vis at $61! + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$.

4.10 La $n \in \mathbb{N}$, $n \geq 2$.
a) Vis at $(n-1)! \equiv 0 \pmod{n}$ når n ikke er et primtall og heller ikke lik 4.
b) Vis at $(n-1)! + 1$ er delelig med n hvis og bare hvis n er et primtall.

4.11 Vis at dersom p er et odde primtall, så er

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

5. Kvadratiske rester

I kapittel 3 så vi at lineære ligninger

$$\bar{a} \cdot \bar{x} = \bar{b}$$

alltid har en løsning i $\mathbb{Z}/(p)$ dersom p er et primtall og $\bar{a} \neq \bar{0}$. I dette kapitlet skal vi studere den aller enkleste annengradsligningen

$$\bar{x}^2 = \bar{a}$$

i $\mathbb{Z}/(p)$. Dersom $p = 2$, har denne ligningen alltid en løsning (dersom $\bar{a} = \bar{0}$, er $\bar{x} = \bar{0}$ en løsning, og dersom $\bar{a} = \bar{1}$, er både $\bar{x} = \bar{1}$ og $\bar{x} = \overline{-1}$ løsninger), men for odde primtall er ikke dette tilfellet; f.eks. ser vi at ligningen har løsninger i $\mathbb{Z}/(3)$ hvis $\bar{a} = \bar{0}$ eller $\bar{a} = \bar{1}$, men ikke hvis $\bar{a} = \bar{2}$.

5.1 Definisjon. Et element $\bar{a} \in \mathbb{Z}/(p)$ kalles en *kvadratisk rest* dersom det finnes en $\bar{x} \in \mathbb{Z}/(p)$ slik at $\bar{x}^2 = \bar{a}$.

5.2 Setning. Anta at $p > 2$ er et primtall og at $\bar{a} \neq \bar{0}$ er en kvadratisk rest i $\mathbb{Z}/(p)$. Da finnes det nøyaktig to elementer $\bar{x}$ i $\mathbb{Z}/(p)$ slik at $\bar{x}^2 = \bar{a}$.

Bevis: Siden $\bar{a}$ er en kvadratisk rest, finnes det en restklasse $\bar{x}$ slik at $\bar{x}^2 = \bar{a}$. Da er også $\overline{(-x)}^2 = \bar{a}^2$, og siden p er odde, er $\bar{x} \neq \overline{-x}$ (sjekk dette!).

Anta nå at $\bar{y}$ er et element slik at $\bar{y}^2 = \bar{a}$. Da er $\bar{x}^2 = \bar{y}^2$, så

$$\bar{0} = \bar{y}^2 - \bar{x}^2 = (\bar{y} - \bar{x})(\bar{y} + \bar{x})$$

Siden $\mathbb{Z}/(p)$ ikke har null-divisorer, må enten $\bar{y} - \bar{x} = \bar{0}$ eller $\bar{y} + \bar{x} = \bar{0}$, og følgelig er $\bar{y} = \bar{x}$ eller $\bar{y} = \overline{-x}$. □

5.3 Setning. Anta at $p > 2$ er et primtall. Av de $p - 1$ ikke-null elementene i $\mathbb{Z}/(p)$ er da nøyaktig halvparten kvadratiske rester.

Bevis: I følge forrige setning er de $p - 1$ uttrykkene

$$\bar{1}^2, \bar{2}^2, \bar{3}^2, \cdots, \overline{(p-1)}^2$$

like to og to, og dermed finnes det $\frac{p-1}{2}$ kvadratiske rester. □

Denne setningen forteller oss at $\mathbb{Z}/(p)$ ligner litt på mengden $\mathbb{R}$ av reelle tall. Også i $\mathbb{R}$ har ligningen $x^2 = a$ løsninger for "halvparten" av de ikke-null elementene a, nemlig for positive a. Men for hvilke $\bar{a}$ har ligningen løsning i $\mathbb{Z}/(p)$? Det er flere måter å besvare dette spørsmålet på, og vi skal bevise et kriterium som går tilbake til Euler. Først en enkel observasjon:

5.4 Setning. Anta at $p > 2$ er et primtall og at $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$. Da er $\bar{a}^{\frac{p-1}{2}}$ lik enten $\bar{1}$ eller $\overline{-1}$.

Bevis: La $\bar{x} = \bar{a}^{\frac{p-1}{2}}$. I følge Fermats lille teorem er

$$\bar{x}^2 = (\bar{a}^{\frac{p-1}{2}})^2 = \bar{a}^{p-1} = \bar{1}.$$

Altså er $\bar{x} = \bar{a}^{\frac{p-1}{2}}$ en løsning av ligningen $\bar{x}^2 = \bar{1}$ som bare har løsningene $\bar{1}$ og $\overline{-1}$. □

5.5 Eulers Kriterium. Anta at $p > 2$ er et primtall og at $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$. Da er $\bar{a}$ en kvadratisk rest hvis og bare hvis $\bar{a}^{\frac{p-1}{2}} = \bar{1}$.

Bevis. Anta først at $\bar{a}$ er en kvadratisk rest og $\bar{x}$ er slik at $\bar{x}^2 = \bar{a}$. Da er $\bar{x} \neq \bar{0}$ siden $\bar{a} \neq \bar{0}$, så $\bar{a}^{\frac{p-1}{2}} = (\bar{x}^2)^{\frac{p-1}{2}} = \bar{x}^{p-1} = \bar{1}$ ved Fermats lille teorem. Dermed er den ene implikasjonen bevist.

La oss så anta $\bar{a}$ *ikke* er en kvadratisk rest. Vi skal bruke nesten samme idé som i beviset for Wilsons teorem. For hver $\bar{x} \in \mathbb{Z}/(p), \bar{x} \neq \bar{0}$, vet vi at det finnes nøyaktig ett element $\bar{x}' \in \mathbb{Z}/(p)$ slik at

$$\bar{x} \cdot \bar{x}' = \bar{a},$$

nemlig $\bar{x}' = \bar{x}^{-1}\bar{a}$. Det er da klart at dersom $\bar{x} \neq \bar{y}$, så er $\bar{x}' \neq \bar{y}'$.

