Workshop i talteori

Rasmus Frigaard Lemvig (rle@unf.dk)

Ungdommens Naturvidenskabelige Forening København

Dato: 23. maj 2023

Introduktion til workshoppen

I denne workshop skal vi arbejde med talteori, som er en af matematikkens ældste grene. I dag er talteori så stort et felt, at vi på ingen måde kan give en fyldestgørende introduktion på én dag. Ikke desto mindre vil vi introducere nogle af de mest grundlæggende begreber. Vi indfører begrebet delelighed og undersøger primtallene og nogle af deres egenskaber. Derefter gennemgår vi Euklids algoritme til at bestemme den største fælles divisor af to heltal. Til slut indfører vi modulær aritmetik, som er en ny måde at regne på, der viser sig at være særdeles nyttig i mange sammenhænge.

Hvad skal I få ud af workshoppen? Jeg håber naturligvis, at I bliver klogere, men endnu vigtigere er det, at I ser, at matematik er mange ting. Det er ikke kun regning, det er også en særdeles kreativ proces, der handler om at udforske ideer og koncepter.

1 Delelighed og primtal

1.1 Grundlæggende begreber

Talteori er studiet af heltallene, dvs. tallene

$$..., -3, -2, -1, 0, 1, 2, 3, ...$$

I dette afsnit laver vi de mest grundlæggende definitioner og observationer. Fra grundskolen har vi allerede en god fornemmelse for en del af de kommende begreber, men det er alligevel værd at definere dem helt formelt. Lad os starte med delelighed.

Definition 1.1. Lad d og a være heltal. Vi siger, at d *deler* a eller, at d er en *divisor/faktor* i a, såfremt der eksisterer et heltal n, sådan at $a = d \cdot n$. I så fald skriver vi $d \mid a$.

Lad os se nogle eksempler på dette.

Eksempel 1.2. 2 deler 6, fordi vi kan skrive $6 = 2 \cdot 3$ (her er $d = 2$, $a = 6$ og $n = 3$ i definitionen ovenover). 2 deler ikke 7, fordi der intet heltal n findes så $7 = 2 \cdot n$.

Bemærkning 1.3. Alle heltal deler 0. Lad d være et vilkårlig heltal, da er $0 = d \cdot 0$.

Delelighed er et fuldstændig fundamentalt begreb i talteori, og alt i denne workshop vil i sidste ende bygge på det. Det er derfor på sin plads, at vi redegør for nogle regneregler for delelighed. For at gøre dette, skal vi dog bruge endnu en definition.

Definition 1.4. *Tværsummen* af et heltal er lig summen af alle cifrene i tallet. Så hvis $a = a_k a_{k-1} ... a_1$ er et heltal (hvor a_i er det i'te ciffer fra venstre), da vil tværsummen være lig $a_k + a_{k-1} + ... + a_1$. Den *alternerende tværsum* er lig summen af heltallets cifre, men hvor fortegnet skifter, dvs. $a_k - a_{k-1} + a_{k-2} - ....$

Det er på sin plads med nogle eksempler.

Eksempel 1.5. Tværsummen af 123 er $1 + 2 + 3 = 6$. Den alternerende tværsum er $1 - 2 + 3 = 2$. Tværsummen af 9415 er $9 + 4 + 1 + 6 = 20$, og den alternerende tværsum er $9 - 4 + 1 - 6 = 0$.

Vi når nu til workshoppens første resultat, nemlig følgende proposition (proposition betyder blot et resultat):

Proposition 1.6. *Lad a være et heltal.*

(i) 2 *deler a hvis og kun hvis a er et lige tal.*

(ii) 3 *deler a hvis og kun hvis* 3 *deler tværsummen af a.*

(iii) 5 *deler a hvis og kun hvis a slutter på 0 eller 5.*

(iv) 9 *deler a hvis og kun hvis* 9 *deler tværsummen af a.*

(v) 10 *deler a hvis og kun hvis a slutter på 0.*

(vi) 11 *deler a hvis og kun hvis* 11 *deler den alternerende tværsum af a.*

Husk, at "hvis og kun hvis" betyder, at de to udsagn på hver side er ækvivalente. F.eks. siger resultatet ovenover, at hvis 3 deler a, da vil 3 dele tværsummen af a, og hvis 3 deler tværsummen af a, da deler 3 også a. En del af regnereglerne er I nok allerede bekendte. Til slut i workshoppen skal vi bruge modulær aritmetik til at give et meget elegant bevis for disse regler. I er dog mere end velkomne til at bruge reglerne allerede nu.

1.2 Primtal

Primtal er en af de mest studerede objekter i talteori og med god grund. De viser sig at have et væld af fascinerende egenskaber, som vi dog kun kan nå at se en brøkdel af i denne workshop.

Definition 1.7. Et *primtal* er et positivt heltal p forskellig fra 1, hvor de eneste positive divisorer i tallet er 1 og tallet selv.

Man kan overbevise sig selv om, at de første primtal er:

$$2, 3, 5, 7, 11, 13, 17, 19$$

Det er i teorien nemt at bestemme om et heltal er et primtal. 5 er et primtal, fordi de eneste positive divisorer i 5 er 1 og 5. Det er jo bare at indse, at 2, 3 og 4 ikke deler 5. Men hvad med et meget stort tal? Hvordan kan vi f.eks. vide, om 4594140411379 er et primtal? For at kunne afgøre dette, skal vi bruge en såkaldt *primtalstest*. En simpel en er givet herunder.

Proposition 1.8. *Et positivt heltal $p > 1$ er et primtal hvis og kun hvis p ingen positive divisorer har mindre end eller lig $\sqrt{p}$ (bortset fra 1).*

Bevis: Antag, at p er et primtal. Så har p ingen positive divisorer udover p eller 1. Specielt har p ingen positive divisorer mindre end $\sqrt{p}$ bortset fra 1.
Antag nu, at p ingen positive divisorer har mindre end $\sqrt{p}$ udover 1. Lad os for modstrid antage, at p ikke er et primtal. Da kan vi skrive $p = a \cdot b$, hvor $a, b > 1$. Per antagelse er $\sqrt{p} < a, b$. I så fald fås $p = \sqrt{p} \cdot \sqrt{p} < a \cdot b = p$, men dette er en modstrid! Et tal er jo ikke skarpt større end sig selv. Vi konkluderer, at antagelsen om, at p ikke er et primtal må være falsk, ergo er p et primtal som ønsket. ■

Eksempel 1.9. Lad os undersøge, om 101 er et primtal. Ifølge propositionen ovenover skal vi kun undersøge, om alle positive heltal større end 1 og mindre end eller lig $\sqrt{101} \approx 10{,}05$ er divisorer. Det er nemt at se, at hverken 2, 3, 4, 5, 6, 7, 8, 9 eller 10 deler 101. Ergo er 101 et primtal.

Der er utallige primtalstests, nogle meget sofistikerede. Det er en central problemstilling i talteori at udvikle mere og mere effektive primtalstests. Vi har følgende hjælperesultat (kaldet et *lemma* i matematik):

Lemma 1.10 (**Euklids lemma**)**.** *Lad a og b være heltal og p et primtal, som deler $a \cdot b$. Da deler p a eller b.*

Bevis: Beviset er udeladt, da vi ikke har teknikkerne til at vise det. Se [5, s. 45]. ■

Det er ikke svært at give et eksempel, hvor lemmaet er falsk, hvis man dropper antagelsen om, at p skal være et primtal. En af de vigtigste resultater i talteori er Aritmetikkens fundamentalsætning. For at kunne skrive den op, skal vi have en sidste definition på plads.

