Forord

Dette heftet i tallteori er tilpasset Matematisk institutts nettbaserte kurs i tallteori og baserer seg i stor grad på Erik Alfsen og Tom Lindstrøms kompendium i tallteori for MA 115/215. Heftet tar for seg elementær tallteori, slik som delelighet og primtall, Euklids algoritme, aritmetikkens fundamentalsats, Fermats lille og Eulers teoremer. Det er også gitt noen praktiske anvendelser, slik som RSA-systemet for kryptering. Et par kapitler tar for seg kongruensregning og løsning av lineære kongruenser, og endelig er det gitt utdrag fra likningsteorien, bl.a. pythagoreiske tripler, Diofants teorem og en liten innføring i Fermats siste teorem, samt en beskrivelse av kvadratsummer. Heftet er skrevet i en matematisk stringent form og kan kanskje virke litt tungt og teoretisk. Den mer lettere tilnærmingen til stoffet finnes i de andre læringsressursene knyttet til nettkurset. Til hvert kapittel er det et lite antall oppgaver. Kapitlene har følgende innhold:

1. Delelighet og Euklids algoritme
2. Primtall og primtallsfaktorisering
3. Kongruensregning
4. Fermats og Eulers teoremer, kryptografi
5. Pythagoreiske tripler, Fermats siste teorem
6. Lineære kongruenser
7. Kvadratsummer
8. Etterord og referanser

Oslo, juni 2001
Arne B. Sletsjøe

1. Delelighet og Euklids algoritme

Delelighet er et grunnbegrep 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

$$a = qb$$

Vi sier også at b *går opp i* a og at b *deler* a. Med symboler skriver vi

$$b|a$$

Et tall a som ikke er delelig med b må ligge mellom to tall qb og $(q+1)b$ som begge *er* delelig med b, og a er derfor på formen

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

Vi sier at q er *kvotienten* og 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:

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

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

□

Den største felles divisoren til to tall m og n, er det største tallet som går opp i både m og n. 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*. Den største felles divisoren til m og n betegnes med

$$(m, n)$$

Vi skal studere egenskaper ved den største felles divisoren. La $a, b \in \mathbf{Z}$. Vi sier at et tall $c \in \mathbf{Z}$ er en *lineær kombinasjon* av a og b dersom det finnes tall $s, t \in \mathbf{Z}$ 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 $d|a$ og $d|b$. 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 $s, t \in \mathbf{Z}$ 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. 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

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

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. $I(a,b)$ består nøyaktig av de tallene som er delelig med den største felles divisoren (a,b).

Bevis: 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 et vilkårlig tall som en lineær kombinasjon av a og b hvis og bare hvis a og b er innbyrdes primiske. □

Vi har sett at dersom c er delelig med største felles divisor til a og b, så finnes det hele tall s og t slik at

$$c = sa + tb,$$

men beviset ga oss ikke noen praktisk metode til å finne s og t. Det finnes imidlertid en eldgammel metode som går tilbake til den greske matematikeren Euklid (rundt 300 f.Kr.).

Metoden består av to deler, og den første delen er ikke noe annet enn en litt uvant måte til å bestemme største felles divisor til a og b. Vi starter med å dele det største av tallene (la oss si det er a) med det minste:

$$a = q_1 b + r_1$$

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

$$b = q_2 r_1 + r_2.$$

Deretter deler vi den første resten med den andre:

$$r_1 = q_3 r_2 + r_3$$

Så deler vi r_2 med 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 $r_n | r_{n-1}$. Fra den nest nederste ligningen følger det at $r_n | r_{n-2}$. Men hvis $r_n | r_{n-1}$ og $r_n | r_{n-2}$, så følger det fra den tredje nederste ligningen at $r_n | r_{n-3}$. 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 $r_n | b$ og $r_n | a$.

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 $c | r_1$. Men hvis $c | b$ og $c | r_1$, så forteller den andre linjen oss at $c | r_2$. Fortsetter vi på samme måte, ser vi at $c | r_3$ osv. Til slutt får vi at $c | r_n$, 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 (fordi store tall er tidkrevende å faktorisere).

Vi er nå klare til å gå løs på andre del av metoden - 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.

Oppgaver.

1. Finnes det hele tall x, y slik at
   a) $7x + 4y = 1$
   b) $9x + 15y = 4$
   c) $28x + 7y = -42$

2. 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?)

3. 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.

4. Kan 21 skrives som en lineær kombinasjon av 455 og 2772? Hvis ja, finn en slik kombinasjon.

5. 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?

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. Elever på mellomtrinnet vil kanskje kunne gjøre faktoriseringen

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

De kan imidlertid ikke føre et bevis for at en slik faktorisering alltid er mulig, eller at den er entydig (når vi ser bort fra faktorenes rekkefølge). Det er disse bevisene vi nå skal se på, og 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 $p|ab$, så må p dele minst ett av tallene a, b.