Siden $\bar{a}$ *ikke* er en kvadratisk rest, vet vi videre at $\bar{x} \neq \bar{x}'$ for alle $\bar{x} \in \mathbb{Z}/(p)$, $\bar{x} \neq \bar{0}$. Dermed kan mengden $\{\bar{1}, \bar{2}, \cdots, \overline{p-1}\}$ skrives som en disjunkt union

$$\{\bar{x}_1, \bar{x}_1'\} \cup \{\bar{x}_2, \bar{x}_2'\} \cup \cdots \cup \{\bar{x}_{\frac{p-1}{2}}, \bar{x}'_{\frac{p-1}{2}}\}.$$

Ved å multiplisere sammen alle elementene får vi at

$$\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{(p-1)} = (\bar{x}_1 \cdot \bar{x}_1')(\bar{x}_2 \cdot \bar{x}_2') \cdots (\bar{x}_{\frac{p-1}{2}} \cdot \bar{x}'_{\frac{p-1}{2}}) = \bar{a}^{\frac{p-1}{2}}$$

I følge Wilsons teorem er $\bar{1} \cdot \bar{2} \cdot \bar{3} ... \overline{(p-1)} = -\bar{1}$, så dette gir oss at

$$\bar{a}^{\frac{p-1}{2}} = -\bar{1}.$$

Dermed er den motsatte implikasjonen vist. □

I praksis er ikke Eulers kriterium særlig effektivt for å avgjøre om en gitt restklasse er en kvadratisk rest fordi vi må utføre altfor mange multiplikasjoner underveis. Et virkelig effektivt redskap får man først når man beviser den så kalte kvadratiske resiprositetssatsen, men den har vi ikke plass til å komme innpå her. La oss likevel se på hvordan Eulers kriterium brukes i praksis.

5.6 Eksempel: Er $\bar{7}$ en kvadratisk rest i $\mathbb{Z}/(13)$?
Vi kan da sjekke om $\bar{7}^6$ er $\bar{1}$ eller $\overline{-1}$. Observer først at $\bar{7}^6 = (\overline{49})^3 = (\overline{-3})^3$. Dermed er

$$\bar{7}^6 = (\overline{-3})^3 = -\overline{27} = \overline{-1},$$

som viser at $\bar{7}$ ikke er en kvadratisk rest. □

Dersom $p > 2$ er et primtall, så er enten $p \equiv 1 \pmod 4$ eller $p \equiv 3 \pmod 4$. I det første tilfellet er $\frac{p-1}{2}$ et partall, i det andre tilfellet et oddetall. Vi har derfor følgende viktige spesialtilfelle av Eulers kriterium:

5.7 Korollar. La p være et primtall. Da er $\overline{-1}$ en kvadratisk rest i $\mathbb{Z}/(p)$ hvis og bare hvis $p = 2$ eller $p \equiv 1 \pmod 4$.

Bevis: For $p = 2$, er $\overline{-1} = \bar{1}$ som opplagt er en kvadratisk rest. For $p > 2$, har vi

$$(-1)^{\frac{p-1}{2}} = 1 \text{ hvis } p \equiv 1 \pmod 4$$

mens

$$(-1)^{\frac{p-1}{2}} = -1 \text{ hvis } p \equiv 3 \pmod 4$$

og korollaret følger fra Eulers kriterium. □

Vi har nå redskap til å avslutte det prosjektet vi startet med setning 2.6.

5.8 Setning. Det finnes uendelig mange primtall som er kongruente med 1 (mod 4).

Bevis. Anta for motsigelse at det bare finnes endelig mange primtall $p_1, p_2, \cdots, p_n$ som er kongruente med 1 (mod 4). La

$$N = (2p_1p_2 \cdots p_n)^2 + 1.$$

Det er innlysende at $p_i \not| N$ for alle i. La nå p være en primfaktor i N. Da er

$$N = (2p_1p_2 \cdots p_n)^2 + 1 \equiv 0 \pmod p,$$

og dette betyr at $\bar{x} = \overline{2p_1p_2 \cdots p_n}$ er en løsning av ligningen $\bar{x}^2 = \overline{-1}$ i $\mathbb{Z}/(p)$. I følge Korollar 5.7 må derfor $p = 2$ eller $p \equiv 1 \pmod 4$. Siden $2 \not| N$, må $p \equiv 1 \pmod 4$, og siden $p|N$, må $p \neq p_i$ for alle i. Vi har altså funnet et primtall p som er kongruente med 1 (mod 4), og som er forskjellig fra $p_1, p_2, \cdots, p_n$, og dermed har vi selvmotsigelsen vi var på jakt etter. □

Vi skal avslutte denne seksjonen med å se på mer generelle annengradsligninger i $\mathbb{Z}/(p)$, $p > 2$. Det viser seg at vi kan bruke den samme fremgangsmåten som for vanlige annengradsligninger. Vi begynner med ligningen

$$\bar{a}\bar{x}^2 + \bar{b}\bar{x} + \bar{c} = \bar{0}$$

der $\bar{a} \neq \bar{0}$. Siden $\mathbb{Z}/(p)$ ikke har nulldivisorer, kan vi gange med $\bar{4}\bar{a}$ og få

$$\bar{4}\bar{a}^2\bar{x}^2 + \bar{4}\bar{a}\bar{b}\bar{x} + \bar{4}\bar{a}\bar{c} = \bar{0}$$

Neste trinn er å fullføre kvadratet. Adderer og subtraherer vi $\bar{b}^2$, får vi

$$\bar{4}\bar{a}^2\bar{x}^2 + \bar{4}\bar{a}\bar{b}\bar{x} + \bar{b}^2 - \bar{b}^2 + \bar{4}\bar{a}\bar{c} = \bar{0}$$

som også kan skrives

$$(\bar{2}\bar{a}\bar{x} + \bar{b})^2 = \bar{b}^2 - \bar{4}\bar{a}\bar{c}$$

Dette viser at ligningen har en løsning hvis og bare hvis $\bar{b}^2 - 4\bar{a}\bar{c}$ enten er $\bar{0}$ eller en kvadratisk rest, og i så fall er løsningene

$$\bar{x} = (\bar{2}\bar{a})^{-1}\left(-\bar{b} \pm \sqrt{\bar{b}^2 - \bar{4}\bar{a}\bar{c}}\right)$$

der $\pm\sqrt{\bar{b}^2 - \bar{4}\bar{a}\bar{c}}$ står for de to kvadratrøttene til $\bar{b}^2 - \bar{4}\bar{a}\bar{c}$ i $\mathbb{Z}/(p)$. Tolker vi divisjon på den naturlige måten, ender vi opp med den vanlige formelen

$$\bar{x} = \frac{-\bar{b} \pm \sqrt{\bar{b}^2 - \bar{4}\bar{a}\bar{c}}}{\bar{2}\bar{a}}$$

for løsningen til annengradsligninger. Vi oppsummerer dette i en setning:

5.9 Setning. Anta at $p > 2$ er et primtall. Da har annengradsligningen

$$\bar{a}\bar{x}^2 + \bar{b}\bar{x} + \bar{c} = \bar{0}$$

løsning i $\mathbb{Z}/(p)$ hvis og bare hvis $\bar{b}^2 - \bar{4}\bar{a}\bar{c}$ enten er $\bar{0}$ eller en kvadratisk rest i $\mathbb{Z}/(p)$, og i så fall er løsningene gitt ved

$$\bar{x} = \frac{-\bar{b} \pm \sqrt{\bar{b}^2 - \bar{4}\bar{a}\bar{c}}}{\bar{2}\bar{a}}$$

5.10 Eksempel: La oss se om vi kan løse

$$\bar{x}^2 + \bar{2}\bar{x} + \bar{5} = \bar{0}$$

i $\mathbb{Z}/(41)$. Annengradsformelen gir oss

$$\bar{x} = \frac{-\bar{2} \pm \sqrt{\bar{2}^2 - \bar{4}\cdot\bar{1}\cdot\bar{5}}}{\bar{2}} = \frac{-\bar{2} \pm \sqrt{-\overline{16}}}{\bar{2}} = \frac{-\bar{2} \pm \sqrt{\overline{25}}}{\bar{2}} = \frac{-\bar{2} \pm \bar{5}}{\bar{2}} = \begin{cases} \frac{\bar{3}}{\bar{2}} \\ \\ \frac{\overline{-7}}{\bar{2}} \end{cases}$$

Siden $\bar{3} = \overline{44}$ og $\overline{-7} = \overline{34}$ i $\mathbb{Z}/(41)$, kan løsningene skrives $\bar{x}_1 = \frac{\bar{3}}{\bar{2}} = \frac{\overline{44}}{\bar{2}} = \overline{22}$ og $\bar{x}_2 = \frac{\overline{-7}}{\bar{2}} = \frac{\overline{34}}{\bar{2}} = \overline{17}$. □

Oppgaver

5.1 Finn de kvadratiske restene i $\mathbb{Z}/(13)$.

5.2 For hvilke primtall p har kongruensen

$$\bar{x}^2 + \bar{2}\bar{x} + \bar{2} \equiv \bar{0} \pmod{p}$$

en løsning?

5.3 Ligningen for det gyldne snitt er

$$\bar{x}^2 - \bar{x} - \bar{1} = \bar{0}$$

Vi skal se på denne ligningen i $\mathbb{Z}/(p)$ for $p = 7$ og $p = 11$.

a) Finn alle kvadratiske rester i $\mathbb{Z}/(7)$ og i $\mathbb{Z}/(11)$.
b) Finn alle løsninger av ligningen i $\mathbb{Z}/(7)$ og i $\mathbb{Z}/(11)$.

5.4 Finn alle løsninger til $\bar{2}\bar{x}^2 - \bar{x} + \bar{2} = \bar{0}$ i $\mathbb{Z}/(19)$.

5.5 Finn de kvadratiske restene i $\mathbb{Z}/(8)$. Hvor mange kvadratrøtter har $\bar{1}$? Hvorfor fungerer ikke beviset for setning 5.2 i dette tilfellet?

5.6 La p være et odde primtall.

a) Vis at

$$A = \{\bar{x}^2 : \bar{x} \in \mathbb{Z}/(p)\} \text{ og } B = \{-\bar{1} - \bar{y}^2 : y \in \mathbb{Z}/(p)\}$$

har nøyaktig $\frac{p+1}{2}$ elementer hver.

b) Vis at A og B har minst ett felles element.

c) Vis at det finnes elementer $\bar{x}, \bar{y} \in \mathbb{Z}/(p)$ slik at

$$\bar{x}^2 + \bar{y}^2 = \overline{-1}\,.$$

d) Hvilke elementer $\bar{b} \in \mathbb{Z}/(p)$ kan skrives som en sum

$$\bar{b} = \bar{u}^2 + \bar{v}^2$$

av to kvadratiske rester?

5.7 La p være et odde primtall. Vi har sett i dette kapitlet at dersom kongruensen $x^2 \equiv -1 \pmod{p}$ er løsbar, så er $p \equiv 1 \pmod{4}$.

a) Vis at dersom $x^4 \equiv -1 \pmod{p}$ er løsbar, så er $p \equiv 1 \pmod{8}$.

b) Vis at dersom $x^8 \equiv -1 \pmod{p}$ er løsbar, så er $p \equiv 1 \pmod{16}$.

c) Formuler og bevis den naturlige generalisering av a) og b).

5.8 Anta at p er et primtall, og at $p \equiv 3 \pmod{4}$.

Vis at $(\frac{p-1}{2})! \equiv \pm 1 \pmod{p}$.