Definition 1.11. Lad a være et heltal. En opskrivning $a = \pm p_1 \cdot \ldots \cdot p_n$, hvor alle p_i er primtal (ikke nødvendigvis forskellige) kaldes en *primtalsfaktorisering/primtalsopløsning* af a.

Eksempel 1.12. Et primtal p har den trivielle/oplagte primtalsfaktorisering $p = p$. En primtalsfaktorisering af 66 er $66 = 2 \cdot 3 \cdot 11$, og en primtalsfaktorisering af -122 er $122 = -2 \cdot 61$.

Sætning 1.13 (**Aritmetikkens fundamentalsætning**). *Alle heltal forskellig fra* -1*, 1 og 0 har en primtalsfaktorisering, som er unik, hvis man ikke skelner mellem to faktoriseringer, hvor primfaktorerne er byttet rundt.*

Bevis: Det er tilstrækkeligt at vise sætningen for positive heltal, da vi blot kan ændre fortegnet på et negativt tal, faktorisere det og tilføje fortegnet igen efterfølgende. Overbevis dig selv om, at dette gælder.

Vi viser nu, at alle heltal større end 1 kan primfaktoriseres. Lad $n > 1$ være et heltal. Antag, at n *ikke* kan skrives som et produkt af primtal. Vi kan også antage, at n er det mindste heltal, som ikke kan skrives som et produkt af primtal. n kan ikke være et primtal (hvorfor?), så $n = a \cdot b$ for to heltal a, b, der begge er mindre end n og større end 1. Per antagelse må a og b kunne skrives som et produkt af primtal. Men da kan n også skrives som et produkt af primtal, en selvmodsigelse. Vi konkluderer, at der ikke findes nogle positive heltal, der ikke kan skrives som et produkt af primtal.

Vi viser nu unikhed. Antag, at $n = p_1 \cdot p_2 \cdot ... \cdot p_m = q_1 \cdot q_2 \cdot ... \cdot q_k$ for primtal p_i og q_j. Per det foregående lemma må vi have, at p_1 deler ét af primtallene q_1, q_2, ... q_k. Men hvis et primtal deler et andet primtal, må de to primtal være ens. Ergo er p_1 lig én af q_i'erne. For overskuelighedens skyld kan vi antage $p_1 = q_1$, og vi deler begge sider med p_1:

$$p_2 \cdot ... \cdot p_m = q_2 \cdot ... \cdot q_k$$

Gentager vi dette argument igen og igen, ender vi til sidst med, at alle primtallene må være lig hinanden parvis, så opskrivningen for n er unik. ■

Bemærkning 1.14. Formuleringen "som er unik, hvis man ikke skelner mellem to faktoriseringer, hvor primfaktorerne er byttet rundt" bliver som regel udtrykt ved "som er unik *op til* ombytning af primfaktorer". *Op til* er et typisk matematiker-udtryk.

Eksempel 1.15. Vi så før, at $66 = 2 \cdot 3 \cdot 11$ er en primtalsfaktorisering af 66. Dette er også den eneste mulighed jævnfør sætning 1.13. Vi kan selvfølgelig også skrive $66 = 3 \cdot 11 \cdot 2$ eller $66 = 3 \cdot 2 \cdot 11$, men vi siger, at disse faktoriseringer er ens, da de samme primtal indgår.

En god fortolkning af Aritmetikkens fundamentalsætning er, at primtallene er "byggeklodserne" for alle heltal. Et andet spørgsmål, man kan stille om primtallene er, hvor mange der er. Følgende sætning giver svaret:

Sætning 1.16. *Der findes uendeligt mange primtal.*

Bevis: Vi kender allerede en del primtal, f.eks. 2, 3 og 5. Lad $p_1, p_2, ..., p_n$ betegne de n første primtal. Vi konstruérer nu et nyt primtal ud fra disse. Lad os gange vores n første primtal sammen og lægge 1 til. Per forrige sætning kan dette heltal faktoriseres i primtal $q_1, q_2, ..., q_l$:

$$p_1 \cdot p_2 \cdots p_n + 1 = q_1 \cdot q_2 \cdots q_l$$

Hvis en af primtallene på højre side q_i er lig en af primtallene p_j på venstre side, omskriver vi ligningen og får:

$$1 = q_1 \cdot q_2 \cdots q_l - p_1 \cdot p_2 \cdots p_n$$

Hvis q_i er lig et p_j, vil q_i dele højresiden og dermed venstresiden, som er lig 1. Altså er $q_i = 1$, men 1 er ikke et primtal. Altså kan et q_i umuligt være lig en af primtallene $p_1, p_2, ..., p_n$. Definér p_{n+1} som det mindste af primtallene $q_1, q_2, ..., q_l$. Dermed har vi konstrueret et nyt primtal ud fra de første n. Vi kan gentage denne proces uendeligt mange gange og dermed lave uendeligt mange primtal. Dette færdiggør beviset. ■

1.3 Opgaver

1.3.1 Opgaver til grundlæggende begreber

- **Opgave 1.1:**
  Afgør, om 3 deler følgende heltal:
  1)123
  2)1477
  3)10000000001
  4)718494

- **Opgave 1.2:**
  Afgør, om 5 deler følgende heltal:
  1)184760
  2)54190672665
  3)193915818
  4)681985

- **Opgave 1.3:**
  Afgør, om 9 deler følgende heltal:
  1)1323
  2)90013
  3)654237
  4)78313

- **Opgave 1.4:**
  Afgør, om 11 deler følgende heltal:
  1)121
  2)211
  3)833074924
  4)55821

- **Opgave 1.5:**
  Hvis, at Euklids lemma (lemma 1.10) ikke holder generelt, hvis man dropper antagelsen om, at p er et primtal.

- **Opgave 1.6:**
  Lad a, b, d være heltal, og antag $d \mid a$ og $d \mid b$. Bevis, at d deler $a + b$ og $a - b$.

- **Opgave 1.7:**
  Lad a og b være heltal. Antag, at a deler b og b deler a. Bevis, at a er lig b eller $-b$. [Vink: Hvis det for heltal c og d gælder, at $c \cdot d = 1$, så må $c = d = \pm 1$]

- **Opgave 1.8:**
  Antag, at et heltal a deler b, og at b deler et andet heltal c. Bevis, at a deler c. Denne egenskab kaldes for *transitivitet*.

1.3.2 Opgaver til primtal

- **Opgave 1.9:**
  Find alle primtal mindre end eller lig 100. Kryds de tal af i nedenstående skema, som ikke er primtal.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- **Opgave 1.10:**
  Vis, at følgende tal er primtal:

  1)107

  2)127

  3)233

- **Opgave 1.11:**
  Find primtalsfaktoriseringen af følgende heltal:

  1)110

  2)79

  3)1728

- **Opgave 1.12:**
  Find primtalsfaktoriseringen af følgende heltal:

  1)100

  2)1000

  3)10000

  4)Hvad er generelt primtalsfaktoriseringen af 10^n hvor n er et positivt heltal?

- **Opgave 1.13: Primorialer**
  Primtalsfaktorisér følgende tal:

  1)2

  2)6

  3)30

  4)210

  Hvad er mon det næste tal i følgen? Denne følge kaldes primorialerne.

- **Opgave 1.14: Sophie Germain-primtal**
  Et primtal p kaldes et *Sophie Germain-primtal* hvis $2p + 1$ også er et primtal. Find de første fem Sophie Germain-primtal.