Bevis: Dersom $p|a$ er det ingenting å vise, så vi kan anta at $p \not| a$ (dette betyr at p ikke deler a), og utlede at da må $p|b$. Siden p er et primtall som ikke deler a, må p og a være innbyrdes primiske. Ifølge Teorem 1.4 finnes det da $s, t \in \mathbf{Z}$ slik at

$$1 = sa + tp$$

Multipliserer vi med b, får vi

$$b = sab + tbp.$$

Siden både ab og p er delelig med p, betyr dette at $p|b$, og vi er ferdige. □

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

$$a = p_1 p_2 \cdot \ldots \cdot p_m$$

der alle faktorene $p_1, p_2, \cdots, p_m$ er primtall. Denne oppspaltingen er entydig i den forstand at dersom vi har

$$a = q_1 q_2 \cdot \ldots \cdot q_n$$

der $q_1, q_2, \cdots, q_n$ er primtall, så er $m = n$, og faktorene q_i er de samme som 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

$$a = p_1 p_2 \cdots p_m \quad b = q_1 q_2 \cdot \ldots \cdot q_n$$

som gir

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

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

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

Siden primtallet p_1 går opp i $a = q_1 q_2 \cdots q_n$, må p_1 gå opp i én av faktorene $q_1, q_2, \cdots, q_n$ ifølge Setning 4.2 (denne setningen gjelder også når vi har flere enn to faktorer, se oppgave 6 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 bevise at $\sqrt{2}$ ikke er et rasjonalt tall (husk at et rasjonalt tall er ett som kan skrives på formen $\frac{m}{n}$ der $m \in \mathbf{Z}$ og $n \in \mathbf{N}$). I geometrisk form (det finnes ikke noe linjestykke som går opp i både siden og diagonalen til et kvadrat) går dette resultatet tilbake til den pythagoreisk skolen i Hellas over 400 år f. Kr.

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.

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

Bevis: Anta motsatt, at det finnes et endelig antall primtall. La $p_1, p_2, \cdots, p_n$ være 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 på p_i for alle i, så $p_i \not| N$. Men ifølge Aritmetikkens Fundamentalteorem 2.3, må N være delelig med et primtall p. Altså er $p \neq p_i$ for alle i og teoremet er bevist. □

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

Bevis: Anta at $\sqrt{2} = \frac{m}{n}$ der $m, n \in \mathbf{N}$. 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. □

2.6 Eksempel Vi skal se på en *kvadratisk utvidelse* av de hele tall, gitt ved

$$R = \mathbf{Z}[\sqrt{-5}] = \{\, a + ib\sqrt{5} \,|\, a, b \in \mathbf{Z}\}$$

der $i^2 = -1$ er den imaginære enheten. Vi kan behandle R som om det skulle være helt vanlige tall, det eneste spesielle er at $i^2 = -1$. I R har vi

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

Vi skal vise at $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ alle er primtall i R og at eksemplet derfor viser at vi ikke har entydig faktorisering i R.

Et nyttig hjelpemiddel for å vise dette er begrepet **norm**, $N(\alpha)$ til et tall $\alpha \in R$. Normen er definert ved

$$N(a + ib\sqrt{5}) = a^2 + 5b^2$$

Vi ser at normen $N(\alpha)$ til α er et positivt heltall som er null hvis og bare hvis $\alpha = 0$. I tillegg kan man vise at $N(\alpha)N(\beta) = N(\alpha\beta)$ for alle $\alpha, \beta \in R$. Hvis normen $N(a + ib\sqrt{5}) = 1$, så har vi $a^2 + 5b^2 = 1$ og derfor $a = \pm 1, b = 0$. Dette er de eneste enhetene i R, dvs. for hvilke det finnes inverser.

Anta nå at 3 ikke er et primtall, dvs. $3 = \alpha\beta$ hvor $\alpha, \beta \neq \pm 1$. Da har vi $9 = N(\alpha)N(\beta)$ og $N(\alpha) = \pm 3$. Men det er opplagt umulig å få til $a^2 + 5b^2 = 3$ (hvorfor?), så 3 er et primtall. Tilsvarende kan vi gjøre for 7.

Anta tilsvarende at $1 + 2\sqrt{-5} = \gamma\delta$. Da har vi

$$21 = N(1 + 2\sqrt{-5}) = N(\gamma)N(\delta)$$

Igjen får vi at enten er γ eller δ lik ± 1, eller så har de norm 3 eller 7. Men det har vi sett er umulig. Altså er $1 + 2\sqrt{-5}$ et primtall. Samme resonnement gjelder for $1 - 2\sqrt{-5}$. Dermed har vi vist at 21 kan faktoriseres på to helt forskjellige måter i R.

Oppgaver

1. To oppgaver om innbyrdes primiske tall:
   a) Vis at dersom a og b er innbyrdes primisk og $a|mb$, så vil $a|m$
   b) Vis at dersom a og b er innbyrdes primiske tall som begge deler c, så vil ab også dele c.

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

3. Vis at normen $N(\alpha)$ til elementer $\alpha \in R$ er multiplikativ, dvs. $N(\alpha\beta) = N(\alpha)N(\beta)$ for alle $\alpha, \beta \in \mathbf{Z}[\sqrt{-5}]$.

3. Kongruensregning

I dette kapitlet lar vi t være et naturlig tall større enn 1. 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 i samme mengde, 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

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

kalles *restklasseringen modulo* t.