6. Kvadratsummer

Skriver vi opp de første primtallene som er kongruente med henholdsvis 1 og 3 modulo 4:

$$p \equiv 1 \pmod 4: \quad 5, 13, 17, 29, 37, 41, 53, \ldots$$
$$p \equiv 3 \pmod 4: \quad 3, 7, 11, 19, 23, 31, 43, \ldots$$

ser vi fort en forskjell; alle tallene i den første gruppen kan skrives som en sum av to kvadrater

$$5 = 1^2 + 2^2,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2,\ 29 = 2^2 + 5^2,$$
$$37 = 1^2 + 6^2,\ 41 = 4^2 + 5^2,\ 53 = 2^2 + 7^2, \ldots$$

mens ingen i den andre gruppen kan skrives på denne måten. Dette fenomenet ble observert av Albert Girard i 1632, og 22 år senere beviste Fermat at Girards observasjon gjelder helt generelt. I dette kapitlet skal vi bevise Fermats resultat pluss noen generaliseringer. La oss for enkelthets skyld bli enige om følgende språkbruk: Et tall a er en *kvadratsum* dersom det finnes $x, y \in \mathbb{Z}$ slik at $a = x^2 + y^2$ (legg merke til at vi tillater at x eller y er lik 0; det vil si at alle kvadrattall regnes som kvadratsummer).

Vi beviser først at et primtall kongruent med 3 (mod 4) ikke kan være en sum av to kvadrater. Dette viser seg å være en ren trivialitet.

6.1 Lemma. Et naturlig tall som er kongruent med 3 (mod 4) er ikke en kvadratsum.

Bevis: Dersom x er et partall, er $x^2 \equiv 0 \pmod 4$. Er x et oddetall, er $x^2 \equiv 1 \pmod 4$. En kvadratsum $x^2 + y^2$ kan derfor være kongruent med 0,1 eller 2 (mod 4) (avhengig av om ingen, ett eller to av tallene x, y er odde), men aldri kongruent med 3. □

6.2 Teorem. Et primtall p er en kvadratsum hvis og bare hvis $p = 2$ eller $p \equiv 1 \pmod 4$.

Bevis: I lys av lemma 6.1, og fordi $2 = 1^2 + 1^2$ er en kvadratsum, gjenstår det bare å vise at dersom $p \equiv 1 \pmod 4$, så er p en kvadratsum. La da K være det største hele tallet som er mindre enn $\sqrt{p}$, og la $i \in \mathbb{Z}$ være valgt slik at $\overline{i}^{\,2} = \overline{-1}$ i $\mathbb{Z}/(p)$. En slik i finnes ved korollar 5.7. Merk også at $K + 1 > \sqrt{p}$: per definisjon av K er $K + 1 \geq \sqrt{p}$, og det er ikke mulig at $K + 1 = \sqrt{p}$ siden et primtall ikke kan være et kvadrattall.

For alle hele tall u, v slik at $0 \leq u, v \leq K$ definerer vi

$$f(u, v) = u + iv.$$

Siden det finnes $(K + 1)^2 > (\sqrt{p})^2 = p$ slike par (u, v), og bare p restklasser i $\mathbb{Z}/(p)$, må det finnes *forskjellige* par (u, v) og (u', v') slik at $f(u, v)$ og $f(u', v')$ tilhører samme restklasse, dvs. slik at

$$u + iv \equiv u' + iv' \pmod p.$$

Setter vi $x = u - u'$ og $y = v' - v$, får vi

$$x \equiv iy \pmod p.$$

Siden $\bar{i}^2 = \overline{-1}$ i $\mathbb{Z}/(p)$, gir dette

$$\bar{x}^2 + \bar{y}^2 = \bar{i}^2\bar{y}^2 + \bar{y}^2 = -\bar{y}^2 + \bar{y}^2 = \bar{0}$$

i $\mathbb{Z}/(p)$, og følgelig finnes det et helt tall n slik at

$$x^2 + y^2 = np.$$

Hvis vi kan vise at $n = 1$, er vi ferdige.

La oss se på størrelsen til x og y. Siden ikke både x og y er null, må $x^2+y^2 > 0$. Dessuten er $x = u - u', y = v' - v$, der $0 \leq u, u', v, v' < \sqrt{p}$, så

$$-\sqrt{p} < x,\ y < \sqrt{p}\,.$$

Altså er

$$0 < x^2 + y^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p\,.$$

Dette betyr at $n = 1$, og beviset er ferdig. □

Vi har nå funnet ut nøyaktig hvilke *primtall* som er kvadratsummer, men vi kan selvfølgelig stille det samme spørsmålet om sammensatte tall. På grunn av det neste lemmaet er ikke dette så vanskelig når man kjenner resultatet for primtall.

6.3 Lemma. Dersom a er et produkt av kvadratsummer, så er a også en kvadratsum.

Bevis: Anta at $a = (b^2 + c^2)(d^2 + e^2)$. Da er

$$a = (bd + ce)^2 + (be - cd)^2$$

(regn ut og kontroller). Dette viser at et produkt av to kvadratsummer er en kvadratsum, og ved induksjon viser man nå lett at et produkt av n kvadratsummer også er en kvadratsum. □

La oss først se på tilfellet hvor de to delene av kvadratsummen er innbyrdes primiske.

6.4 Lemma. Anta at $a = x^2 + y^2$ der x og y ikke har felles faktorer. Da er a ikke delelig med noe primtall $p \equiv 3 \pmod 4$.

Bevis: Anta at p er et primtall som deler a; vi må vise at $p \not\equiv 3 \pmod 4$. Observer først at hverken x eller y kan være delelig med p - var den ene det, ville den andre også være det, og det strider mot antagelsen om ingen felles faktorer.

Siden $p \mid a$, er $\bar{a} = \bar{x}^2 + \bar{y}^2 = \bar{0}$ i $\mathbb{Z}/(p)$. Siden $p \nmid y$, er $\bar{y} \neq \bar{0}$, og det finnes et element $\bar{k} \in \mathbb{Z}/(p)$ slik at $\bar{k}\bar{y} = \bar{x}$. Dette gir

$$\bar{0} = \bar{x}^2 + \bar{y}^2 = \bar{k}^2\bar{y}^2 + \bar{y}^2 = (\bar{k}^2 + \bar{1})\bar{y}^2.$$

Siden $\bar{y} \neq \bar{0}$, kan vi forkorte og får da

$$\bar{k}^2 = \overline{-1},$$

som er umulig når $p \equiv 3 \pmod 4$ ved korollar 5.7. □

6.5 Lemma. Anta at a er en kvadratsum og at p er et primtall som er kongruent med 3 (mod 4). Da går p opp i a et like antall ganger (dvs. $a = p^{2m}c$ der m er et ikke-negativt helt tall og c ikke er delelig med p).