●● **Opgave 1.15: Mersenne-primtal**
Et primtal på formen $2^p - 1$, hvor p er et andet primtal, kaldes et *Mersenne-primtal*. Find de første tre Mersenne-primtal.

●● **Opgave 1.16: Fermat-primtal**
Et primtal på formen $2^{2^k} + 1$, hvor k er et positivt heltal, kaldes et *Fermat-primtal*. Vis, at $2^{2^k} + 1$ er et Fermat-primtal for $k = 0, 1, 2, 3$.

2 Euklids algoritme

2.1 Største fælles divisorer og euklidisk division

Euklids algoritme er en fremgangsmåde til at bestemme den største fælles divisor i to heltal. Definitionen ses herunder.

Definition 2.1. Lad a og b være heltal. Den *største fælles divisor* for a og b er det største heltal d, som deler både a og b. Helt stringent: Hvis et andet heltal d' deler a og b, da deler d' også d.

Bemærkning 2.2. $\gcd(a,0) = \gcd(0,a) = a$ for alle heltal $a \neq 0$. Vi definerer $\gcd(0,0) = 0$.

Eksempel 2.3. Vi ønsker at finde $\gcd(10,25)$. Divisorerne for 10 er $\pm 1, \pm 2, \pm 5$ og ± 10. Divisorerne for 25 er $\pm 1, \pm 5$ og ± 25. Man kan f.eks. se dette ved at primtalsfaktorisere 10 og 25. Vi ser, at den største fælles divisor er 5.

Det er ikke svært at forestille sig, at det hurtigt bliver svært at bestemme den største fælles divisor af to heltal med den slaviske metode ovenover. Resten af dette afsnit er dedikeret til at give en meget effektiv metode. Lad os først vise et smart hjælperesultat, der viser, at vi kan antage, at a og b i definition 2.1 er positive.

Lemma 2.4. *For to heltal a og b gælder:*

$$\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b)$$

Proof. Vi nøjes med at bevise $\gcd(a,b) = \gcd(-a,b)$. De andre ligheder vises på samme måde. Lad $d_1 = \gcd(a,b)$ og $d_2 = \gcd(-a,b)$. d_1 deler både $-a$ og b, så $d_1 \mid d_2$, da d_2 er største fælles divisor for $-a$ og b. d_2 deler dog også både a og b, så $d_2 \mid d_1$. Da både d_1 og d_2 er positive, må $d_1 = d_2$ som ønsket (se opgave 1.7). ■

Eksempel 2.5. Fra forrige eksempel ved vi, at $\gcd(10,25) = 5$. Per lemmaet har vi $\gcd(-10,25) = 5$ også.

For at kunne udføre Euklids algoritme, skal vi indfører euklidisk divison, også kaldet divison med rest. Vi husker, at absolutværdien $|\cdot|$ er defineret til at være $|a| = a$ hvis $a \geq 0$ og $|a| = -a$, hvis $a < 0$ (eller på godt dansk: $|a|$ er blot a, men med fortegnet fjernet).

Sætning 2.6 (**Euklidisk division**). *Lad a og $b \neq 0$ være heltal. Da eksisterer der unikke heltal q og r, der opfylder $a = qb + r$ og $0 \leq r < |b|$.*

Bevis: Vi starter med at vise, at der findes heltallene q og r med $a = qb + r$. Vi har to tilfælde, nemlig $b > 0$ og $b < 0$. Lad os først antage $b > 0$. Vi kan opdele tallinjen i stykker af halvåbne intervaller $[nb, (n+1)b)$, hvor n løber over alle heltallene:

$$\ldots < -2b < -b < 0 < b < 2b < \ldots \tag{1}$$

a må ligge i netop én af disse intervaller. Lad dette interval være $[qb, (q+1)b)$. Lad $r = a - qb$, da må vi have $0 \leq r < b = |b|$ og $a = qb + r$ som ønsket. Dette viser eksistensdelen for $b > 0$. Hvis $b < 0$, er $-b > 0$. Det, vi lige har vist, giver, at der findes heltal q og r, så $a = q(-b) + r$ med $0 \leq r < -b = |b|$. Ergo kan vi blot vælge $-q$ i stedet for q, og eksistensdelen er færdig. Unikhedsdelen af beviset overlades som opgave 2.7. ■

Sætningen er heldigvis nem at forstå i praksis. Hvis vi f.eks. har to tal a og b, hvor a og b er positive med $a > b$, skal vi blot tjekke, hvor mange gange vi kan lade b gå op i a. Dette tal er q i sætningen. Differensen $a - q \cdot b$ er lig r.

Eksempel 2.7. Se på 146 og 55. Vi ser, at 55 deler 146 to gange, og $146 - 2 \cdot 55 = 36$, og dermed er $146 = 2 \cdot 55 + 36$.

Sætning 2.6 giver anledning til følgende definition.

Definition 2.8. Opskrivningen $a = qb + r$ for to givne heltal a og $b \neq 0$ kaldes for *euklidisk division* eller *division med rest* på a og b. r kaldes for *resten* og q for *kvotienten*.

2.2 Euklids algoritme

Euklids algoritme bygger på en meget vigtig observation. Lad a og b være positive heltal med $a > b$. Hvis vi skal bestemme $\gcd(a, b)$ og vi laver Euklidisk division på a og b, så vi har $a = qb + r$, da vil $\gcd(a, b) = \gcd(b, r)$. Størrelsen $\gcd(b, r)$ er klart nemmere at udregne, fordi $a > b$ og $b > r$, så vi har reduceret problemets størrelse. Vi skal selvfølgelig bevise, at $\gcd(a, b) = \gcd(b, r)$. En anelse mere generelt gælder der:

Lemma 2.9. *For heltal a og b gælder, at hvis $a = qb + r$ for heltal q og r, da vil* $\gcd(a, b) = \gcd(b, r)$.

Bevis: Lad $d_1 = \gcd(a, b)$ og $d_2 = \gcd(b, r)$. Det er nok at vise, at $d_1 \mid d_2$ og $d_2 \mid d_1$, idet begge tal er positive. d_1 deler både a og b, så d_1 deler også r, da $r = a - qb$. Dermed deler d_1 både b og r. Da d_2 er den største fælles divisor for b og r, vil $d_1 \mid d_2$. Da d_2 deler r og b, vil d_2 også dele $a = qb + r$. Men da har vi også $d_2 \mid d_1$, hvilket fuldfører beviset. ■

Euklids algoritme

Lad heltallene a og b være givet. Per lemma 2.4 kan vi antage, at hverken a eller b er negative. Af hensyn til notation omdøber vi $a = r_0$ og $b = r_1$. Skriv $r_0 = q_1 r_1 + r_2$ med $0 \leq r_2 < r_1$. Gentag på følgende måde:

$$r_0 = q_1 r_1 + r_2 \quad \text{hvor } 0 \leq r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 \quad \text{hvor } 0 \leq r_3 < r_2$$

$$\ldots$$

$$r_{n-1} = q_n r_n$$

indtil resten bliver 0. Den sidste ikke-nul rest r_n er lig $\gcd(r_0, r_1) = \gcd(a, b)$.

Vi skal naturligvis bevise, at denne fremgangsmåde er korrekt. Først er det dog på sin plads med et eksempel.

