Marianne Terp og Peter Trosborg: Noter om talteori. Februar 1995.

TALTEORI

1. Primtal

Som bekendt siger vi, at et tal $d \in N$ *går op i* et tal $a \in N$, (eller at d er *divisor* i a), og vi skriver

$$d|a \quad ,$$

dersom a kan skrives på formen

$$a = q \cdot d \ , \quad \text{hvor} \quad q \in N \quad .$$

Når d er divisor i a, siger vi, at a er *delelig* med d. En divisor i a, der ikke er lig med a, kaldes en *ægte* divisor. Ethvert tal har som divisorer i hvert fald sig selv og tallet 1; disse kaldes for de *trivielle* divisorer. Hvis p er et naturligt tal større end 1, der kun har de trivielle divisorer, kaldes p et *primtal*. Naturlige tal større end 1, der ikke er primtal, kaldes *sammensatte* tal.

Eksempel 1.1. Der gælder $3|18$, fordi $18 = 6 \cdot 3$; 18 er ikke et primtal, da 3 er divisor i tallet; 18 er et sammensat tal. Tallet 17 er et primtal, fordi 1 og 17 er de eneste divisorer i 17. Tallet 1 er ikke et primtal, og det er heller ikke et sammensat tal.

Bemærk, at relationen "går op i" er transitiv, dvs. at der gælder

$$a|b \ \wedge \ b|c \quad \Rightarrow \quad a|c \quad .$$

Hvis nemlig $b = q_1 a$ og $c = q_2 b$, gælder $c = q_2 q_1 a$ og dermed $a|c$.

Sætning 1.1. Lad $n \in N$ være større end 1. Lad d være den mindste divisor større end 1 i tallet n. Så er d et primtal.

Bevis. Hvis d ikke var et primtal, ville d have en ægte divisor større end 1. Denne ville ifølge bemærkningen ovenfor også være divisor i n i strid med,

at d var den mindste sådanne divisor. $\diamond$

Primtallenes rolle som byggesten for alle naturlige tal fremgår af følgende sætning:

Sætning 1.2. (Aritmetikkens fundamentalsætning). Ethvert naturligt tal større end 1 kan på entydig måde opløses i primfaktorer.

Bevis. Beviset falder i to dele. Først vises eksistensen af en sådan opløsning, altså at ethvert tal kan skrives som produkt af faktorer, der alle er primtal. Dernæst vises, at en sådan fremstilling er i det væsentlige entydig, altså at der ikke kan findes to forskellige primtalsopløsninger af samme tal. Bemærk, at det er beviset for entydigheden, der kræver mest arbejde.
Eksistens: Lad n være et vilkårligt naturligt tal. Lad d_1 være den mindste divisor større end 1 i n. Så er d_1 et primtal, og vi kan skrive $n = d_1 \cdot q_1$, hvor $q_1 \in N$. Hvis $q_1 = 1$, er vi færdige. Ellers fortsættes således: lad d_2 være den mindste divisor større end 1 i q_1; så er d_2 et primtal, og vi har $n = d_1 \cdot d_2 \cdot q_2$, $q_2 \in N$. Hvis $q_2 = 1$, er vi færdige. Ellers fortsættes som før. Da tallene $q_1, q_2, ...$ udgør en aftagende følge af positive hele tal, vil vi før eller siden nå til et $q_r = 1$, og så er $n = d_1 \cdot d_2 \cdot ... \cdot d_r$. Hermed er eksistensen af en primfaktoropløsning påvist.
Entydighed: Vi skal bevise, at alle naturlige tal har den egenskab, at deres primfaktoropløsning er entydig. Vi fører beviset indirekte og antager derfor, at der findes tal med flere forskellige primfaktoropløsninger. Lad n betegne det mindste sådanne naturlige tal. For tallet n findes der altså ifølge antagelsen to forskellige primfaktoropløsninger:

$$p_1 \cdot p_2 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot ... \cdot q_s \quad .$$

Her kan ingen faktor på venstre side også forekomme på højre side, for så ville man jo ved at bortforkorte den pågældende fælles faktor få et mindre tal med to forskellige primfaktoropløsninger - i strid med definitionen af n. Betragt nu primtallet p_1; der gælder enten $p_1 < q_1$ eller $p_1 > q_1$. Hvis $p_1 < q_1$, danner vi tallet

$$m = (q_1 - p_1) \cdot q_2 \cdot ... \cdot q_s \quad ,$$

som er mindre end n. Endvidere gælder, at m har to forskellige primfaktoropløsninger; vi kan jo skrive

$$m = q_1 \cdot q_2 \cdot ... \cdot q_s - p_1 \cdot q_2 \cdot ... \cdot q_s = n - p_1 \cdot q_2 \cdot ... \cdot q_s$$

$$= p_1 \cdot p_2 \cdot ... \cdot p_r - p_1 \cdot q_2 \cdot ... \cdot q_s = p_1 \cdot (p_2 \cdot ... \cdot p_r - q_2 \cdot ... \cdot q_s) \quad ,$$

hvoraf det fremgår, at m har en primfaktoropløsning indeholdende p_1; men af definitionen af m ovenfor fremgår, at m også har en primfaktoropløsning, hvori p_1 ikke indgår (da p_1 jo ikke går op i $(q_1 - p_1)$). Herved har vi opnået en modstrid. På tilsvarende måde nås til en modstrid i tilfældet $p_1 > q_1$. Hermed er beviset ført. $\diamond$

Eksempel 1.2. Tallet 1140 ønskes opløst i primfaktorer. Det kan f.eks. gøres således: $1140 = 114 \cdot 10 = 2 \cdot 57 \cdot 2 \cdot 5 = 2 \cdot 3 \cdot 19 \cdot 2 \cdot 5$ eller $1140 = 190 \cdot 6 = 19 \cdot 2 \cdot 5 \cdot 2 \cdot 3$. Entydigheden sikrer, at man når til samme resultat (nemlig $2^2 \cdot 3 \cdot 5 \cdot 19$), uanset hvilke mellemregninger man vælger.