Bevis: La $a = x^2 + y^2$, la d være den største felles faktoren til x og y, og la $x_0 = x/d, y_0 = y/d$. Da har x_0 og y_0 ingen felles faktor, så $x_0^2 + y_0^2$ er ikke delelig med p ifølge foregående lemma. Siden $a = d^2(x_0^2 + y_0^2)$, betyr dette at p går opp i a like mange ganger som den går opp i d^2, altså et like antall ganger. □

Vi har nå alle de opplysningene vi trenger:

6.6 Teorem. Et naturlig tall a kan skrives som en sum av to kvadrater hvis og bare hvis hver primfaktor i a som er kongruent med 3 (mod 4) forekommer et like antall ganger.

Bevis: Fra foregående lemma vet vi at dersom en primfaktor $p \equiv 3 \pmod 4$ deler a et odde antall ganger, så er a ikke en kvadratsum. Forekommer derimot enhver slik primfaktor et like antall ganger, kan vi skrive

$$a = (p_1 p_2 \cdots p_m)^2 q_1 q_2 \cdots q_k$$

der p_i'ene er primfaktorer som er kongruente med 3 (mod 4), mens q_j'ene er primfaktorer som ikke er kongruente med 3. I følge teorem 6.2 er hver q_j en kvadratsum, og siden ethvert kvadrattall regnes som en kvadratsum, er $(p_1 p_2 \cdots p_m)^2$ også en kvadratsum. Dermed er a et produkt av kvadratsummer, og teoremet følger fra lemma 6.3. □

Et naturlig spørsmål er hva som skjer dersom vi tillater summer av mer enn to kvadrater. Kanskje kan et hvilket som helst tall skrives som en sum av tre kvadrater? Det er lett å se at så ikke er tilfellet; 7 kan ikke skrives som en slik sum, og det kan heller ikke noe annet tall som er kongruent med 7 (mod 8). Carl Friedrich Gauss (1777-1855) og Adrien Marie Legendre (1752-1833) viste at et helt tall kan skrives som en sum av tre kvadrater hvis og bare hvis det ikke er på formen $4^m(8k + 7)$. Men allerede i 1770 hadde Joseph Louis Lagrange (1736-1813) vist at ethvert naturlig tall kan skrives som en sum av *fire* kvadrater.

Man kan generalisere problemstillingen til å spørre om det for ethvert naturlig tall k finnes et tall $g(k)$ slik at alle naturlige tall kan skrives som en sum av $g(k)$ k-te potenser. (Lagranges teorem sier altså at $g(2) = 4$). Dette spørsmålet ble stilt av den engelske matematikeren Waring i 1770, men det var først i 1909 at David Hilbert (1862-1943) viste at Warings formodning var riktig. Hilberts bevis er et rent eksistensbevis som viser at $g(k)$ må finnes, men det gir ingen metode for å finne ut hvor stor $g(k)$ er. Slike estimater kom senere.

Oppgaver

6.1 Kan noen av tallene 34153 og 35819 skrives som en sum av to kvadrater?

6.2 Vis ved induksjon at dersom a er et produkt av n kvadratsummer, så er a selv en kvadratsum (dvs. fullfør beviset for lemma 6.3)

6.3

a) Vis at dersom $k \equiv 7 \pmod 8$, så kan k ikke skrives som en sum av tre kvadrater.

b) Vis at dersom 4a kan skrives som en sum av tre kvadrater, så kan a også skrives som en slik sum.
c) Vis at et tall på formen $4^m(8k+7), m, k \in \mathbb{N}$, aldri kan skrives som en sum av tre kvadrater. (Dette er den enkle delen av Gauss' resultat).

Tilsammen gir de to neste oppgavene et alternativ til den vanskeligste delen av argumentet ovenfor - beviset for at ethvert primtall som er kongruent med 1 (mod 4) er en kvadratsum. Idéen går tilbake til den franske matematikeren Charles Hermite (1822-1901).

6.4 Målet er å vise at dersom a er et reelt tall og n er et naturlig tall, så finnes det hele tall k og m slik at $1 \leq m < n$ og

$$|a - k/m| \leq \frac{1}{m(n+1)} .$$

Dette resultatet sier altså noe om hvor godt vi kan tilnærme vilkårlige reelle tall ved hjelp av brøker med begrensede nevnere. Vi skal benytte notasjonen $[b]$ for det største heltallet mindre enn eller lik b ($[b]$ kalles ofte heltallsdelen til b).

a) La $a_0, a_1, a_2, \cdots, a_n$ være tallene

$$0 \cdot a - [0 \cdot a], 1 \cdot a - [1 \cdot a], 2 \cdot a - [2 \cdot a], \cdots, n \cdot a - [n \cdot a]$$

Tenk deg at disse tallene er lagt etter hverandre etter størrelsen rundt en sirkel med omkrets 1. Vis at det må finnes to slike punkter (tilsvarende a_i og a_j) som har avstand (målt langs sirkelen) mindre enn $1/(n+1)$.
b) Vis at $a_i - a_j = (i-j) \cdot a + N$ for et helt tall N. Forklar hvorfor dette medfører at ulikheten over holder med $|k/m| = |N/(i-j)|$.

6.5 Anta at p er primtall, $p \equiv 1 \pmod 4$. La u være en løsning av kongruensen $u^2 \equiv -1 \pmod p$.

a) Vis at det finnes hele tall k og x slik at $1 \leq x \leq [\sqrt{p}]$ og

$$|-(u/p) - (k/x)| < \frac{1}{x([\sqrt{p}]+1)} .$$

b) La $y = xu + kp$. Vis at $|y| < \sqrt{p}$.
c) Vis at $0 < x^2 + y^2 < 2p$.
d) Vis at $x^2 + y^2 \equiv 0 \pmod p$.
e) Forklar hvorfor c) og d) medfører at $x^2 + y^2 = p$.

I neste oppgave skal vi gi enda et bevis for at ethvert primtall som er kongruent med 1 (mod 4) er en kvadratsum. Dette beviset skyldes den amerikanske matematikeren Don Zagier (1951-) som presterte å presentere det i én setning.