Eksempel 2.10. Vi ønsker at finde $\gcd(1957, 446)$. Vi følger proceduren ovenover:

$$\begin{aligned}
1957 &= 4 \cdot 446 + 173 \\
446 &= 2 \cdot 173 + 100 \\
173 &= 1 \cdot 100 + 73 \\
100 &= 1 \cdot 73 + 27 \\
73 &= 2 \cdot 27 + 19 \\
27 &= 1 \cdot 19 + 8 \\
19 &= 2 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Det ses, at den sidste rest forskellig fra 0 er 1. Ergo er $\gcd(1957, 446) = 1$.

Lad os give et bevis for, at Euklids algoritme fungerer.

Sætning 2.11 (**Korrekthed af Euklids algoritme**). *Euklids algoritme anvendt på to ikke-negative heltal a og b giver den største fælles divisor* $\gcd(a, b)$.

Proof. Lad os først vise, at algoritmen faktisk terminerer (slutter). Når vi laver den beskrevne procedure, får vi en række rester $r_0, r_1, r_2, ...$ Disse rester er alle større end eller lig 0, og vi har $r_0 > r_1 > r_2 > ....$ En vilkårlig rest bliver altså skarpt mindre end den forrige rest i hvert trin. Da de alle er ikke-negative, må proceduren stoppe på et tidspunkt, nemlig når resten bliver 0.

Algoritmen returnerer altså altid et output, nemlig r_n. Vi skal blot vise, at $r_n = \gcd(a, b)$. Dette følger ved blot at benytte lemma 2.9 på hver opskrivning i algoritmen. Vi har nemlig

$$\gcd(a, b) = \gcd(b, r_2) = \gcd(r_2, r_3) = ... = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n$$

som ønsket. ■

Bemærkning 2.12. At bevise korrekthed af en algoritme i datalogi eller matematik involverer altid at vise, at algoritmen slutter, og at algoritmen altid returnerer det korrekte output.

Euklids algoritme er ekstrem effektiv i praksis. I nogle af øvelserne kan I undersøge, hvornår Euklids algoritme indeholder flest trin, altså hvornår den er mindst effektiv. Man kan faktisk vise, at antallet af trin aldrig er mere end 5 gange antallet af cifre i det mindste af de to tal a og b [2]. Hvis f.eks. a eller b har 100 cifre, da kræver algoritmen ikke mere end 500 trin uanset størrelsen af det andet tal. Til sammenligning kan selv en billig mobiltelefon foretage milliarder af beregninger på et sekund.

2.3 Opgaver

- **Opgave 2.1:**
  Brug Euklids algoritme til at udregne følgende:

  1) $\gcd(134, 82)$

  2) $\gcd(211, -78)$

  3) $\gcd(712, 90)$

- **Opgave 2.2:**
  Brug Euklids algoritme til at udregne følgende:

  1) $\gcd(-245, 135)$

  2) $\gcd(1200, 195)$

  3) $\gcd(-28, -568)$

- **Opgave 2.3:**
  Hvad er $\gcd(p, q)$, når p og q er forskellige primtal?

- **Opgave 2.4:**
  Udregn følgende:

  1) $\gcd(2003, -17)$ [Vink: 2003 er et primtal]

  2) $\gcd(66000, 11)$

- **Opgave 2.5:**
  Antag, at vi vælger at droppe antagelsen om, at resten r fra euklidisk division skal være større end eller lig 0, men blot at $r < |b|$. Giv et eksempel, der viser, at division med rest ikke behøver at have unik rest og kvotient.

- **Opgave 2.6:**
  Bevis, at hvis d_1 og d_2 begge er største fælles divisorer for a og b, da vil $d_1 = d_2$. [Vink: lad dig inspirere af beviset for lemma 2.4]

- **Opgave 2.7: Unikhed i sætning 2.6**
  Lad a og $b \neq 0$ være heltal. I beviset for sætning 2.6 om euklidisk division har vi vist, at der findes heltal q, r, så $a = qb + r$ med $0 \leq r < |b|$. Vis, at q og r er unikke. [Vink: Antag, at q', r' er en anden løsning. Vis, at der må gælde $b(q - q') = r' - r$. Idet $0 \leq r, r' < |b|$, må deres forskel $|r' - r|$ være mindre end $|b|$. Brug dette til at vise $|q - q'| < 1$ og konkludér, at $q = q'$ og $r = r'$, så opskrivningen $a = qb + r$ er unik.]

  I de kommende opgaver vil vi undersøge, for hvilke a og b Euklids algoritme kræver flest trin.

- **Opgave 2.8: Fibonacci-tal**
  Definér $F_0 = 0, F_1 = 1$ og $F_n = F_{n-1} + F_{n-2}$. Sådan en definition kaldes *rekursiv*. Tallene F_n udgør en talfølge kaldet *Fibonacci-tallene*.

  1) Overbevis dig selv om, at de første led i følgen er:

$$0, 1, 1, 2, 3, 5, 8, ... \tag{2}$$

2)Udregn de næste fem led i Fibonacci-følgen (2), dvs. F_7, F_8, F_9, F_{10} og F_{11}.

3)Lav euklidisk division på F_{n+2} med F_{n+1} ($a = F_{n+2}$ og $b = F_{n+1}$ i definitionen). Hvad er resten?

●● **Opgave 2.9:**

1)Udregn $\gcd(3,2)$, $\gcd(5,3)$, $\gcd(8,5)$, $\gcd(13,8)$, $\gcd(21,13)$ med Euklids algoritme (ja, det virker lidt unødvendigt, men der er en pointe!). Hvor mange trin bruger du i hvert tilfælde? [Vink: prøv at starte bagfra, altså udregn $\gcd(21,13)$, derefter $\gcd(13,8)$ osv. Kan du genbruge nogle udregninger?]

2)Bevis, at $\gcd(F_{n+2}, F_{n+1}) = 1$ for alle positive heltal n ved at benytte Euklids algoritme. Konkludér ud fra udregningen, at algoritmen bruger n trin på at udregne $\gcd(F_{n+2}, F_{n+1}) = 1$.

Hvor hurtig er Euklids algoritme? I de ovenstående opgaver har vi vist, at Fibonacci-tallene F_n giver en nedre grænse på, hvor hurtig algoritmen udregner $\gcd(F_{n+2}, F_{n+1})$. Dette kræver n trin. Er to på hinanden følgende Fibonacci-tal det "værste" input, man kan kan give algoritmen? Svaret viser sig at være ja:

Sætning 2.13 (**Lamé's sætning**). *Lad a og b være heltal med $a > b \geq 1$ og $b < F_{n+2}$. Udregningen af $\gcd(a,b)$ med Euklids algoritme indeholder færre end n trin.*

Vi refererer til [1, s. 935 - 936] for et bevis for denne sætning. Denne sætning kan man bruge til at give en konkret øvre grænse for Euklids algoritme for alle input a og b.

3 Modulær aritmetik

3.1 Motivation og regneregler

Her til slut vil vi indføre en ny måde at regne med heltal på. "Ny" er faktisk ikke helt korrekt, da I implicit har regnet på den her måde før. Forestil jer et ur med 24 timer. Hvis klokken er 23, og vi går 2 timer frem, er klokken ikke 25, men derimod 1. Det er præcis denne form for regning, vi skal have formaliseret.

Definition 3.1. Lad n være et positivt heltal og a, b heltal. Vi siger, at a er *kongruent med b modulo n* hvis $n \mid (a-b)$, og vi skriver $a \equiv b \pmod{n}$.

Eksempel 3.2. Lad $n = 24$. Vi hævder, at $25 \equiv 1 \pmod{24}$. Vi har $25-1 = 24$, og 24 deler 24, hvilket viser det ønskede. Dette er en matematisk formalisering af, at klokken 25 og klokken 1 er det samme. En matematiker vil sige, at 25 og 1 er kongruente modulo 24.