Når man kender primfaktoropløsningen af et tal n, har man overblik over samtlige divisorer i tallet; primfaktorerne i en divisor i n vil jo gå op i n og dermed ifølge entydigheden forekomme i primfaktoropløsningen af n. Kendes primfaktoropløsningen for to tal, kan deres største fælles divisor findes som produktet af de fælles primfaktorer i den laveste potens.

Øvelse 1.1. Opskriv samtlige divisorer i tallet 1140.

Øvelse 1.2. Opløs tallet 13794 i primfaktorer.

Øvelse 1.3. Find største fælles divisor for tallene 1140 og 13794.

Øvelse 1.4. Find mindste fælles multiplum for tallene 1140 og 13794.

Øvelse 1.5. Går 1140 op i tallet $81 \cdot 210 \cdot 607$?

Øvelse 1.6. Tallet 20! ender på et antal nuller. Hvor mange?

Øvelse 1.7. 1) Gør rede for, at hvis et primtal p går op i et produkt, går det op i mindst en af faktorerne. 2) Gør rede for, at påstanden ikke gælder, hvis p ikke er et primtal.

Øvelse 1.8. Bevis, at der for enhver værdi af $n \in N$ gælder, at tallet $n^3 - n$ er deleligt med 6.

Øvelse 1.9. Lad tallet n have primfaktoropløsningen $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$. Vis, at antallet af divisorer i n er $(\alpha_1 + 1)(\alpha_2 + 1) \cdot ... \cdot (\alpha_r + 1)$.

2. Regning med kongruenser

Inden for mængden af hele tal Z defineres delelighed på tilsvarende måde som i N: vi siger, at $d \in Z$ går op i $a \in Z$, og skriver $d|a$, hvis $a = q \cdot d$, hvor $q \in Z$.

Definition 2.1. Lad $n \in N$. Tallet $a \in Z$ siges at være *kongruent modulo* n med tallet $b \in Z$, og vi skriver

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

dersom

$$n|b - a \ .$$

Eksempel 2.1. Der gælder $7|21$, $-7|21$ og $7|0$. Der gælder $3 \equiv 24 \pmod{7}$ og $3 \equiv -11 \pmod{7}$.

Bemærkning. Bemærk, at $a \equiv 0 \pmod{n}$ er ensbetydende med at $n|a$.

Øvelse 2.1. For hvilke $x \in Z$ gælder $x \equiv 3 \pmod{7}$?

Øvelse 2.2. Hvad betyder $a \equiv b \pmod{2}$?

Øvelse 2.3. Hvad betyder $a \equiv b \pmod{1}$?

Øvelse 2.4. Hvordan kan man umiddelbart se på to naturlige tal, om de er kongruente modulo 10?

Bemærk, at den indførte relation er en *ækvivalensrelation* i Z, dvs. at den har følgende tre egenskaber:

(i) den er *refleksiv*, dvs.

$$a \equiv a \pmod{n} \ ,$$

(ii) den er *symmetrisk*, dvs.

$$a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n} \ ,$$

(iii) den er *transitiv*, dvs.

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

(Påstandene *(i)* og *(ii)* eftervises let ved brug af definitionen; ved beviset for *(iii)* benyttes omskrivningen $(c-b)+(b-a)=c-a$).

For kongruens modulo n gælder følgende nyttige regneregler:

Sætning 2.1. Lad $n \in N$. For alle $a, b, c, d \in Z$ gælder:
1) $a \equiv b \pmod{n} \ \wedge \ c \equiv d \pmod{n} \quad \Rightarrow \quad a+c \equiv b+d \pmod{n}$,
2) $a \equiv b \pmod{n} \ \wedge \ c \equiv d \pmod{n} \quad \Rightarrow \quad a-c \equiv b-d \pmod{n}$,
3) $a \equiv b \pmod{n} \ \wedge \ c \equiv d \pmod{n} \quad \Rightarrow \quad a \cdot c \equiv b \cdot d \pmod{n}$.

Bevis. 1) Da $a \equiv b \pmod{n}$ og $c \equiv d \pmod{n}$, gælder $n|b-a$ og $n|d-c$, og dermed $n|(b-a)+(d-c) = (b+d)-(a+c)$ som ønsket. 2) bevises tilsvarende. Til 3) anvendes omskrivningen $bd-ac = b(d-c)+(b-a)c$. ◇

Sætningen fortæller, at man i mange henseender kan regne med kongruenser ligesom med almindelige ligninger: man kan lægge dem sammen, trække dem fra hinanden og gange dem med hinanden. Bemærk specielt, at man kan *lægge samme tal til* eller *trække samme tal fra* på hver side af en kongruens (det fremgår af sætningens del 1 og 2 med $c = d$):

$$a \equiv b \pmod{n} \quad \Rightarrow \quad a+c \equiv b+c \pmod{n} \ ,$$

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

Det betyder, at man ganske som ved almindelige ligninger kan *flytte et led* fra den ene side af en kongruens til den anden side *ved at ændre fortegn.* Man kan også *gange med samme tal* på hver side af en kongruens (benyt sætningens 3. del med $c = d$):

$$a \equiv b \pmod{n} \quad \Rightarrow \quad ca \equiv cb \pmod{n} \ .$$

NB! Bemærk implikationspilens retning. Normalt kan man ikke "komme tilbage". Det skyldes, at der ikke er en generel regel vedrørende division og kongruenser. Her kan det gå helt galt. (I afsnittet om primiske rester vender vi tilbage til dette "problem".)