Hvorfor $\mathbf{Z}/(t)$ 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. Legg merke til a og b tilhører samme restklasse hvis og bare hvis $a - b$ er delelig med t. Dersom dette er tilfelle, sier vi at a og b er *kongruente modulo* t og skriver

$$a \equiv b \ (mod\ t)$$

For et vilkårlig helt tall c lar vi $\bar{c}$ være restklassen som c tilhører (tidligere har vi bare brukt denne skrivemåten for $c = 0, 1, \cdots, t-1$). Vi har nå tre ekvivalente tolkninger av formelen $a \equiv b \ (mod\ t)$:

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

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 $a_1 \equiv a_2 (mod\ t)$ og $b_1 \equiv b_2 (mod\ t)$. Da er

$$a_1 + b_1 \equiv a_2 + b_2 (mod\ t) \text{ og } a_1 b_1 \equiv a_2 b_2 (mod\ t)$$

Bevis: Siden $a_1 \equiv a_2 (mod\ t)$ og $b_1 \equiv b_2 (mod\ t)$, 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 $a_1 + b_1 \equiv a_2 + b_2 (mod\ t)$. 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 $a_1 b_1 \equiv a_2 b_2 (mod\ t)$. □

På grunn av denne setning kan vi definere addisjon og multiplikasjon av restklasser.

3.2 Definisjon. Dersom $\bar{a}, \bar{b} \in \mathbf{Z}/(t)$ 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 $\overline{a_2 + b_2}$?

3.3 Eksempel. La oss regne ut $\bar{5} + \bar{6}$ og $\bar{5} \cdot \bar{6}$ i $\mathbf{Z}/(13)$. Ifølge definisjon er

$$\bar{5} + \bar{6} = \overline{5+6} = \overline{11}$$

Tilsvarende er

$$\bar{5} \cdot \bar{6} = \overline{5 \cdot 6} = \overline{30}$$

Dette 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 $30 \equiv 4 (mod\ 13)$. Altså er

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

Ved å gå fram på denne måten kan vi lage addisjons- og multiplikasjonstabellen for $\mathbf{Z}/(t)$.

La oss nå skrive ned de grunnleggende regnereglene for $\mathbf{Z}/(t)$:

3.4 Setning. I $\mathbf{Z}/(t)$ 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) $\bar{a} + \bar{0} = \bar{a}$ (nullelement)
(v) $\bar{a} \cdot \bar{1} = \bar{a}$ (nøytralt element)
(vi) $\bar{a} + \overline{(-a)} = 0$ (motsatt element)

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

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

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

□

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 $\mathbf{Z}/(t)$.

Regnereglene ovenfor er så like de vi er vant til at det er lett å tro at regning i $\mathbf{Z}/(t)$ er akkurat som regning i $\mathbf{Z}$. Men ser vi nøyere på multiplikasjonstabellen for $\mathbf{Z}/(6)$

$$\begin{array}{llllll} \bar{1}\cdot\bar{1}=\bar{1} & \bar{2}\cdot\bar{1}=\bar{2} & \bar{3}\cdot\bar{1}=\bar{3} & \bar{4}\cdot\bar{1}=\bar{4} & \bar{5}\cdot\bar{1}=\bar{5} \\ & \bar{2}\cdot\bar{2}=\bar{4} & \bar{3}\cdot\bar{2}=\bar{0} & \bar{4}\cdot\bar{2}=\bar{2} & \bar{5}\cdot\bar{2}=\bar{4} \\ & & \bar{3}\cdot\bar{3}=\bar{3} & \bar{4}\cdot\bar{3}=\bar{0} & \bar{5}\cdot\bar{3}=\bar{3} \\ & & & \bar{4}\cdot\bar{4}=\bar{4} & \bar{5}\cdot\bar{4}=\bar{2} \\ & & & & \bar{5}\cdot\bar{5}=\bar{1} \end{array}$$

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 å få $\bar{1}=\bar{4}$. 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. Et element $\bar{a}\in\mathbf{Z}/(t)$ kalles en *nulldivisor* dersom $\bar{a}\neq\bar{0}$ og det finnes et annet element $\bar{b}\neq\bar{0}$ slik at $\bar{a}\cdot\bar{b}=\bar{0}$.

3.6 Setning. Dersom t er et primtall, finnes det ingen nulldivisor i $\mathbf{Z}/(t)$. Dersom t ikke er et primtall, så vil $\bar{a}$ være en nulldivisor hvis og bare hvis $\bar{a}$ ikke er innbyrdes primisk med t.

Bevis: Den første påstanden er bare et spesialtilfelle av den andre, så vi nøyer oss med å bevise den andre. Anta at a og t ikke er innbyrdes primiske; da finnes det et tall $d>1$ slik at $a=nd, t=md$. Dermed er

$$\bar{a}\cdot\bar{m}=\overline{nd}\cdot\bar{m}=\overline{md}\cdot\bar{n}=\bar{t}\cdot\bar{n}=\bar{0}$$

som viser at $\bar{a}$ er en nulldivisor.

Anta omvendt at $\bar{a}$ er en nulldivisor og at $\bar{a}\bar{b}=\bar{0}$, der $\bar{b}\neq\bar{0}$. Dette betyr at $t|ab$. Ser vi på en vilkårlig primfaktor q i t, vet vi fra Setning 2.2 at q må dele enten a eller b. Nå kan ikke alle primfaktorene i t dele b, for da ville $t|b$, og det strider mot antagelsen om at $\bar{b}\neq 0$. Altså må minst én primfaktor i t dele a, og følgelig er ikke a og t innbyrdes primiske. □

Kjenner vi nulldivisorene, er det lett å løse forkortningsproblemet:

3.7 Setning. I restklasseringen $\mathbf{Z}/(t)$ gjelder forkortningsregelen

$$\bar{a}\bar{x} = \bar{a}\bar{y} \Rightarrow \bar{x} = \bar{y}$$

hvis og bare hvis a og t er innbyrdes primiske. Spesielt gjelder forkortningsregelen for alle $\bar{a} \neq \bar{0}$ dersom t er et primtall.