Bemærkning 3.3. For alle positive n er $n \equiv 0 \pmod{n}$. Hvorfor?

Eksempel 3.4. Der er 360° hele vejen rundt i en cirkel. Hvis vi starter i et vilkårligt punkt og bevæger os 360° i én af de to retninger rundt i cirklen, havner vi præcist der, hvor vi startede. Dette er en mulig visuel fortolkning af udsagnet $360 \equiv 0 \pmod{360}$. På samme måde ses, at hvis vi bevæger os 400° rundt, svarer det blot til at bevæge sig 40° i samme retning. Med vores nye begreb: $400 \equiv 40 \pmod{360}$.

Hvordan regner vi så mere konkret på kongruenser? Følgende proposition giver endnu en smart fortolkning af begrebet.

Proposition 3.5. *Følgende udsagn er ækvivalente for heltal a og b samt et positivt heltal n:*

(i) $a \equiv b \pmod{n}$

(ii) Der findes et heltal k, så $a = b + kn$.

(iii) a og b har samme rest ved division med n.

Bevis: Vi beviser propositionen ved at vise, at (i) medfører (ii), at (ii) medfører (iii), og at (iii) medfører (i). Lad os først vise, at (i) medfører (ii). Hvis (i) gælder, må $n \mid (a-b)$ per definition. Men per definition af delelighed betyder dette, at $a-b = k \cdot n$ for et heltal k, og dermed gælder (ii) altså. Antag, at (ii) gælder. Lav euklidisk division $a = q_1 \cdot n + r_1$ og $b = q_2 \cdot n + r_2$, hvor $0 \leq r_1, r_2 < n$. Vi har da:

$$\begin{aligned} r_1 - r_2 &= (a - q_1 \cdot n) - (b - q_2 \cdot n) = (a-b) - q_1 \cdot n + q_2 \cdot n \\ &= k \cdot n + (q_2 - q_1) \cdot n = (k + q_2 - q_1) \cdot n \end{aligned}$$

Vi ser, at n deler højresiden, og altså må n dele $r_1 - r_2$. Men eftersom både r_1 og r_2 er ikke-negative og mindre end n, bliver vi nødt til at have $r_1 - r_2 = 0$ dvs. $r_1 = r_2$, og (iii) gælder. Antag nu, at (iii) gælder. Dermed kan vi skrive $a = q_1 \cdot n + r$ og $b = q_2 \cdot n + r$. Vi har da:

$$a - b = (q_1 \cdot n + r) - (q_2 \cdot n + r) = q_1 \cdot n - q_2 \cdot n = (q_1 - q_2) \cdot n$$

Vi ser, at n deler højresiden og dermed også $a-b$, så per definition har vi $a \equiv b \pmod{n}$, og (i) gælder. Beviset er færdigt. ■

Sætningen ovenover fortæller os noget meget vigtigt, som vi opsummerer i følgende korollar (følgeresultat).

Korollar 3.6. *Lad n være et positivt heltal, lad a være et heltal, $a = q \cdot n + r$ divisionen med rest af a og n. Da er $a \equiv r \pmod{n}$.*

Det følgende resultat er også vigtigt i vores mål for at forstå kongruenser.

Proposition 3.7. *Lad n være et positivt heltal. For heltal a, b og c gælder*

(i) $a \equiv a \pmod{n}$ *(refleksivitet).*

(ii) Hvis $a \equiv b \pmod{n}$ *gælder også* $b \equiv a \pmod{n}$ *(symmetri).*

(iii) Hvis $a \equiv b \pmod{n}$ *og* $b \equiv c \pmod{n}$ *gælder* $a \equiv c \pmod{n}$ *(transitivitet).*

Bevis: Se opgaverne. ■

Fortolkningen af propositionen ovenover er, at $\equiv$ opfører sig på samme måde som et klassisk lighedstegn $=$. En relation som $=$ og $\equiv$, der opfylder de tre egenskaber i propositionen herover, kaldes en *ækvivalensrelation*. Næste skridt er at definere regning modulo n. Mere formelt, lad a og b være heltal. Det ville være praktisk, hvis vi kunne definere $a+b$ modulo n helt naivt og ligeledes for $\cdot$. Men hvordan kan vi være sikker på, at dette virker? Lad c og d være heltal med $a \equiv c \pmod{n}$ og $b \equiv d \pmod{n}$. Kan vi være sikre på, at $a + b \equiv c + d \pmod{n}$? Og kan vi være sikre på, at $ab \equiv cd \pmod{n}$? Svaret er heldigvis ja.

Proposition 3.8. *Med antagelser som i forrige paragraf gælder:*

$$a + b \equiv c + d \pmod{n} \quad \textit{og} \quad ab \equiv cd \pmod{n}$$

Bevis: Per proposition 3.5 har vi $a = c + k_1 \cdot n$ og $b = d + k_2 \cdot n$ for heltal nogle heltal k_1 og k_2. Vi har da

$$a + b = c + k_1 \cdot n + d + k_2 \cdot n = c + d + (k_1 + k_2) \cdot n,$$

så igen per proposition 3.5 har vi $a + b \equiv c + d \pmod{n}$. Dermed er $+$ en veldefineret regneregel. For $\cdot$ har vi

$$\begin{aligned} ab &= (c + k_1 \cdot n)(d + k_2 \cdot n) \\ &= cd + c \cdot k_2 \cdot n + k_1 \cdot n \cdot d + k_1 \cdot n \cdot k_2 \cdot n \\ &= cd + (c \cdot k_2 + k_1 \cdot d + k_1 \cdot k_2 \cdot n) \cdot n, \end{aligned}$$

og igen giver proposition 3.5, at $ab \equiv cd \pmod{n}$, så $\cdot$ er også en veldefineret regneregel. ■

Nu ved vi, at vi kan regne med heltal modulo n på næsten samme måde som med almindelige heltal. Vi skal blot lægge/gange sammen som sædvanligt, hvorefter vi plejer at reducere modulo n (dvs. erstatte resultatet med det mindste positive tal, det er kongruent med modulo n).

Eksempel 3.9. Vi har $13 + 2 \cdot 12 = 37 \equiv 2 \pmod{5}$, fordi 2 er resten, når vi laver division med rest på 37 med 5. Vi kunne faktisk også skyde genvej og bemærke, at $13 \equiv 3 \pmod{5}$ og $12 \equiv 2 \pmod{5}$, så vi får $13 + 2 \cdot 12 \equiv 3 + 2 \cdot 2 \equiv 7 \equiv 2 \pmod{5}$. Dette trick er tilladt pga. proposition 3.8.

Eksempel 3.10. Lad os tage et mere snedigt eksempel. Hvad er 9^{100} modulo 10? Vi bemærker, at $9 \equiv -1 \pmod{10}$. 100 er et lige tal, så $(-1)^{100} = 1$ (husk, at et lige antal fortegn går ud). Dvs. $9^{100} \equiv (-1)^{100} \equiv 1 \pmod{10}$. Dette fortæller os også, at 1 er det sidste ciffer i 9^{100}. Hvorfor?