Eksempel 2.2. Vi har $2 \cdot 5 \equiv 2 \cdot 2 \pmod 6$, men ikke $5 \equiv 2 \pmod 6$.

Vedrørende multiplikation fremhæves følgende sætning:

Sætning 2.2. Lad $n \in N$. For alle $a, b \in Z$ og alle $k \in N$ gælder

$$a \equiv b \pmod n \quad \Rightarrow \quad a^k \equiv b^k \pmod n \ .$$

Bevis. Sætningen bevises ved induktion. For $k = 1$ er påstanden triviel. Antag nu, at påstanden gælder for et vist k. Så gælder den også for $k+1$: af $a \equiv b \pmod n$ og $a^k \equiv b^k \pmod n$ fås nemlig (if. 3. del af sætningen ovenfor), at $a \cdot a^k \equiv b \cdot b^k \pmod n$, altså at $a^{k+1} \equiv b^{k+1} \pmod n$ som ønsket. $\diamond$

Definitionen af kongruens modulo n kan udtrykkes på en anden måde. Vi minder først om *division med rest*: når $a \in Z$, kan a skrives som et helt multiplum af n plus en rest r:

$$a = qn + r \ , \ q \in Z \ , \ r \in Z \ .$$

En ligning af denne form kaldes en *divisionsligning*. For givet n og givet a er der mange mulige valg af q og r. Hvis man kræver, at $r \in \{0, ..., n-1\}$, er r (og dermed også q) entydigt bestemt; den pågældende værdi af r kaldes *den principale rest* ved division med n.

Sætning 2.3. Lad $n \in N$. For alle $a, b \in Z$ gælder da, at $a \equiv b \pmod n$, hvis og kun hvis a og b giver samme rest ved division med n.

Bevis. Antag først, at a og b giver samme rest ved division med n, altså at vi kan skrive $a = q_1 n + r$ og $b = q_2 n + r$. Heraf fås $b - a = (q_2 - q_1)n$ og dermed $n | b - a$. Hvis vi omvendt ved, at $a \equiv b \pmod n$, dvs. at vi kan skrive $b - a = kn$, og $a = qn + r$, fås $b = (k+q)n + r$; b giver altså samme rest som a ved division med n. $\diamond$

Eksempel 2.3. Vi vil bestemme den rest, som tallet $23^5 \cdot 89^{367} \cdot 113$ giver ved division med 5. Ved at regne modulo 5 og udnytte regnereglerne fra sætning 2.1 og 2.2 finder vi

$$23^5 \cdot 89^{367} \cdot 113 \equiv 3^5 \cdot (-1)^{367} \cdot 3 \equiv 3 \cdot (3^2)^2 \cdot (-1) \cdot 3$$

$$\equiv 3 \cdot (-1)^2 \cdot (-1) \cdot 3 \equiv -9 \equiv 1 \pmod 5 \ .$$

Resten modulo 7 findes på tilsvarende måde:

$$23^5 \cdot 89^{367} \cdot 113 \equiv 2^5 \cdot (-2)^{367} \cdot 1 \equiv 2^3 \cdot 2^2 \cdot ((-2)^3)^{122} \cdot (-2) \cdot 1 \equiv 8 \cdot 4 \cdot (-8)^{122} \cdot (-2) \cdot 1$$

$$\equiv 1 \cdot 4 \cdot (-1)^1 22 \cdot (-2) \cdot 1 \equiv -8 \equiv 6 \pmod 7 \ .$$

Øvelse 2.5. Angiv samtlige løsninger til hver af kongruenserne

$$x \equiv 4 \pmod 6 \ \text{ og } \ x \equiv 4 \pmod 5 \ .$$

Øvelse 2.6. Bestem ved at regne modulo 10 det sidste ciffer i tallet

$$2004^7 - 6722^{87} \cdot 549 \ .$$

Øvelse 2.7. Løs for $n = 5$ og for $n = 6$ hver af kongruenserne

$$x^2 \equiv 3 \pmod n \ \text{ og } \ x^2 \equiv 4 \pmod n \ .$$

Øvelse 2.8. 1) Gør rede for, at hvis p er et primtal, gælder *nulreglen* for kongruens modulo p, dvs.

$$a \cdot b \equiv 0 \pmod p \ \Rightarrow \ a \equiv 0 \pmod p \ \vee \ b \equiv 0 \pmod p \ .$$

2) Gør rede for, at nulreglen ikke gælder, hvis p er et sammensat tal.

Øvelse 2.9. 1) Gør rede for, at når p er et primtal, gælder *forkortningsreglen*

$$ca \equiv cb \pmod p \ \Rightarrow \ a \equiv b \pmod p$$

for $c \not\equiv 0 \pmod p$.
2) Gør rede for, at forkortningsreglen ikke gælder, når p er et sammensat tal.