Bevis: Anta at a og t er innbyrdes primiske. Da er $\bar{a}$ ikke en nulldivisor, og vi har

$$\bar{a}\bar{x} = \bar{a}\bar{y} \Leftrightarrow \bar{a}(\bar{x} - \bar{y}) = \bar{0} \Leftrightarrow \bar{x} - \bar{y} = \bar{0} \Leftrightarrow \bar{x} = \bar{y}.$$

Dersom a og t ikke er innbyrdes primiske, er $\bar{a}$ en nulldivisor, så vi kan finne en $\bar{b} \neq \bar{0}$ slik at $\bar{a} \cdot \bar{b} = \bar{0}$. Velg en $\bar{x} \in \mathbf{Z}/(t)$ og la $\bar{y} = \bar{x} + \bar{b}$. Da er

$$\bar{a}\bar{y} = \bar{a}(\bar{x} + \bar{b}) = \bar{a}\bar{x} + \bar{a}\bar{b} = \bar{a}\bar{x} + \bar{0} = \bar{a}\bar{x},$$

men $\bar{y} \neq \bar{x}$. □

3.8 Eksempel. La oss avslutte dette kapitlet med 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 $a_n a_{n-1} a_{n-2} \cdots a_1 a_0$, der a'ene angir sifrene. Størrelsen til tallet er dermed

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

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

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

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

Oppgaver

1. Lag en addisjons- og en multiplikasjonstabell for $\mathbf{Z}/(7)$.

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

3. Vis at dersom $7|(a^2 + b^2)$, så må både $7|a$ og $7|b$ (Hint: Betrakt a^2 og b^2 modulo 7)

4. Bevis alle punktene i Setning 3.4

5. 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.

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

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

8. a) Bevis følgende påstand, ofte kalt "Det kinesiske restteorem": Anta at $r_1, r_2, \cdots, r_n$ er hele tall, at innbyrdes primiske for $i \neq j$. Vis at det fins ett og bare ett helt tall x slik at $0 \leq x < m_1 \cdots m_n$ og

$$\begin{aligned} x &\equiv r_1(mod\ m_1) \\ x &\equiv r_2(mod\ m_2) \\ &\vdots \\ x &\equiv r_n(mod\ m_n) \end{aligned}$$

   (Hint: Vis ved induksjon på k at det fins et tall x_k på formen

$$x_k = a_1 + a_2 m_1 + a_3 m_1 m_2 + \cdots + a_k m_1 m_2 \cdots m_{k-1}$$

   med $a_i < m_i$, og slik at $x_k \equiv r_1(mod\ m_1), x_k \equiv r_2(mod\ m_2), \cdots, x_k \equiv r_k$
   – $(mod\ m_k)$).
   b) Finn det minste positive tallet x slik at $x \equiv 5(mod\ 7), x \equiv 7(mod\ 11), x \equiv 3(mod\ 13)$.
   c) Anta at $m_1, m_2 \in \mathbf{N}$ *ikke* er innbyrdes primiske. Vis at det finnes tall r_1, r_2 slik at ligningssystemet

$$\begin{aligned} x &\equiv r_1(mod\ m_1) \\ x &\equiv r_2(mod\ m_2) \end{aligned}$$

   – ikke har løsning.

4. Fermats lille teorem og Eulers generalisering med anvendelser

De regnereglene vi hittil har sett på i $\mathbf{Z}/(t)$, er regler som restklasseringen har arvet fra $\mathbf{Z}$. Men det finnes også nye regneregler i $\mathbf{Z}/(t)$ som ikke har noen motsvarighet i $\mathbf{Z}$. 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 $\mathbf{Z}/(p)$ istedenfor $\mathbf{Z}/(t)$.

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

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

Bevis: $\mathbf{Z}/(p)$ 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 $p-1$ forskjellige, ikke-null elementer

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

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

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

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 $\bar{a} \in \mathbf{Z}/(p)$.

Bevis: Dersom $\bar{a} = \bar{0}$, er begge sider i ligningen null, og dersom $\bar{a} \neq 0$, multipliserer vi bare ligningen 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

$$7n^{12} + 6 \equiv 7 + 6 \equiv 13 \equiv 0 \ (mod\ 13)$$

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

4.4 Eksempel. Vis 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

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

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 $\bar{a}\bar{1}, \bar{a}\bar{2}, \cdots, \bar{a}\overline{(t-1)}$ være forskjellige med mindre a og t er innbyrdes primiske (husk setning 3.7), og for det andre kan vi ikke forkorte med $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdot ... \overline{(t-1)}$ i ligningen

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

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* $\phi : \mathbf{N} \to \mathbf{N}$ er gitt ved

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

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

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

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 3.7 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 med t, er mengdene

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

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

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

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 se på en anvendelse av Eulers teorem innen kryptografi, kjent under betegnelsen RSA (oppkalt etter Rivest, Shamir og Adleman som beskrev metoden i 1977). RSA-systemet er ofte beskrevet på følgende måte: Alice plasserer et objekt i en metallboks og låser med kombinasjonslås som Bob har etterlatt. Bob er den eneste som kan åpne boksen siden han er den eneste som kjenner kombinasjonen. Problemet er altså å sende informasjon, kryptert på en slik måte at det kun er den rette mottaker som kan forstå meldingen. Vi lar x være et tall (eller *klartekst*: informasjonen som skal overføres). Krypteringsalgoritmen erstatter klartteksten x med et nytt tall $y = e(x)$ (kryptert tekst) som kan sendes åpent ut i verden. Systemet er laget slik at kun den rette mottakeren kjenner dekrypteringsalgoritmen d som løser $d(y) = d(e(x)) = x$. Vi skal se nærmere på hvordan det hele virker.