3.2 Opgaver

- **Opgave 3.1:**
  Find det mindste positive heltal, som passer ind i følgende:
  1) $1 \equiv ?\pmod 4$
  2) $32 \equiv ?\pmod{24}$
  3) $49 \equiv ?\pmod{32}$
  4) $144 \equiv ?\pmod{23}$
  5) $7 \cdot 4 \equiv ?\pmod 5$
  6) $4 \cdot 5 \equiv ?\pmod 7$

- **Opgave 3.2:**
  Vis, at følgende gælder:
  1) $1 \equiv -1 \pmod 2$
  2) $10234875 \equiv 0 \pmod{10234875}$
  3) $7 \equiv 3 \pmod 4$
  4) $17 \equiv 1 \pmod 4$
  5) $22 \equiv 2 \pmod 5$
  6) $11 \equiv 3 \pmod 4$
  7) $11 + 3 \equiv 2 \pmod{12}$

- **Opgave 3.3:**
  Vis, at der for heltal a og b gælder

$$(a+b)^2 \equiv a^2 + b^2 \pmod 2.$$

- **Opgave 3.4:**
  Bevis proposition 3.7. [Vink til (iii): $a - c = a - b + b - c$]

- **Opgave 3.5:**
  Man kan vise, at der for et primtal p gælder

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

  for alle heltal a. Dette resultat er kendt som *Fermat's lille sætning*. Brug denne sætning til at vise, at der for alle heltal a og primtal p gælder

$$(a+b)^p \equiv a^p + b^p \pmod p.$$

  Dette resultat kaldes ofte *Freshman's dream*.

- **Opgave 3.6:**
  Udregn følgende
  1) $3^{100} \equiv ?\pmod{10}$.
  2) $5^{100} \equiv ?\pmod 8$ [Vink: start med at reducere 5^2 modulo 8]
  3) $6^{1000} \equiv ?\pmod 5$

3.3 Perspektivering og anvendelser af modulær aritmetik

3.3.1 Regneregler for delelighed

Lad os som en første anvendelse bevise proposition 1.6. Vi skal dog lige genkalde, hvordan 10-tals-systemet fungerer. Ethvert (positivt) heltal a har en opskrivning

$$a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10 + a_0,$$

hvor $a_k, ..., a_0$ er cifrene i tallet fra venstre mod højre. F.eks. har vi

$$1742 = 1 \cdot 10^3 + 7 \cdot 10^2 + 4 \cdot 10 + 2$$

Bevis for proposition 1.6: Punkt (i) gælder per definition. For at vise (ii), skriv da heltallet a som $a = a_k a_{k-1} ... a_0$, hvor $a_k, a_{k-1}, ..., a_0$ betegner cifrene fra venstre mod højre. Da har vi:

$$a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_0$$

Vi husker, at $3 \mid a$ hvis og kun hvis $a \equiv 0 \pmod 3$, og at $10 \equiv 1 \pmod 3$. Reducerer vi summen ovenover modulo 3 ovenover fås altså:

$$a \equiv a_k \cdot 1 + a_{k-1} \cdot 1 + ... + a_0 \cdot 1 \equiv a_k + a_{k-1} + ... + a_0 \pmod 3$$

Højresiden er netop tværsummen for a. Altså deler 3 a hvis og kun hvis 3 deler tværsummen. For at vise (iii), skal vi blot bemærke, at $10 \equiv 0 \pmod 5$, så vi har med notationen ovenover, at

$$a \equiv a_0 \pmod 5,$$

hvilket klart giver, at 5 deler a hvis og kun hvis 5 deler det sidste ciffer, altså at dette ciffer er 0 eller 5. Strategien til at vise (iv) er identisk med strategien for (ii). (v) vises på præcist samme facon som (iii). Lad os vise (vi). Vi ser, at $10 \equiv -1 \pmod{11}$, så $10^k \equiv (-1)^k \pmod{11}$ for alle positive heltal k. Reducerer vi summen modulo 11, fås:

$$a \equiv a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + ... + a_0 \cdot 1 \pmod{11}$$

Dette er netop den alternerende tværsum, så 11 deler a hvis og kun hvis 11 deler den alternerende tværsum. ■

3.3.2 ISBN

Et *ISBN* (International Standard Book Number) er en serie af tal, der står i (næsten) alle bøger, som identificerer netop den bog. Vi ser her på 13-ciffer-ISBN. Lad os se på et eksempel:

978-0-471-43334-7

978 er altid de første tre cifre. De andre cifre fortæller om udgiver, titel med mere. Det sidste ciffer er et såkaldt *tjek-ciffer*. Lad x_1, x_2, ..., x_{13} betegne de 13 cifre fra venstre mod højre. Tjek-cifferet er det ciffer x_{13} mellem 0 og 9, der opfylder:

$$(x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + x_{13}) \equiv 0 \pmod{10}$$

I ovenstående eksempel er 7 tjek-cifferet. Lad os verificere dette. Vi udregner:

$$9 + 3 \cdot 7 + 8 + 3 \cdot 0 + 4 + 3 \cdot 7 + 1 + 3 \cdot 4 + 3 + 3 \cdot 3 + 3 + 3 \cdot 4 + 7 = 110 \equiv 0 \pmod{10}$$

Tjek-cifre tillader en hurtig metode til at tjekke gyldigheden af ISBN for bøger. Man kan f.eks. vise, at tjek-cifferet altid bliver ugyldigt, hvis blot ét ciffer i nummeret ændres.

●● **Opgave 3.7:**
Lad os regne nogle tjek-cifre!

1)Find tjek-cifferet for 978-0-387-24527-?.

2)Find tjek-cifferet for 978-82-15-02710-?.

3.3.3 Løsning af heltalsligninger

Et essentielt spørgsmål i talteori er, hvornår ligninger har heltalsligninger. F.eks. har ligningen $x^2 + y^2 = 1$ uendelig mange heltalsløsninger (som udgør enhedscirklen med centrum i origo). I heltallene er der kun fire løsninger, nemlig $(0, 1), (0, -1), (1, 0)$ og $(-1, 0)$. Dette kan vises ved blot at bemærke, at hvis $|x| > 1$ eller $|y| > 1$, da bliver x^2+y^2 klart større end 1. Men hvad med en ligning som $3x^2+4y^2 = 98$? Hvordan kan vi undersøge, om der findes en heltalsløsning på en nem måde? Én metode er følgende sætning (bemærk det meget simple bevis!):

Sætning 3.11 (**Lokale obstruktioner**). *Hvis en ligning i heltallene ingen løsning har modulo n, hvor n er et vilkårligt positivt heltal, da findes ingen løsninger i heltallene heller.*

Bevis: Antag, at vi har en ligning med ingen løsninger modulo n. Hvis et heltal a er en løsning til ligningen, da vil a også være en løsning til ligningen modulo n, hviket er en selvmodsigelse. Altså findes ingen heltalsløsninger til ligningen. ■

Sætningen er simpel, men er også baseret på en smule held. Ikke desto mindre kan den til tider føles som magi, når man benytter den.

Eksempel 3.12. Lad os undersøge ligningen $3x^2+4y^2 = 98$. Lad os reducere ligningen modulo 3. Da fås $98 = 3x^2 + 4y^2 \equiv y^2 \pmod 3$ og da $98 \equiv 2 \pmod 3$, bliver ligningen blot til $y^2 \equiv 2 \pmod 3$. Alle heltal har en rest på 0, 1 eller 2, når man laver division med rest med 3. Dog har vi:

$$0^2 \equiv 0 \pmod 3, \quad 1^2 \equiv 1 \pmod 3, \quad 2^2 \equiv 1 \pmod 3$$

og altså findes ingen løsning til $y^2 \equiv 2 \pmod 3$ og dermed heller ingen heltalsløsning til den oprindelige ligning $3x^2 + 4y^2 = 98$.