Øvelse 2.10. 1) Bevis, at når p er et primtal større end 2, har kongruensen

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

præcis to løsninger i $\{0, ..., p-1\}$. (Vink: omskriv til $(x-1)(x+1) \equiv 0 \pmod p$ og brug nulreglen.)
2) Hvad sker der for $p = 2$?
3) Find eksempler, der viser, at der kan være mere end to løsninger, hvis p ikke er et primtal.

Øvelse 2.11. Undersøg kongruenser af typen $x^2 \equiv a \pmod{p}$, når p er et primtal. Hvad kan siges om antallet af løsninger i $\{0, ..., p-1\}$?

Et berømt resultat inden for talteorien er *Fermats lille sætning.*

Sætning. (Fermats lille sætning). Lad p være et primtal. Lad $a \in Z$ være et tal, som ikke er deleligt med p. Så gælder

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

Beviset kan føres på grundlag af resultaterne i ovenstående øvelser, men da Fermats lille sætning er et specialtilfælde af Euler-Fermats sætning, som vises senere, forbigås beviset her. (Og vi bygger naturligvis ikke på sætningen i det følgende!).

Øvelse 2.12. *(Om personnumre).* Alle danske CPR-numre

$$c_1c_2c_3c_4c_5c_6 - c_7c_8c_9c_{10}$$

opfylder følgende kongruensrelation modulo 11:

$$4c_1 + 3c_2 + 2c_3 + 7c_4 + 6c_5 + 5c_6 + 4c_7 + 3c_8 + 2c_9 + c_{10} \equiv 0 \pmod{11} \ .$$

a) Check dit eget personnummer.
b) Er 040383-5125 et lovligt personnummer?

Som yderligere eksempler på modulo-regning kan vi bevise nogle af de velkendte delelighedsregler. Vi minder om, at *tværsummen* af et tal defineres som summen af dets cifre. I det følgende vil vi betegne tværsummen af et tal x med $t(x)$.

Sætning 2.4. (Om delelighed med 3). Et tal er deleligt med 3, hvis og kun hvis 3 går op i tallets tværsum.

Bevis. Lad $a_k, a_{k-1}, ..., a_1, a_0$ være cifrene i det tal x, vi skal undersøge, så at

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

Da $10 \equiv 1 \pmod{3}$ og dermed $10^i \equiv 1^i \equiv 1 \pmod{3}$ for alle $i = 0, 1, ..., k$, gælder

$$x \equiv a_k \cdot 1 + a_{k-1} \cdot 1 + ... + a_1 \cdot 1 + a_0 \pmod{3},$$

dvs.

$$x \equiv t(x) \pmod 3 \ .$$

Det betyder, at tallet og dets tværsum giver samme rest ved division med 3. Specielt fås altså resten 0, hvis og kun hvis tværsummen giver resten 0. $\diamond$

Øvelse 2.13. Bevis den tilsvarende regel for division med 9.

Øvelse 2.14. *(Om 9-prøven).* I tidligere tiders regneundervisning, hvor man ofrede megen omhu på at lære eleverne at gange store tal fejlfrit sammen, opfordrede man dem til at kontrollere deres resultater med "9-prøven", der beskrives her: lad n og m være de to tal, der skal ganges sammen, og lad r være det opnåede resultat. Dan den reducerede tværsum $T(n), T(m)$ og $T(r)$ af hvert af tallene n, m og r. (At danne den reducerede tværsum betyder blot at danne tværsum gentagne gange, indtil der fremkommer et 1-cifret tal. Når man danner den reducerede tværsum, kan man undlade at medregne 9-taller. (Hvorfor?)). Hvis r er det korrekte resultat, vil $T(r)$ være den reducerede tværsum af produktet $T(n) \cdot T(m)$.
a) Bevis dette.
b) Undersøg, om $3128 \cdot 8214 = 25692392$.
c) Gør rede for, at man godt kan regne galt, uden at det afsløres af 9-prøven.
d) Gælder 9-prøven også for addition?

Øvelse 2.15. Den *alternerende tværsum* af et tal dannes ved, at man skiftevis adderer og subtraherer cifrene i tallet (den alternerende tværsum af 23758 er således $2 - 3 + 7 - 5 + 8 = 9$). Bevis, at et tal er deleligt med 11, hvis og kun hvis 11 går op i den alternerende tværsum.

Øvelse 2.16. Hvordan undersøger man, om et tal er deleligt med 2? med 6? med 15? med 18? med 25?

Øvelse 2.17. Gælder tværsumsreglen for delelighed med 3 i 2-tals-systemet? I 5-talssystemet? For hvilke værdier af a gælder reglen i a-tals-systemet?

For givet $a \in Z$ indføres betegnelsen $(a)_n$ for mængden af tal, der er kongruente modulo n med a, altså

$$(a)_n = \{..., a - 2n, a - n, a, a + n, a + 2n, ...\} \ ;$$

denne mængde kaldes en *restklasse*, og a kaldes en *repræsentant* for restklassen. Bemærk, at

$$a \equiv b \pmod n \quad \Leftrightarrow \quad (a)_n = (b)_n \ .$$

Hver restklasse indeholder netop ét element tilhørende $\{0, ..., n-1\}$; dette kaldes *den principale repræsentant* for restklassen. For givet n er der ialt n forskellige restklasser.

Eksempel 2.4. Der gælder

$$(3)_2 = \text{mængden af ulige tal} \quad \text{og} \quad (3)_7 = \{..., -11, -4, 3, 10, 17, ...\}.$$

Øvelse 2.18. Er $(635422)_{14} = (635450)_{14}$?