Hver aktør som deltar i kommunikasjonen velger seg ut to odde primtall p og q (i praksis veldig store). La $n = pq$. Dette tallet offentliggjør vi (gjerne i en slags telefonkatalog eller krypteringskatalog). Når p og q er veldig store er det svært vanskelig og i praksis umulig å finne faktoriseringen $n = pq$ når faktorene ikke er kjent. Vi beregner $\phi(n) = (p-1)(q-1)$ og velger oss to tall a, b slik at $\bar{a}\bar{b} = \bar{1}$ i $\mathbf{Z}/(\phi(n))$. I tillegg til n offentliggjøres b. Når man ikke kjenner p og q er det umulig å beregne $\phi(n)$ og derfor umulig å finne a selv om b er kjent. Krypteringsalgoritmen er gitt ved

$$e(x) = \bar{x}^b \quad \text{i} \quad \mathbf{Z}/(n)$$

mens dekrypteringsalgoritmen er gitt ved

$$d(y) = \bar{y}^a \quad \text{i} \quad \mathbf{Z}/(n)$$

Merk at krypteringen kan gjøres av enhver, bare ved å slå opp i krypteringskatalogen og lese av den utvalgte mottakerens offentlige nøkkkel. Men kun den som kjenner a, dvs den rette mottakeren kan dekryptere meldingen. Det skjer på følgende måte (la $y = e(x)$):

$$\begin{aligned} d(y) = d(e(x)) &= e(x)^a = (\bar{x}^b)^a \\ &= \bar{x}^{ab} = \bar{x}^{1+t\phi(n)} = \bar{x}(\bar{x}^{\phi(n)})^t \\ &= \bar{x} \end{aligned}$$

I den siste overgangen har vi brukt Eulers teorem til å beregne

$$(\bar{x}^{\phi(n)})^t = \bar{1}^t = \bar{1}$$

Vi skal konkretisere hele prosedyren i et eksempel.

4.7 Eksempel. Vi lar Bob sine odde primtall være $p = 31$ og $q = 19$. Det gir $n = 589$ og $\phi(589) = 540$. I tillegg velger han $b = 43$, som gir $a = 427$ (husk at $\overline{43} \cdot \overline{427} = \overline{18361} = \overline{540 \cdot 34 + 1} = \bar{1}$ i $\mathbf{Z}/(540)$). I krypteringskatalogen offentliggjør

Bob tallene $(589, 427)$. Hvis Alice nå ønsker å sende meldingen $x = 105$ til Bob, beregner hun

$$\begin{aligned}\overline{105}^{427} &= \overline{105}^{256+128+32+8+2+1} \\ &= \overline{105}^{2^8}\overline{105}^{2^7}\overline{105}^{2^5}\overline{105}^{2^3}\overline{105}^{2^1}\overline{105}^{2^0} \\ &= \overline{241}\end{aligned}$$

Alle regningene er gjort modulo 589.
Denne meldingen er den hun sender. Utregningen over gir en effektiv måte å beregne slike store potenser, kun ved å kvadrerere modulo et gitt tall. En ukjent lytter kjenner nå de tre tallene $589, 427, 241$. Det er svært komplisert, i praksis umulig (når tallene er store nok) å finne p, q, a og x utelukkende med disse tre tallene som basis. Bob derimot, kjenner p, q, a, men ikke x. Den kan han imidlertid beregne ved å regne ut

$$\overline{241}^a = \overline{241}^{43} = \overline{105}$$

gjerne ved å bruke kvadreringsoppskriften over og oppsplittingen

$$43 = 2^5 + 2^3 + 2^1 + 2^0$$

Dermed har Bob funnet tilbake til den opprinnelige meldingen.

Oppgaver

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 $n \in \mathbf{N}$.
   d) Vis at $n^7 - n$ er delelig med 42 for alle $n \in \mathbf{Z}$.

2. La a være et helt tall. Vis at

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

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

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

4. La n og k være hele tall, $0 \leq k \leq n$. Definer *n-fakultet* ved $0! = 1, 1! = 1, n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$. Definer *binomialkoeffisientene* 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 $r \in \mathbf{N}$. 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 $n^p \equiv n (mod\ p)$ for alle $n \in \mathbf{N}$ ved induksjon.
   e) Bruk d) til å vise Fermats "lille" teorem.

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

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

5. 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

$$(p^2 - q^2)^2 + (2pq)^2 = (p^2 + q^2)^2 \tag{5.1}$$

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 Diofant (som sannsynligvis levde rundt 300 e.Kr.). I sin bok "Arithmetika" viser han at alle pythagoreiske tripler framkommer ved å velge passende verdier for p og q i (5.1). I dette kapitlet skal vi utlede Diofants 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.