6.6 Anta at A er en ikke-tom, endelig mengde. En funksjon $i : A \to A$ kalles en *inversjon* dersom den er bijektiv og $i^{-1} = i$. Et punkt $a \in A$ kalles et *fikspunkt* for i dersom $i(a) = a$. Et (uordnet) par $\{b, c\}$ av elementer i A kalles et *inverst par* hvis $b \neq c$ og $i(b) = c, i(c) = b$.

a) Anta at $i : A \to A$ er en inversjon. Forklar at A kan skrives som en disjunkt union

$$A = \{a_1\} \cup \{a_2\} \cup \ldots \cup \{a_n\} \cup \{b_1, c_1\} \cup \{b_2, c_2\} \cup \ldots \cup \{b_k, c_k\}$$

der $a_1, a_2, \ldots, a_n$ er fikspunkter for i og $\{b_1, c_1\}, \{b_2, c_2\}, \ldots, \{b_k, c_k\}$ er inverse par. (Vi tillater at $n = 0$ eller $k = 0$ slik at det enten ikke finnes fikspunkter eller ikke finnes inverse par.)

b) Vis at dersom antall elementer i A er et like tall (partall), så har en inversjon $i : A \to A$ enten ingen eller et like antall fikspunkter. Vis at det alltid finnes en inversjon uten fikspunkter i dette tilfellet.

c) Vis at dersom antall elementer i A er et oddetall, så har en inversjon $i : A \to A$ alltid minst ett fikspunkt.

La p være et primtall slik at $p \equiv 1 \pmod 4$, og definer

$$A = \{(x, y, z) \in \mathbb{N}^3 \,:\, x^2 + 4yz = p\}$$

d) Vis at A er en ikke-tom, endelig mengde, og forklar at man kan definere en inversjon fra A til A ved $i(x, y, z) = (x, z, y)$.

e) Definer tre delmengder av A ved:

$$A_1 = \{(x, y, z) \in A \,|\, x < y - z\}$$
$$A_2 = \{(x, y, z) \in A \,|\, y - z < x < 2y\}$$
$$A_3 = \{(x, y, z) \in A \,|\, x > 2y\}$$

Vis at A_1, A_2, A_3 er en partisjon av A, dvs. at A_1, A_2, A_3 er disjunkte og at $A = A_1 \cup A_2 \cup A_3$

f) Definer en funksjon $j : A \to \mathbb{Z}^3$ ved:

$$j(x, y, z) = \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{hvis} \quad (x, y, z) \in A_1 \\ (2y - x,\ y,\ x - y + z) & \text{hvis} \quad (x, y, z) \in A_2 \\ (x - 2y,\ x - y + z,\ y) & \text{hvis} \quad (x, y, z) \in A_3 \end{cases}$$

Vis at j er en inversjon av A. (*Hint:* Sjekk først at j avbilder A_1 inn i A_3, A_2 inn i A_2 og A_3 inn i A_1).

g) Vis at $j : A \to A$ har nøyaktig ett fikspunkt (husk at $p \equiv 1 \pmod 4$).

h) Vis at den opprinnelige inversjonen i i punkt d) må ha et fikspunkt, og bruk dette til å bevise at det finnes naturlige tall x, u slik at $p = x^2 + u^2$.

Hvis du lurer på hvordan Zagier greide å presentere dette beviset i én setning, kan du ta en kikk her:

`http://www.jstor.org/stable/2323918?seq=1#page_scan_tab_contents`

7. Pythagoreiske tripler og Fermats siste teorem.

Alle som har drevet trekantberegninger med Pythagoras' setning, vet at det finnes rettvinklede trekanter med sider 3, 4 og 5, dvs.

$$3^2 + 4^2 = 5^2$$

Ganger vi hver av sidene med den samme faktoren, får vi nye relasjoner - multipliserer vi f.eks. med 2, får vi

$$6^2 + 8^2 = 10^2.$$

Men det finnes også slike relasjoner som ikke framkommer gjennom forstørrelse av den opprinnelige figuren; f.eks. er

$$5^2 + 12^2 = 13^2.$$

Et trippel x, y, z av naturlige tall kalles et *pythagoreisk trippel* dersom

$$x^2 + y^2 = z^2$$

Vi skal bruke geometrisk terminologi og kalle x og y *katetene* og z *hypotenusen* i trippelet. Vårt mål i dette kapitlet er å finne alle pythagoreiske tripler.

Dette problemet har dype historiske røtter. I 1937 tydet den kjente matematikkhistorikeren Otto Neugebauer en babylonsk leirtavle ("Plimpton 322") fra ca. 1700-1800 f.Kr. som viste seg å inneholde en tabell over Pythagoreiske tripler. Mye tyder på at denne tabellen er konstruert ut i fra identiteten

$$(p^2 - q^2)^2 + (2pq)^2 = (p^2 + q^2)^2 \tag{7.1}$$

Også pythagoréerne (ca. 500 f.Kr.) var interessert i slike tripler, og de hadde mer spesielle formler som ga mange (men ikke alle) eksempler; blant annet brukte de formelen

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

Den endelige løsningen fikk problemet hos Euklid (som sannsynligvis levde rundt 300 f.Kr.). Han viste at alle pythagoreiske tripler framkommer ved å velge passende verdier for p og q i (7.1). Problemet er også behandlet i Diofants bok "Arithmetika" fra ca. 300 e. Kr., og som vi skal se, fikk dette stor betydning for matematikkhistorien. I dette kapitlet skal vi utlede Euklids resultat, og i det siste kapitlet skal vi på noen av de følgene det fikk for tallteoriens historie.

Et pythagoreisk trippel (x, y, z) kalles *primitivt* dersom 1 er den største felles faktoren til x, y og z. Kjenner vi de primitive pythagoreiske triplene, kan vi finne alle de andre ved å multiplisere med en passende faktor. Vi kan derfor konsentrere oss om å finne de primitive triplene. Vi begynner med et lemma.

7.1 Lemma. Anta at x, y, z er et primitivt pythagoreisk trippel. Da er den ene kateten et partall og den andre et oddetall, mens hypotenusen er et oddetall.