Øvelse 2.19. Angiv de principale repræsentanter for $(67)_5, (-1)_5, (35)_5$ og $(-14366)_5$.

3. Euklids algoritme

Hvis primfaktoropløsningen af to tal foreligger, kan man let finde deres største fælles divisor. I princippet kan denne metode til at bestemme største fælles divisor altid benyttes, da jo alle tal kan opløses i primfaktorer. Men i praksis er dette langsommeligt for store tal. Her er *Euklids algoritme*, som nu gennemgås, mere effektiv. Euklids algoritme har også teoretiske anvendelser.

Med (a, b) betegnes største fælles divisor for to tal $a, b \in Z$.

Lad nu $a, b \in N$ være forelagt. Vi kan antage, at $a \geq b$. Sæt $r_0 = b$. Så kan vi opskrive divisionsligningen

$$a = q_1 r_0 + r_1 \ , \ q_1 \in N \ , \ r_1 \in \{0, ..., r_0 - 1\} \ .$$

Det er klart, at enhver fælles divisor for r_0 og r_1 også går op i a; og da $r_1 = a - q_1 r_0$, vil omvendt enhver fælles divisor for a og $b = r_0$ også gå op i r_1. Mængden af fælles divisorer for a og b er altså lig med mængden af fælles divisorer for r_0 og r_1, og dermed er

$$(a, b) = (a, r_0) = (r_0, r_1) \ .$$

Hvis nu $r_1 = 0$, er $(r_0, r_1) = (r_0, 0) = r_0$, og bestemmelsen af største fælles divisor er afsluttet. Hvis $r_1 > 0$, kan vi opskrive divisionsligningen

$$r_0 = q_2 r_1 + r_2 \ , \ q_2 \in N \ , \ r_2 \in \{0, ..., r_1 - 1\} \ .$$

Som før kan vi argumentere for, at

$$(r_0, r_1) = (r_1, r_2) \text{ og dermed } (a, b) = (r_1, r_2) \quad .$$

Hvis $r_2 = 0$, er vi færdige; ellers fortsættes:

$$r_1 = q_3 r_2 + r_3 \ , \ q_3 \in N \ , \ r_3 \in \{0, ..., r_2 - 1\} \quad .$$

Så er

$$(a, b) = (r_2, r_3) \quad .$$

Denne proces fortsættes, indtil vi når en rest $r_k = 0$, hvilket vil indtræffe efter et endeligt antal skridt, da talfølgen $r_0, r_1, r_2...$ er aftagende og består af hele ikke-negative tal. Største fælles divisor for a og b er da den sidst mødte positive rest:

$$(a, b) = (r_{k-1}, 0) = r_{k-1} \quad .$$

En vigtig konsekvens af Euklids algoritme er følgende

Sætning 3.1. Lad $a, b \in Z$, og lad d være største fælles divisor for a og b. Så kan d skrives som en heltallig linearkombination af a og b, dvs. der findes hele tal x og y med

$$d = xa + yb \quad .$$

Bevis. Det er tilstrækkeligt at bevise påstanden for naturlige tal a og b. Vi antager $a \geq b$ og forestiller os divisionsligningerne opskrevet som ovenfor. Bemærk nu, at hver af de optrædende rester r_i kan udtrykkes som heltalskombination af de to forudgående rester og dermed, ved indsættelse, som kombination af a og b. Specielt gælder dette for d, der jo fremkommer som den sidste rest. $\diamond$

Bemærk, at tallene x og y i sætningen ovenfor ikke er entydigt bestemt. (Hvis tallet m er deleligt med både a og b, kan vi skrive $m = aa_1 = bb_1$ og dermed gælder $d = (x - a_1)a + (y + b_1)b$).

Eksempel 3.1. Vi vil finde største fælles divisor for tallene 1078 og 70. Vi opskriver divisionsligningerne

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

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

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

Altså er (1078,70)=14 . Ved at gå baglæns i ligningerne ser vi, at vi kan udtrykke 14 som heltallig linearkombination af 1078 og 70 :

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

Øvelse 3.1. Bestem største fælles divisor for tallene 1140 og 13794 ved hjælp af Euklids algoritme. (Sml. øv. 1.3).

Øvelse 3.2. Lad $a, b \in Z$. For hvilke værdier af $c \in Z$ har ligningen $ax + by = c$ heltallige løsninger?

Øvelse 3.3. Find hele tal x og y med $209x + 628y = 13$.

4. Primiske rester

Vi vil nu indføre et vigtigt begreb.

Definition 4.1. To tal $a, b \in Z$ siges at være *primiske* , hvis

$$(a, b) = 1 \quad .$$

Tallene a og b er altså primiske, hvis deres største fælles divisor er 1, dvs. hvis de ikke har nogen fælles primfaktor. Bemærk, at hvis a og b er primiske, findes der if. sætning 3.1 hele tal x og y med $xa + yb = 1$.

Lad nu $n \in N$. Et tal, der er primisk med n, kaldes en *primisk rest* modulo n. De primiske rester spiller en særlig rolle, når man regner modulo n. Disse tal kan man nemlig i en vis forstand "dividere" med i forbindelse med kongruenser, og de får derved en stilling, der svarer til tallene forskellige fra 0 i forbindelse med almindelig regning. NB: den "division", vi skal indføre, er *ikke* den sædvanlige division - men den kan *bruges* i forbindelse med kongruenser på samme måde som almindelig division kan bruges i forbindelse med almindelige ligninger.