En særlig interessant anvendelse historisk set omhandler summer af kvadrater. Hvilke heltal a kan skrives på formen $a = x^2 + y^2$, hvor x og y er heltal? Første skridt er at bestemme, hvornår et primtal kan skrives som en sum af to kvadrater. Vi viser først følgende hjælperesultat:

Lemma 3.13. *Et kvadrattal (dvs. et heltal a på formen $a = b^2$ for et heltal b) er kongruent med 0 eller 1 modulo 4.*

Bevis: Lad $a = b^2$ være et kvadrattal. b har rest 0, 1, 2 eller 3, når man laver divison med rest med 4. Lad os undersøge disse tilfælde for sig:

$$\begin{aligned}
b \text{ har rest } 0: &\quad b^2 \equiv 0 \pmod 4 \\
b \text{ har rest } 1: &\quad b^2 \equiv 1 \pmod 4 \\
b \text{ har rest } 2: &\quad b^2 \equiv 4 \equiv 0 \pmod 4 \\
b \text{ har rest } 3: &\quad b^2 \equiv 9 \equiv 1 \pmod 4
\end{aligned}$$

Disse udregninger viser det ønskede. ■

Dette fører til følgende observation:

Proposition 3.14. *Et ulige primtal p, der kan skrives som en sum af to kvadrater, er kongruent med 1 modulo 4.*

Bevis: Et ulige primtal er kongruent med 1 eller 3 modulo 4 (overvej hvorfor). Lad $p = x^2 + y^2$ for heltal x og y. Da er x^2 og y^2 hver især kongruente med 0 eller 1 modulo 4 per forrige lemma. Vi har da mulighederne $p \equiv 0, 1, 2 \pmod 4$. 0 og 2 er dog udelukket som tidligere nævnt, og derfor er $p \equiv 1 \pmod 4$. ■

Eksempel 3.15. Primtallene 3, 7 og 11 kan ikke skrives som en sum af to kvadrater, da de hver er kongruente med 3 modulo 4. 5 kan skrives som en sum af to kvadrater, f.eks. er $5 = 2^2 + 1^2$.

Da $p \equiv 1 \pmod 4$ er en nødvendig betingelse for, at et ulige primtal p kan skrives som en sum af to kvadrater, kan man spørge sig selv, om det også er en tilstrækkelig betingelse. Med andre ord, kan alle primtal kongruent med 1 modulo 4 skrives som en sum af to kvadrater. Følgende sætning giver det fulde svar:

Sætning 3.16. ***Fermat's sætning om summer af kvadrater*** *Et primtal p kan skrives som en sum af to kvadrater hvis og kun hvis $p = 2$ eller $p \equiv 1 \pmod 4$.*

Bevis: Beviset er ret omstændigt. En grundig gennemgang kan f.eks. findes i kapitel 6 i [6]. ■

Og for generelle heltal har vi:

Sætning 3.17. *Et positivt heltal n er en sum af to kvadrater hvis og kun hvis ethvert primtal p kongruent med 3 modulo 4 i n's primtalsfaktorisering dukker op med en lige potens.*

Bevis: Vi henviser atter til kapitel 6 i [6]. ■

Eksempel 3.18. Betragt 4410 og 188760. Vi har $4410 = 2 \cdot 3^2 \cdot 5 \cdot 7^2$. 3 og 7 er de eneste primtal kongruente med 3 modulo 4 i faktoriseringen, og de har begge en lige potens. Ergo er 4410 lig en sum af to kvadrater. En mulighed er $4410 = 21^2 + 63^2$. En fremgangsmåde til at bestemme sådan en opskrivning er mere omstændig, men matematik-software som f.eks. Maple har kommandoer til det. Tværsummen af 188760 er 30, som 3 deler. Derfor er 3 en divisor i 188760. Deler $3^2 = 9$ 188760? Nej, thi tværsummen er ikke delelig med 9. Derfor er 3 en primdivisor med en ulige potens, så 188760 kan ikke skrives som en sum af to kvadrater.

3.3.4 Kvadratiske rester

I forrige afsnit undersøgte vi, hvornår et primtal er en sum af to kvadrater. Dette problem er tæt relateret til bestemmelse af *kvadratiske rester*. Vi har faktisk allerede set eksempler fra denne teori i eksempel 3.12.

Definition 3.19. Et heltal $a \neq 0$ er *kvadratisk rest* modulo primtallet $p > 2$ hvis der eksisterer et heltal x, så $x^2 \equiv a \pmod p$. Ellers kaldes a en *kvadratisk ikke-rest*.

Vil man finde ud af, om et heltal a er en kvadratisk rest modulo p, skal man altså undersøge, om der findes et heltal x, så $x^2 \equiv a \pmod p$.

Bemærkning 3.20. 0 betegnes hverken som en kvadratisk rest eller ikke-rest modulo noget primtal. Der er flere grunde til dette, specielt når man vil arbejde mere algebraisk med teorien, se f.eks. [6, s. 33]. Der er en række tekniske grunde til at udelukke primtallet 2 fra definitionen. Dog er problemet med at finde løsninger til alle andengradsligninger modulo 2 ikke svært, se opgave 3.15.

Eksempel 3.21. Lad $p = 7$ og $a = 2$. Idet $3^2 \equiv 2 \pmod 7$, er 2 en kvadratisk rest modulo 7. Dog er 5 en kvadratisk ikke-rest modulo 7. I eksempel 3.12 så vi, at 2 er en kvadratisk ikke-rest modulo 3.

For små primtal p er det ikke svært at kortlægge, hvilke heltal, der er kvadratiske rester modulo p, som følgende lemma viser:

Lemma 3.22. *Lad $p > 2$ være et primtal. En kvadratisk rest modulo p er kongruent til netop én af tallene* $1 \pmod p, 2^2 \pmod p, 3^2 \pmod p, ..., (p-1)^2 \pmod p$.

Proof. Antag, at a er en kvadratisk rest modulo p. Da findes et heltal x, så $x^2 \equiv a \pmod p$. Hvis $x < p$, er vi færdige. Ellers skriver vi $x = qp + r$, hvor $0 \leq r < p$. Da er $x \equiv r \pmod p$ og dermed $r^2 \equiv a \pmod p$. Dette beviser lemmaet. ■

Lad os se dette lemma i praksis.

Eksempel 3.23. Lad os finde samtlige kvadratiske rester modulo 7 ved at opstille følgende tabel:

a	1	2	3	4	5	6
a^2	1	4	9	16	25	36
$a^2 \pmod 7$	1	4	2	2	4	1

Af den her tabel aflæser vi, sammen med lemma 3.22, at alle kvadratiske rester modulo 7 er kongruent med enten 1, 2 eller 4. Så f.eks. er 79 kvadratisk rest modulo 7, da $79 \equiv 2 \pmod 7$, som du kan tjekke. På samme måde ser vi, at 26 er en kvadratisk ikke-rest modulo 7, idet $26 \equiv 5 \pmod 7$, og 5 ikke er en af tallene på tredje række i tabellen ovenover.

Vi kan benytte fremgangsmåden i eksemplet til at finde alle mulige rester for et kvadrattal ved division med et heltal n (der ikke nødvendigvis er et primtal). Her skal vi blot huske at inkludere 0.

Eksempel 3.24. Hvilke rester kan vi få, når vi deler et kvadrattal med 6? Lad os lave en tabel:

a	0	1	2	3	4	5
a^2	0	1	4	9	16	25
$a^2 \pmod 6$	0	1	4	3	4	1

Vi ser, at det er muligt at få resterne $0, 1, 3$ og 4. Dog er det umuligt at dele et kvadrattal med 6 og få en rest på 2 eller 5.