Bevis: For $a \in \mathbb{Z}$ er

$$a^2 \equiv \begin{cases} 0 \pmod 4 & \text{for a like} \\ 1 \pmod 4 & \text{for a odde} \end{cases}$$

Dersom $x^2 + y^2 = z^2$, er det derfor bare to muligheter; enten er x, y og z alle like, eller så er z og én av katetene x og y odde. Siden x, y og z ikke har felles faktorer, er den første muligheten utelukket, og lemmaet er bevist. □

7.2 Teorem. Anta at x, y, z er et primitivt pythagoreisk trippel hvor x er den odde og y den like kateten. Da finnes det naturlige tall p, q slik at $(p, q) = 1$ og

$$x = p^2 - q^2 \ , \ y = 2pq \ , \ z = p^2 + q^2$$

Bevis: La oss først se hva p og q må være dersom disse ligningene skal holde. Adderer og subtraherer vi ligningene $z = p^2 + q^2, x = p^2 - q^2$, får vi

$$z + x = (p^2 + q^2) + (p^2 - q^2) = 2p^2$$
$$z - x = (p^2 + q^2) - (p^2 - q^2) = 2q^2,$$

som gir

$$p = \sqrt{\frac{z+x}{2}} \quad , \ q = \sqrt{\frac{z-x}{2}}.$$

Vi ser at p og q da også løser den tredje ligningen:

$$2pq = 2\sqrt{\frac{z+x}{2}}\sqrt{\frac{z-x}{2}} = \sqrt{z^2 - x^2} = y$$

Det er altså tilstrekkelig å vise at $p = \sqrt{\frac{z+x}{2}}$, $q = \sqrt{\frac{z-x}{2}}$ er hele tall, det vil si at $\frac{z+x}{2}$ og $\frac{z-x}{2}$ er kvadrattall.

Vi observerer først at siden både z og x er odde, så er $\frac{z+x}{2}$ og $\frac{z-x}{2}$ hele tall. Dessuten er

$$\frac{z+x}{2} \cdot \frac{z-x}{2} = \frac{z^2 - x^2}{4} = \frac{y^2}{4} = k^2$$

(der k er helt tall) siden y er like. Dersom r er en primfaktor i k, må r gå opp i enten $\frac{z+x}{2}$ eller $\frac{z-x}{2}$. Legg merke til at r ikke kan gå opp i begge disse faktorene, for da vil den også gå opp i summen

$$\frac{z+x}{2} + \frac{z-x}{2} = z$$

og i differensen

$$\frac{z+x}{2} - \frac{z-x}{2} = x,$$

og det er umulig siden trippelet x, y, z er primitivt.

Dette betyr at primfaktorene i k faller i to grupper; de $r_1, r_2, \cdots, r_m$ som går opp i $\frac{z+x}{2}$ og de $r'_1, r'_2, \cdots, r'_k$ som går opp i $\frac{z-x}{2}$. Altså er

$$\frac{z+x}{2} \cdot \frac{z-x}{2} = k^2 = (r_1 r_2 \cdots r_m)^2 (r'_1 r'_2 \cdots r'_k)^2,$$

og følgelig er $\frac{z+x}{2} = (r_1 r_2 \cdots r_m)^2$, $\frac{z-x}{2} = (r'_1 r'_2 \cdots r'_k)^2$. Dermed er teoremet bevist med ett lite unntak - vi har ennå ikke sjekket om p og q er innbyrdes

primiske. Men det er lett - dersom p og q hadde en felles faktor d, så ville d^2 være en felles faktor i x, y og z, og det strider mot at trippelet x, y, z er primitivt. □

Den franske matematikeren Pierre de Fermat (1601-1665) hadde for vane å gjøre tallteoretiske notater i margen til sin utgave av Diofants "Arithmetica". Ved siden av Diofants behandling av den pythagoreiske ligningen

$$x^2 + y^2 = z^2$$

skrev han i en kommentar at han hadde funnet et vidunderlig bevis for at ligningen

$$x^n + y^n = z^n$$

ikke har løsninger $x, y, z \in \mathbb{N}$ når $n \geq 3$, men at det ikke var plass til beviset i margen.

Mange matematikere forsøkte i tidens løp å gjenskape Fermats forsvunne bevis uten å lykkes, og problemet ble etterhvert et av de mest berømte i matematikken - det kalles gjerne "Fermats formodning" eller "Fermats store teorem" eller "Fermats siste teorem" (fordi det var det siste gjenværende av Fermats margproblemer).

Spesialtilfeller ble etterhvert kjent; Fermat hadde selv et gyldig bevis for $n = 4$, Euler ga et for $n = 3$, og Legendre og Dirichlet fant uavhengig av hverandre bevis for $n = 5$. Dirichlet løste også problemet for $n = 14$, og Lamé beviste det vanskeligere tilfellet $n = 7$ i 1839. I 1847 presenterte så Lamé et generelt bevis for det franske vitenskapsakademiet. Det viste seg fort at beviset var galt, men i kjølvannet utviklet det seg teknikker som gjorde at man kunne vise at dersom Fermats ligning skulle ha løsninger, måtte n være svært stor.

Det neste store framskrittet kom midt på 1980-tallet da man ble klar over den nære sammenhengen mellom Fermats formodning og såkalte elliptiske kurver. Det viste seg at flere naturlige formodninger om elliptiske kurver ville medføre Fermats formodning dersom de var sanne. Den 23. juli, 1993, la den engelske matematikeren Andrew Wiles fram en delvis løsning av en av disse formodningene (Taniyamas formodning), og dermed også et bevis for Fermats hypotese.

Alt dette er temmelig langt fra Fermats vidunderlige bevis som ikke fikk plass i margen, og bare de aller største romantikerne er vel istand til å tro at Fermat virkelig hadde et elementært bevis som alle andre har oversett. Vi kan selvfølgelig ikke se på Wiles' bevis her, men vi skal ta en kikk på det som Fermat helt klart hadde vist - nemlig tilfellet $n = 4$.