5.1 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 $a \in \mathbf{Z}$ er

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

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. □

5.2 Diofants 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 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

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

og følgelig er $\frac{z+x}{2} = (r_1 r_2 \cdot \ldots \cdot r_m)^2$, $\frac{z-x}{2} = (r'_1 r'_2 \cdot \ldots \cdot r'_k)^2$. 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 Fermat 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 $x, y, z \in \mathbf{N}$ 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 $n = 4$.

5.3 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:

5.4 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 5.4 medfører Teorem 5.3.

For å vise Teorem 5.4 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.

5.5 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 $t|c$, 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. Etter Diofants teorem 5.2 finnes det 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.

5.6 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 $(\frac{y}{2})^2 = pc$.

5.7 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

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

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 5.4: 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 5.7 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 5.4 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

1. 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 $n \geq 3$.

2. 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 $m, n \in \mathbf{N}$ 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 $x = a(a^m + b^m)^u$.)

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

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?

6. Lineære kongruenser

I dette kapitlet skal vi se hvordan vi kan løse lineære ligninger $\bar{a} \cdot \bar{x} = \bar{b}$ i $\mathbf{Z}/(t)$. Vi begynner med hovedresultatet.

6.1 Teorem. Ligningen $\bar{a} \cdot \bar{x} = \bar{b}$ har en løsning i $\mathbf{Z}/(t)$ 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
$$\bar{b} = \overline{xa + yt} = \bar{x} \cdot \bar{a} + \bar{y}\bar{t} = \bar{x} \cdot \bar{a}$$
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
$$b = xa + mt \quad \text{for en } m \in \mathbf{Z}$$
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 t er et primtall, så har ligningen $\bar{a}\bar{x} = \bar{b}$ alltid en løsning når $\bar{a} \neq \bar{0}$. I dette tilfelle er løsningen entydig (dersom både $\bar{x}$ og $\bar{y}$ er løsninger, må $\bar{a}\bar{x} = \bar{a}\bar{y}$, og dermed $\bar{x} = \bar{y}$ ifølge Setning 3.7), men hvis t ikke er et primtall, kan det godt hende at ligningen har flere løsninger (se oppgave 4).

Innebygget i beviset for Teorem 6.1 er en metode til å løse ligningen. Vi viser den gjennom et eksempel.

6.2 Eksempel. Løs ligningen $\overline{11}\bar{x} = \bar{3}$ i $\mathbf{Z}/(37)$. Vi bruker 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 $\bar{b} = \bar{1}$. Hvis t er et primtall, har denne ligningen alltid (dvs. for $\bar{a} \neq \bar{0}$) en entydig løsning. Denne løsningen kalles den *inverse til* $\bar{a}$ og betegnes med $\bar{a}^{-1}$. Vi har altså

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

6.3 Setning. Dersom t er et primtall, er den entydige løsningen til $\bar{a}\bar{x} = \bar{b}$ i $\mathbf{Z}/(t)$ lik $\bar{x} = \bar{a}^{-1}b$.

Bevis: Vi multipliserer ligningen $\bar{a}\bar{x} = \bar{b}$ med $\bar{a}^{-1}$:

$$\begin{aligned} \bar{a}^{-1}(\bar{a}\bar{x}) = \bar{a}^{-1}\bar{b} &\overset{(ii)}{\Leftrightarrow} (\bar{a}^{-1}\bar{a})\bar{x} = \bar{a}^{-1}\bar{b} \Leftrightarrow \\ \Leftrightarrow \bar{1} \cdot \bar{x} = \bar{a}^{-1}\bar{b} &\overset{(v)}{\Leftrightarrow} \bar{x} = \bar{a}^{-1}\bar{b}, \end{aligned}$$

hvor vi har brukt regnereglene i Setning 3.4. □

6.4 Eksempel. Vi skal se på et eksempel på bruk av kongruensregning. Alle som bor i Norge har et 11-sifret personnummer. Personnummeret består av et 6-sifret fødsels-nummer, 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 $\mathbf{Z}/(11)$ 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 $\mathbf{Z}/(11)$ 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 likningene 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

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

2. Finn de inverse elementene til
   a) $\overline{49}$ i $\mathbf{Z}/(61)$
   b) alle elementene i $\mathbf{Z}/(11)$.

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

4. I denne oppgaven er $a, b, c \in \mathbf{Z}, a, b \neq 0$.
   a) Når kan c skrives som en lineær kombinasjon av a og b (dvs. når fins det $x, y \in \mathbf{Z}$ slik at $c = ax + by$)?
   – Heretter antar vi at c kan skrives som en lineær kombinasjon av a og b, og vi lar $x_0, y_0 \in \mathbf{Z}$ være slik at $c = ax_0 + by_0$.
   b) La $m \in \mathbf{Z}$, og sett $x = x_0 + m\frac{b}{d}, y = y_0 - m\frac{a}{d}$, der d er den største felles faktoren til a og b. Vis at
   $$c = ax + by$$
   c) La $x, y \in \mathbf{Z}$ være to tall slik at $c = ax + by$. Vis at det fins $m \in \mathbf{Z}$ slik at
   $$x = x_0 + m\frac{b}{d} \quad , \quad y = y_0 - m\frac{a}{d}$$
   d) Anta at $b > 0$. Hvor mange løsninger har likningen
   $$\bar{a}\bar{x} = \bar{c}$$
   i $\mathbf{Z}/(b)$?
   e) Finn alle løsningene til $\overline{35} \cdot \bar{x} = \bar{7}$ i $\mathbf{Z}/(49)$

7. Kvadratsummer

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

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

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

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

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 $x, y \in \mathbf{Z}$ 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.