Vi vil nu undersøge begrebet lidt. Vi samler en række væsentlige egenskaber i følgende sætning:

Sætning 4.1. Lad $n \in N$. For alle $a, b, x, y \in Z$ gælder
1) egenskaben at være primisk med n bevares ved kongruens, dvs.

$$(a, n) = 1 \ \wedge \ a \equiv b \pmod{n} \quad \Rightarrow \quad (b, n) = 1$$

2) egenskaben bevares ved multiplikation, dvs.

$$(a,n)=1 \ \wedge \ (b,n)=1 \quad \Rightarrow \quad (ab,n)=1$$

3) forkortningsreglen gælder for primiske rester, dvs.

$$(a,n)=1 \ \wedge \ ax \equiv ay \pmod{n} \quad \Rightarrow \quad x \equiv y \pmod{n}$$

4) hver primisk rest har en multiplikativ invers, dvs.

$$(a,n)=1 \quad \Rightarrow \quad \exists\, a' \in Z : a'a \equiv 1 \pmod{n} \ ;$$

endvidere gælder, at ethvert inverst element a' til a selv er en primisk rest, og at a' er entydigt bestemt pånær kongruens modulo n.

Bevis. 1) Største fælles divisor d for b og n vil gå op i $b-a$ (da $d|n$ og $n|b-a$) og dermed i a (da $d|b$ og $d|b-a$) og altså være fælles divisor for a og n; men så er $d=1$, hvilket skulle vises. 2) Det er klart ud fra entydigheden af primtalsopløsningen af tal, at enhver primdivisor i ab må være primdivisor i enten a eller b; et primtal, der går op i både ab og n, vil altså være fælles divisor for enten a og n eller b og n, og dette er i modstrid med antagelsen $(a,n)=1$ og $(b,n)=1$. 4) Inden beviset for 3) bevises eksistensdelen af påstand 4): da $(a,n)=1$, findes hele tal x og y med

$$xa+yn=1 \ .$$

Men så kan vi bruge x som a', idet jo

$$xa \equiv xa+yn=1 \pmod{n} \ .$$

3) Lad a' være et inverst element til a; så gælder

$$x=1\cdot x \equiv a'a\cdot x \equiv a'\cdot ax \equiv a'\cdot ay \equiv a'a\cdot y \equiv 1\cdot y = y \pmod{n}.$$

4) Her bevises resten af påstand 4). Entydigheden er nu klar ud fra forkortningsreglen: hvis a'_1 og a'_2 begge er inverse til a, gælder $a'_1a \equiv a'_2a \pmod{n}$ og dermed ved forkortning $a'_1 \equiv a'_2 \pmod{n}$. At a' nødvendigvis er primisk med n, indses således: største fælles divisor d for a' og n går op i $a'a-1$ (da jo $n|a'a-1$) og dermed i 1 (da $d|a'a$ og $d|a'a-1$). Men så er $d=1$. $\diamond$

Ved hjælp af inverse elementer kan man løse "førstegrads-kongruenser": hvis a er en primisk rest modulo n og a' dens inverse, gælder

$$ax+b \equiv c \pmod{n} \quad \Leftrightarrow \quad ax \equiv c-b \pmod{n}$$

$$\Leftrightarrow a'ax \equiv a'(c-b) \pmod{n} \quad \Leftrightarrow \quad x \equiv a'(c-b) \pmod{n} \ .$$

Eksempel 4.1. Da $2 \cdot 3 \equiv 1 \pmod 5$, er 3 inverst til 2, når vi regner modulo 5. Kongruensen $2x + 34 \equiv 13 \pmod 5$ kan da løses således:

$$2x + 34 \equiv 13 \pmod 5 \Leftrightarrow 2x - 1 \equiv 3 \pmod 5$$

$$\Leftrightarrow 2x \equiv 4 \pmod 5 \Leftrightarrow x \equiv 3 \cdot 4 \pmod 5 \Leftrightarrow x \equiv 2 \pmod 5 \ .$$

Øvelse 4.1. Angiv samtlige primiske rester modulo 15. Angiv for hver primisk rest dens inverse modulo 15.

Øvelse 4.2. En person har skrevet sit personnummer ned. Et af cifrene er desværre ulæseligt. Kan problemet klares?

Øvelse 4.3. Find et inverst element til 32 modulo 85. (Benyt Euklids algoritme).

Øvelse 4.4. 1) Gør rede for, at der for ethvert n større end 1 gælder, at tallene 1 og $n-1$ er primiske rester modulo n, og at de er inverse til sig selv (dvs. de opfylder $x^2 \equiv 1 \pmod n$) .
2) Gør rede for, at hvis n er et primtal, så er 1 og $n-1$ de eneste tal i $\{1, ..., n-1\}$ med den nævnte egenskab.

Definition 4.2. En restklasse modulo n kaldes *primisk*, hvis dens repræsentanter er primiske med n.

Bemærk, at hvis én repræsentant for en restklasse er primisk med n, gælder det samme for alle repræsentanter (ifølge første del af sætningen ovenfor).