Lad os se på en simpel anvendelse af teorien, vi har arbejdet med indtil videre:

Eksempel 3.25. Se på talfølgen $75, 775, 7775, \ldots$. Vi hævder, at denne følge ikke indeholder nogle kvadrattal. Ved at lave en simpel omskrivning af følgen til $70 + 5, 770 + 5, 7770 + 5, \ldots$ ser vi, at alle led i følgen er kongruent til 5 modulo 7. Per eksempel 3.23 kan et kvadrattal ikke have rest 5 modulo 7, ergo kan ingen tal i følgen være kvadrattal.

Lad os afslutte dette afsnit med et meget interessant faktum. Lad p og q være forskellige ulige primtal. Man kan spørge sig selv, om der er nogen som helst sammenhæng mellem ligningerne:

$$x^2 \equiv p \pmod{q} \quad \text{og} \quad x^2 \equiv q \pmod{p}$$

Svaret viser sig at være ja. Vi har resultatet:

Sætning 3.26 (**Kvadratisk reciprocitet**)**.** *Lad $p, q > 2$ være forskellige primtal.*

1. *Hvis $p \equiv 1 \pmod 4$ eller $q \equiv 1 \pmod 4$, er p kvadratisk rest modulo q hvis og kun hvis q er kvadratisk rest modulo p. Hvis både $p \equiv 3 \pmod 4$ og $q \equiv 3 \pmod 4$, er p kvadratisk rest modulo q hvis og kun hvis q er en kvadratisk ikke-rest modulo p.*
2. *-1 er en kvadratisk rest modulo p hvis og kun hvis $p \equiv 1 \pmod 4$.*
3. *2 er en kvadratisk rest modulo p hvis og kun hvis $p \equiv 1 \pmod 8$ eller $p \equiv 7 \pmod 8$.*

Historien bag denne sætning er lang og interessant. Leonhard Euler var den første til at beskrive et resultat som sætningen ovenover i 1744. Adrien-Marie Legendre var den første til at udgive sætningen i en moderne formulering i 1788 [3, s. 6] sammen med et ufuldstændigt bevis. Det første fulde bevis blev fundet af Carl Friedrich Gauss, som i 1818 havde udgivet ikke mindre end seks forskellige beviser, og yderligere to blev fundet i hans noter efter hans død [3, s. 9]. Gauss kaldte sætningen "aureum theorema", der betyder "den gyldne sætning" på latinsk. Sætningen og teknikkerne til at bevise den er senere blevet en hjørnesten i meget moderne matematik. Til slut skal nævnes, at der findes over 300 forskellige beviser for sætningen [6, s. 34]. For en ikke-komplet liste, se [4].

3.4 Opgaver

- **Opgave 3.8:**

  Lad $p > 2$ være et primtal. Lad a være et kvadrattal. Vis, at a er en kvadratisk rest modulo p.

- **Opgave 3.9:**
  Brug lemma 3.22 til at finde alle kvadratiske rester modulo:

  1)3

  2)5

  3)11

- **Opgave 3.10:**
  Hvad er de mulige rester, hvis man dividerer et kvadrattal med:

  1)4

  2)8

  3)14

- **Opgave 3.11:**

  1)Betragt talfølgen $2, 22, 222, 2222, ...$ Bevis, at intet tal i denne følge er et kvadrattal.

  2)Gentag for talfølgen $1, 11, 111, 1111, ...$
  [Vink: benyt evt. opgave 3.10]

- **Opgave 3.12:**

  Vi vil verificere den kvadratiske reciprocitetslov, sætning 3.26, for primtallene $p = 3$ og $q = 5$. Det er helt lovligt at bruge resultatet fra opgave 3.9.

  1)Bemærk, at $5 \equiv 1 \pmod 4$. Vis, at 3 er kvadratisk rest modulo 5 og, at 5 er kvadratisk rest modulo 3.

  2)Vis, at -1 er en kvadratisk rest modulo 5, men en kvadratisk ikke-rest modulo 3.

  3)Vis, at 2 er en kvadratisk ikke-rest modulo 3 og 5.

  4)Stemmer alle delopgaverne overens med sætningen?

- **Opgave 3.13:**

  Vi verificerer igen den kvadratiske reciprocitetslov, denne gang for $p = 7$ og $q = 11$.

  1)Vis, at 7 er en kvadratisk ikke-rest modulo 11, men at 11 er en kvadratisk rest modulo 7.

  2)Vis, at -1 er en kvadratisk ikke-rest modulo 7 og 11.

  3)Vis, at 2 er en kvadratisk rest modulo 7, men en kvadratisk ikke-rest modulo 11.

  4)Stemmer alle delopgaverne overens med sætningen?

- **Opgave 3.14:**
  Betragt ligningen $x^2 - 5y^2 = 2$. Vi viser, at denne ligning ingen heltalsløsninger har

for x og y.

1)Reducér ligningen modulo 5

2)Vis, at ligningen har en løsning modulo 5 hvis og kun hvis 2 er kvadratisk rest modulo 5

3)Vis, at ligningen ingen heltalsløsninger har. [Vink: sætning 3.11]

●●●● **Opgave 3.15: Tilfældet $p = 2$**

1)Opskriv samtlige andengradsligninger (dvs. ligninger på formen $ax^2 + bx + c = 0$) modulo 2. [Vink: koefficienterne a, b og c er hver især kongruente til enten 0 eller 1 modulo 2, så det er nok at betragte disse tilfælde. Husk dog, at $a \neq 0$!]

2)Hvilke af ligningerne har heltalsløsninger modulo 2? Find løsningerne til dem, der har.

●●●● **Opgave 3.16: Andengradsligninger modulo p**

En motivation for at kigge på kvadratiske rester angår løsninger til andengradsligninger modulo et primtal $p > 2$. Man kan vise, at et polynomium $ax^2 + bx + c \pmod p$ har rødder, netop hvis diskriminanten $D = b^2 - 4ac$ fra tidligere er en kvadratisk rest modulo p [6, p. 32].

1)Findes der rødder i polynomiet $3x^2 + 2x + 4 \pmod 5$? Hvis ja, hvad er rødderne?

2)Findes der rødder i polynomiet $x^2 + 7x + 3 \pmod{11}$? Hvad med modulo 13?

Lad os til sidst se, hvordan dette kan bruges til at afgøre, om der findes heltalsrødder i et andengradspolynomium:

3)Findes der "almindelige" heltalsrødder i polynomiet $x^2 + 17x + 2$? [Vink: Benyt det ovenstående med sætning 3.11. Man skal ikke lede længe efter et n, der virker.]

4 Litteraturliste

[1] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*. Massachusetts Institute of Technology, 3 edition, 2009. ISBN 978-0-262-53305-8.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, 3 edition, 2003. ISBN 978-0-471-43334-7.

[3] Franz Lemmermeyer. *Reciprocity Laws From Euler to Eisenstein*. Springer-Verlag, 3 edition, 2000. ISBN 3-540-66957-4.

[4] Franz Lemmermeyer. Proofs of the quadratic reciprocity law, 2013. URL `https://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`.

[5] Jesper Lützen. *Diskrete Matematiske Metoder*. Københavns Universitet, 2 edition, 2019.

[6] Morten S. Risager. *Introduction to number theory*. University of Copenhagen, 2020. URL `http://web.math.ku.dk/~risager/introtal/main`.