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

Bevis: Dersom x er et partall, er $x^2 \equiv 0$ (mod 4). Er x et oddetall, er $x^2 \equiv 1$ (mod 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.

□

7.2 Teorem. Et primtall p er en kvadratsum hvis og bare hvis $p = 2$ eller $p \equiv 1$ (mod 4).

Bevis: Siden $2 = 1^2 + 1^2$ er en kvadratsum, gjenstår det bare å vise at dersom $p \equiv 1$ (mod 4), så er p en kvadratsum. La K være det største hele tallet mindre enn $\sqrt{p}$, og la $i \in \mathbf{Z}$ være valgt slik at $\bar{i}^2 = -1$ i $\mathbf{Z}/(p)$ (man kan vise at en slik i finnes). 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 $\mathbf{Z}/(p)$, må det finnes *forskjellige* par (u, v) og (u', v') slik at $f(u, v)$ og $f(u', v')$ tilhører samme restklasse, dvs.

$$u + iv \equiv u' + iv' \ (mod\ p)$$

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

$$x \equiv iy \ (mod\ p)$$

Siden $\bar{i}^2 = -\bar{1}$ i $\mathbf{Z}/(p)$, 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 $\mathbf{Z}/(p)$, 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.

7.3 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.

7.4 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 $p|a$, er $\bar{a} = \bar{x}^2 + \bar{y}^2 = \bar{0}$ i $\mathbf{Z}/(p)$. Siden $p \not| y$, er $\bar{y} \neq \bar{0}$, og det finnes et element $\bar{k} \in \mathbf{Z}/(p)$ slik at $\bar{k}\bar{y} = \bar{x}$. Dette gir

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

og siden $\bar{y} \neq \bar{0}$, kan vi forkorte og få

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

som er umulig når $p \equiv 3 \pmod 4$ (ikke opplagt, men trenger et argument som vi ikke skal gå inn på her).

□

7.5 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 og kan trekke konklusjonen.

7.6 Teorem. Et naturlig tall a kan skrives som en sum av to kvadrater hvis og bare hvis hver primfaktor 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

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

der p'ene er primfaktorer som er kongruente med 3 (mod 4), mens q'ene er primfaktorer som ikke er kongruente med 3. Ifølge Teorem 7.2 er hver q_i 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 7.3.

□

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 tilfelle; 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.

Oppgaver

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

2. Vis ved induksjon at dersom a er et produkt av n kvadratsummer, så er a selv en kvadratsum (dvs. fullfør beviset for lemma 11.3)

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 $4^m(8k + 7), m, k \in \mathbf{N}$, 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. Ideen går tilbake til den franske matematikeren Charles Hermite (1822-1901).

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 $|k/m| = |N/(i-j)|$.

5. Anta at p er primtall, $p \equiv 1$ (mod 4). La u være en løsning av kongruensen $u^2 \equiv -1$ (mod 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 $x^2 + y^2 \equiv 0$ (mod p).

e) Forklar hvorfor c) og d) medfører at $x^2 + y^2 = p$.

8. Litt fra tallteoriens historie

Allerede i de tidligste matematiske kildene vi har, finnes det tallteoretiske resultater. I Kapittel 5 så vi at babylonerne hadde tabeller over pythagoreiske tripler for nesten 4000 år siden, og omtrent samtidig utviklet egypterne et finurlig brøksystem som krevde stor tallteoretisk innsikt. Gresk og hellenistisk matematikk var i hovedsak geometrisk, men ga også viktige bidrag til tallteorien (slik som Euklids algoritme og hans bevis for at det finnes uendelig mange primtall). Den største tallteoretikeren innenfor denne tradisjonen er Diofant - en person vi ikke vet noen ting om bortsett fra at han må ha levd mellom år 100 og 300 e.Kr. Store deler av Diofants hovedverk "Arithmetika" har overlevd, og det første resultatet der er den karakteriseringen av pythagoreiske tripler som vi ga i Kapittel 5. Heltallige løsninger av ulike typer ligninger, f.eks.

$$7x + 4y = 5$$
$$x^2 + y^2 = z^2.$$

kalles *diofantiske ligninger* til ære for Diofant.

Sin første virkelige blomstring fikk tallteorien i Asia - i indisk og kinesisk matematikk. Som et eksempel kan vi nevne at Brahmagupta (ca. 625) og Bhaskaracharya (ca. 1100) studerte ligninger av typen

$$Dx^2 + 1 = y^2$$

lenge før de dukket opp i europeisk litteratur (- hvor de forøvrig kalles Pell'ske ligninger etter engelskmannen John Pell, 1610-85). Bhaskaracharyas "sykliske metode" for løsning av slike ligninger er høydepunktet i klassisk indisk tallteori.

Et høydepunkt i kinesisk tallteori er det som idag kalles det kinesiske restteorem (Kapittel 3, oppgave 8). Sin endelige form fikk det av Chin Chiu Shao i hans hovedverk "Su Shu Chiu Chang" (Ni kapitler med matematikk) fra 1247.