Som et eksempel på anvendelsen af inverse elementer vises

Sætning 4.2. (Wilson's sætning.) For ethvert primtal p gælder

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

Bevis. For $p = 2$ fås $(p-1)! = 1 \equiv -1 \pmod 2$. Lad nu p være et primtal større end 2. Vi danner produktet

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1)$$

og bemærker, at der til hver faktor a i produktet også må forekomme en multiplikativ invers a' til a (der findes jo et inverst element til a, og a' kan

vælges som en repræsentant i $\{1, ..., p-1\}$). Ifølge øvelsen ovenfor er $a \neq a'$ undtagen for tallene 1 og $p-1$. Idet $a \cdot a' \equiv 1 \pmod{p}$, har vi derfor

$$2 \cdot 3 \cdot ... \cdot (p-2) \equiv 1 \pmod{p} \ ,$$

og dermed

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

som ønsket. $\diamond$

5. Eulers φ-funktion og Euler-Fermats sætning

I dette afsnit vil vi indføre en vigtig talteoretisk funktion, nemlig Eulers φ-funktion, og benytte denne til at generalisere Fermats lille sætning. Vi definerer nu Eulers φ-funktion som en afbildning fra N til N ved følgende

Definition 5.1. For $n \in N$ betegnes med $\varphi(n)$ *antallet af primiske restklasser modulo n.*

Som repræsentanter for restklasserne er det naturligt at vælge tal i $\{1, ..., n-1\}$ (0 kommer ikke på tale, da 0 ikke er primisk med n).

Eksempel 5.1. Der findes 8 primiske restklasser modulo 15, nemlig de 8 restklasser givet ved repræsentanterne 1, 2, 4, 7, 8, 11, 13, 14. Derfor er $\varphi(15) = 8$. Der gælder $\varphi(4) = 2$.

Øvelse 5.1. Bestem $\varphi(2), ..., \varphi(16)$.

For primtal er det let at opskrive værdien af Eulers φ-funktion:

Sætning 5.1. For et primtal p gælder

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

Bevis. Alle tallene $1, ..., p-1$ er primiske med p. $\diamond$

Nedenfor (sætn. 5.4) beviser vi, hvordan værdien af Eulers φ-funktion kan findes, når man kender tallets primfaktoropløsning. Først to hjælperesultater:

Sætning 5.2. For et primtal p og for $\alpha \in N$ gælder

$$\varphi(p^\alpha) = p^{\alpha-1} \cdot (p-1) \quad .$$

Bevis. Når man fra tallene $\{1, 2, ..., p^\alpha\}$ fjerner alle de $p^{\alpha-1}$ multipla af p, bliver netop de primiske rester tilbage. Deres antal er altså $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. $\diamond$

Sætning 5.3. Lad $k, m \in N$ være indbyrdes primiske. Så gælder

$$\varphi(k \cdot m) = \varphi(k) \cdot \varphi(m) \quad .$$

Bevis. Sæt $n = k \cdot m$. Da k og m er primiske, er $\varphi(n)$ netop antallet af tal i $\{0, ...n-1\}$, der er primiske med både k og m. Vi vil optælle de pågældende tal. For at få overblik opstiller vi tallene fra 0 til $n-1$ i dette skema:

0	1	2	.	.	k-1
k	k+1	k+2	.	.	k+(k-1)
2k	2k+1	2k+2	.	.	2k+(k-1)
.	.	.			.
.	.	.			.
(m-1)k	(m-1)k+1	(m-1)k+2	.	.	(m-1)k+(k-1)

Bemærk nu først, at første række indeholder $\varphi(k)$ tal primiske med k. De øvrige tal primiske med k befinder sig (af kongruensgrunde) lodret under disse. De tal, der er primiske med k, er altså samlet i $\varphi(k)$ søjler. Vi vil nu bevise, at der i hver søjle er netop $\varphi(m)$ tal primiske med m. Tallene i en tilfældigt valgt given søjle er på formen $qk + r$, $q \in \{0, ..., m-1\}$. Hvis $q_1 k + r \equiv q_2 k + r \pmod{m}$ for $q_1, q_2 \in \{0, ..., m-1\}$, vil m gå op i $(q_1 - q_2)k$, og dermed, da m er primisk med k, i $q_1 - q_2$, hvorfor $q_1 = q_2$. Dette viser, at de m tal i søjlen repræsenterer m forskellige restklasser modulo m; følgelig er netop $\varphi(m)$ af disse tal primiske med m. Ialt er der altså i skemaet $\varphi(k) \cdot \varphi(m)$ tal, der er primiske med både k og m. $\diamond$

Eksempel 5.2. Resultaterne fra eks. 5.1 kan nu (gen)findes således: $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$ og $\varphi(4) = \varphi(2^2) = 2^1 \cdot 1 = 2$.

Øvelse 5.2. Gennemfør beviset for sætn. 5.3. i tilfældet $k = 15$ og $m = 4$.

Øvelse 5.3. Bevis, at $\varphi(pq) = (p-1)(q-1)$, når p og q er to forskellige primtal.