7.3 Teorem. Det finnes ikke naturlige tall x, y, z slik at

$$x^4 + y^4 = z^4$$

I virkeligheten viste Fermat et litt sterkere resultat:

7.4 Teorem. Det finnes ingen naturlige tall x, y, u slik at

$$x^4 + y^4 = u^2$$

Ved å sette $u = z^2$, ser vi at teorem 7.4 medfører teorem 7.3.

For å vise teorem 7.4 antar vi at teoremet er galt, og lar x, y, u være en løsning med minst mulig u-verdi. Strategien er å benytte denne løsningen til å produsere en løsning med enda mindre tredjekomponent, og på den måten framtvinge en selvmotsigelse. Beviset formuleres enklest gjennom en kjede av lemmaer.

7.5 Lemma. x, y og u har ingen felles faktor.

Bevis: Anta at x, y og u har en felles primfaktor t slik at $x = ta, y = tb, u = tc$. Da vil $x^4 + y^4 = u^2$ medføre $t^4a^4 + t^4b^4 = t^2c^2$, som etter forkortning gir

$$t^2(a^4 + b^4) = c^2$$

Dette betyr at $t \mid c$, så vi kan skrive $c = td$. Innsatt i ligningen ovenfor gir dette $t^2(a^4 + b^4) = t^2d^2$, det vil si

$$a^4 + b^4 = d^2.$$

Dermed har vi funnet en løsning med mindre tredjekomponent enn u, og det strider mot vår antagelse. □

Lemmaet forteller oss at (x^2, y^2, u) er et primitivt pythagoreisk trippel. Lar vi x være den odde kateten, finnes det etter teorem 7.2 hele tall p, q slik at

$$x^2 = p^2 - q^2, \quad y^2 = 2pq, \quad u = p^2 + q^2$$

der p og q er innbyrdes primiske.

7.6 Lemma. p er odde og q er like.

Bevis: Vi vet at x - og dermed x^2 - er odde. Siden $x^2 = p^2 - q^2$, må ett av tallene p og q være odde og det andre like. Siden x er et oddetall, vil $x^2 \equiv 1 \pmod 4$. Altså er $p^2 - q^2 \equiv 1 \pmod 4$, og det betyr at det er p som er odde og q som er like. □

Siden q er et partall, kan vi skrive $q = 2c$. Dermed er $y^2 = 2pq = 4pc$, så $(\frac{y}{2})^2 = pc$.

7.7 Lemma. p og c er kvadrattall.

Bevis: Siden p og q er innbyrdes primiske, må også p og c være det. Lar vi $\frac{y}{2} = p_1p_2 \cdot ...p_k$ være primtallsfaktoriseringer av $y/2$, får vi

$$pc = (\frac{y}{2})^2 = p_1^2p_2^2 \cdots p_k^2.$$

Siden p og c ikke har felles faktorer, må enten begge eller ingen av p_i-faktorene være en faktor i p. Dermed inneholder p og c bare kvadratfaktorer og må selv være kvadrater. □

Bevis for teorem 7.4: Siden p og c er kvadrater, kan vi skrive $p = d^2, c = f^2$. Siden $x^2 = p^2 - q^2 = (d^2)^2 - (2c)^2 = (d^2)^2 - (2f^2)^2$, så er

$$x^2 + (2f^2)^2 = (d^2)^2.$$

Legg merke til at siden p og q ikke har felles faktorer, så har heller ikke $x, 2f^2$ og d^2 felles faktorer. Dette betyr at $(x, 2f^2, d^2)$ er et primitivt pythagoreisk trippel som kan skrives

$$x = l^2 - m^2, \quad 2f^2 = 2lm, \quad d^2 = l^2 + m^2,$$

der l og m er innbyrdes primiske. Altså er $f^2 = lm$, der l og m er innbyrdes primiske, og akkurat som i beviset for lemma 7.7 kan vi konkludere med at l og m er kvadrattall. Altså er $l = r^2, m = s^2$, og dermed blir

$$r^4 + s^4 = l^2 + m^2 = d^2.$$

Vi har funnet en ny løsning av vår ligning $x^4 + y^4 = u^2$, og kan vi bare vise at $d < u$, har vi fått den selvmotsigelsen vi er på jakt etter. Går vi gjennom resonnementet en gang til, ser vi at

$$u = p^2 + q^2 > p = d^2 \geq d,$$

og dermed er teorem 7.4 bevist. □

Beviset vi nettopp har vært igjennom er et typisk eksempel på "nedstigningsmetoden" - en av Fermats yndlingsteknikker for å vise at noe er umulig.

Oppgaver

7.1 Finn alle pythagoreiske tripler med hypotenus $z \leq 50$.

7.2 Anta at

$$x^n + y^n = z^n$$

ikke har noen heltallig løsning når $n = 4$ eller når n er et odde primtall. Vis at ligningen ikke har heltallige løsninger for noen $n \geq 3$.

7.3 I denne oppgaven skal vi se at ligninger som ligger nær opptil Fermats, kan ha mange løsninger.

a) Vis at ligningen $x^n + y^n = z^{n+1}$ har uendelig mange heltallige løsninger (Vink: Prøv med $x = a(a^n + b^n)$ og $y = b(a^n + b^n)$.)
b) Gitt $m, n \in \mathbb{N}$ slik at $(m, n) = 1$ og $m, n > 1$. Vis at da har ligningen $x^m + y^m = z^n$ uendelig mange heltallige løsninger
(Vink: Skriv $1 = vn - um$ og prøv $x = a(a^m + b^m)^u$.)

7.4 La (x, y, z) være et primitivt pytagoreisk trippel.

a) Vis at nøyaktig ett av tallene x eller y må være delelig med 3. (*Hint*: Hvert av tallene x, y og z kan være kongruent med 0, 1 eller 2 modulo 3 (dvs. av formen $3k, 3k+1$ eller $3k+2$ for et helt tall k). Undersøk hvilke muligheter som kan forekomme).
b) Vis at nøyaktig ett av tallene x eller y må være delelig med 4. Konkluder at arealet av den rettvinklede trekanten med sider x, y, z må være delelig med 6.
c) Vis at nøyaktig ett av tallene x, y, z må være delelig med 5.
d) For hvilke naturlige tall n gjelder det at nøyaktig ett av tallene i ethvert pytagoreisk trippel (x, y, z) må være delelig med n?