I 1621 utga den franske matematikeren Bachet de Mézeriac (1587-1638) en trykt utgave av Diofants "Arithmetika". Et eksemplar falt i hendene på en jurist og hobbymatematiker fra Toulouse - Pierre de Fermat (1601-1665) - og dermed begynte den moderne tallteoriens historie. Fermat publiserte ikke sine resultater, men noen kjenner vi fra hans brev, og andre fra hans notater i margen til "Arithmetika". Etter Fermats død utga hans sønn en ny utgave av "Arithmetika" med farens margkommentarer.

Fermat arbeidet på mange områder innenfor matematikken; han var en av forløperne til integral- og differensialregningen, han brevvekslet med Pascal om sannsynlighetsteoriens grunnlag, og han ga et viktig bidrag til matematisk fysikk ("Fermats prinsipp"). Selv om ettertiden har vurdert hans tallteoretiske arbeider høyest, skapte de ikke skole i samtiden, og det var først den store sveitsiske matematikeren Leonard Euler (1707-1783) som for alvor tok opp arven etter Fermat.

Euler beviste mange av de resultatene Fermat hadde framsatt uten bevis, han fant den kvadratiske resiprositetssatsen som en empirisk lov, og han var den første til å oppdage sammenhengen mellom ζ-funksjonen og primtall.

Eulers eneste rival som den ledende matematikeren på 1700-tallet var Joseph Louis Lagrange (1736-1813). Tallteori var bare en bibeskjeftigelse i hans matematiske virke, men i 1770 viste han ett av de mest slående tallteoretiske resultater - ethvert naturlig tall kan skrives som en sum av fire kvadrater.

Langt mer av en hovedbeskjeftigelse var tallteorien for Adrien Marie Legendre (1752-1833), og hans lærebok bidro sterkt til å øke emneområdets popularitet. I tillegg til å innføre Legendre-symbolet og formulere den kvadratiske resiprositetssatsen, er Legendre særlig kjent for karakteriseringen av de heltallene som kan skrives som en sum av tre kvadrater.

Den neste, store revolusjonen i tallteorien kom med Carl Friedrich Gauss (1777-1855). Allerede som nittenåring ga han det første fullstendige beviset for den kvadratiske resiprositetssatsen, og i 1801 kom hans store verk om tallteori "Disquisitiones Arithmeticae". I tillegg til et utall av nye, dype resultater inneholder denne boken en ny synsvinkel på tallteorien - restklasseringene $\mathbf{Z}/(t)$ innføres og brukes systematisk i oppbygningen av teorien.

Med Gauss avsluttes på mange måter den klassiske perioden i tallteorien. I den videre historien knyttes tallteorien i sterkere grad til andre deler av matematikken; til analysen av Dirichlet og Riemann i deres bruk av Fourier-rekker og kompleks funksjonsteori, og til algebraen av Kummer, Dedekind og Kronecker i

deres bruk av idealer og polynomringer. Denne utviklingstendensen fortsetter fram til idag.

I første halvdel av dette århundre var tallteori det sterkeste matematiske fagområdet i Norge. Mange forskere nådde resultater som har blitt stående, og spesielt er det naturlig å trekke fram Axel Thue (1863-1922), Viggo Brun (1885-1978) og Atle Selberg (1917-). Disse tre er nærmere omtalt i Karl Egil Auberts artikkel [1].

I dette hefte har vi hovedsakelig holdt oss til tallteori som ren matematikk. I kapittel 4 har vi plassert et av unntakene, nemlig anvendelser av tallteori i kryptografi - teorien for koding og dekoding av informasjon. Tidligere var det nesten bare militære som brydde seg om kryptografi, men idag gjør datamaskiner, telekommunikasjon og "intelligente" kort det til et viktig område også for sivile. To gode artikler om disse temaene er skrevet av Ben Johnsen [5] og Leif Nilsen [6].

For dem som ønsker å lære mer om tallteori, er Hardy og Wright [4] og Niven, Zuckerman og Montgomery [7] to klassiske tekster som har kommet i mange utgaver. Begge er lange og forutsetter at leseren er istand til å putte inn en del mellomregninger selv. Burton [2], Flath [3] og Stewart [8] er kortere og vennligere mot leseren. For dem som ønsker et historisk perspektiv, er Weil [9] en utmerket kilde (men vær klar over at mange av kommentarene ikke er ment for begynnere!)

Referanser

1. K.E. Aubert: Norske tallteoretikere, i Per Hag & Ben Johnsen (red.): *Fra Matematikkens Spennende Verden*, Tapir, 1993, 43-62.
2. D.M. Burton: *Elementary Number Theory*, Allyn & Bacon, 1976.
3. D.E. Flath: *Introduction to Number Theory*, John Wiley & Sons, 1989.
4. G.H. Hardy & E.M. Wright: *An Introduction to the Theory of Numbers*, Clarendon Press, 1938 (mange senere utgaver).
5. B. Johnsen: Kryptografi - en gammel disiplin med moderne anvendelser, i Per Hag & Ben Johnsen (red.): *Fra Matematikkens Spennende Verden*, Tapir, 1993, 123-134.
6. L. Nilsen: Modulære kvadratrøtter og moderne kryptologi, *Normat*, **40** (1992), 75-89.
7. I. Niven, H.S. Zuckerman, H.L. Montgomery: *An Introduction to the Theory of Numbers*, 5th Edition, John Wiley & Sons, 1991.
8. B.M. Stewart: *Theory of Numbers*, 2nd Edition, MacMillan, 1964.
9. A. Weil: *Number Theory: An Approach through History*, Birkhäuser, 1984.