Det første hovedresultat i dette afsnit er følgende udtryk for φ-funktionen:

Sætning 5.4. Hvis $n \in N$ har primfaktoropløsningen $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$, så er

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot ... \cdot (1 - \frac{1}{p_r})$$
$$= p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot \ddots \cdot p_r^{\alpha_r - 1} \cdot (p_r - 1) \quad .$$

Bevis. Med brug af sætn. 5.3 og sætn. 5.2 fås

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r})$$
$$= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot ... \cdot \varphi(p_r^{\alpha_r})$$
$$= p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot ... \cdot p_r^{\alpha_r - 1} \cdot (p_r - 1) \quad .$$

Ved at sætte p_i uden for parentes i hver faktor og gange sammen fås udtrykket $\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot ... \cdot (1 - \frac{1}{p_r})$.$\diamond$

Vi formulerer det andet hovedresultat i dette afsnit:

Sætning 5.5. (Euler-Fermat). Lad $n \in N$ og $a \in Z$. Hvis a er primisk med n, gælder

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

Bevis. Lad

$$a_1, ..., a_{\varphi(n)}$$

være repræsentanter for de ialt $\varphi(n)$ primiske restklasser. Betragt endvidere de $\varphi(n)$ tal

$$a \cdot a_1, ..., a \cdot a_{\varphi(n)} \quad .$$

Ifølge sætningen om regning med primiske rester er disse $\varphi(n)$ tal selv primiske rester, og ifølge forkortningsreglen repræsenterer de forskellige restklasser. De repræsenterer altså netop samtlige primiske restklasser, og deres produkt vil derfor være kongruent med produktet af samtlige de oprindeligt valgte repræsentanter:

$$a \cdot a_1 \cdot ... \cdot a \cdot a_{\varphi(n)} \equiv a_1 \cdot ... \cdot a_{\varphi(n)} \pmod{n} \quad .$$

Vi har altså ved ombytning af faktorernes orden på venstre side

$$a^{\varphi(n)} \cdot a_1 \cdot ... \cdot a_{\varphi(n)} \equiv a_1 \cdot ... \cdot a_{\varphi(n)} \pmod{n} \quad ,$$

hvoraf ved forkortning

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad . \diamond$$

Af Euler-Fermats sætning fås som specialtilfælde den tidligere nævnte Fermats lille sætning. For et primtal p er jo $\varphi(p) = p - 1$, og Euler-Fermats sætning udsiger da netop, at

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

for alle a, som ikke er delelige med p.

Bemærkning. Når $\varphi(n)$ kendes, fås via Euler- Fermats sætning en repræsentant for det inverse element til a, nemlig $a^{\varphi(n)-1}$: sætningen siger jo netop, at produktet af dette tal og a er kongruent med 1.

Eksempel 5.3. Det inverse til 2 modulo 5 er

$$2^{\varphi(5)-1} = 2^{4-1} = 8 \equiv 3 \pmod{5} \quad .$$

Øvelse 5.4. Find det inverse til 7 modulo 16.

Øvelse 5.5. Vis, at

$$k \equiv m \pmod{\varphi(n)} \quad \Rightarrow \quad a^k \equiv a^m \pmod{n} \quad .$$

6. Pythagoræiske talsæt

Et talsæt (a, b, c) , hvor $a, b, c \in N$ og $a^2 + b^2 = c^2$, kaldes et *pythagoræisk* talsæt (eller tripel). Et tripel (a, b, c) med egenskaben, at a, b og c ikke har nogen fælles divisor større end 1, kaldes *primitivt*.

Ethvert talsæt af formen $(s^2 - t^2, 2st, s^2 + t^2)$ er pythagoræisk, idet der gælder

$$(s^2 - t^2)^2 + (2st)^2 = s^4 - 2s^2t^2 + t^4 + 4s^2t^2 = s^4 + 2s^2t^2 + t^4 = (s^2 + t^2)^2 \quad .$$

Nedenfor vises, at ethvert *primitivt* pythagoræisk talsæt er af denne form (endda med visse restriktioner på s og t). Dermed er alle pythagoræiske talsæt bestemt, idet et vilkårligt pythagoræisk talsæt kan dannes ud fra et primitivt ved multiplikation.

Sætning 6.1. Lad (a, b, c) være et primitivt pythagoræisk talsæt. Så er (a, b, c) (eller (b, a, c)) af formen

$$(s^2 - t^2, 2st, s^2 + t^2) \quad ,$$

hvor $s, t \in N$ er indbyrdes primiske og af modsat paritet.

Bevis. 1) Vi indser først, at i triplet (a, b, c) (primitivt pythagoræisk) må a og b have modsat paritet (dvs. det ene tal er lige og det andet ulige), og c må være ulige: det er nemlig oplagt, at a, b og c må være parvis primiske (en fælles divisor for to af dem vil via $a^2 + b^2 = c^2$ også være divisor i det tredie tal); følgelig må mindst to af de tre tal være ulige, og de kan ikke alle tre være ulige (ulige+ulige $\not\equiv$ *ulige*).$Talletcmåværeulige, forvarclige, såvarc^2$ delelig med 4, men en kvadratsum af to ulige tal kan ikke være delelig med 4: $(2n + 1)^2 + (2m + 1)^2 = 4(n^2 + m^2 + n + m) + 2 \equiv 2 \pmod 4$.
2) Vi kan antage, at a er ulige og b lige (og altså c ulige). Da er $b^2 = c^2 - a^2 = (c + a)(c - a)$, hvor både $c + a$ og $c - a$ er lige. Her må $(c + a)/2$ og $(c - a)/2$ være primiske, for om deres største fælles divisor d må gælde, at d går op både i deres sum c og deres differens a, altså må $d = 1$.
3) Vi betragter nu den entydigt bestemte primfaktoropløsning af tallet

$$(\frac{b}{2})^2 = \frac{c + a}{2} \cdot \frac{c - a}{2} \quad .$$

Da venstre side er et kvadrat, må hver primfaktor optræde et lige antal gange. Da faktorerne på højre side er primiske, må hver af primfaktorerne fra venstre side optræde et lige antal gange i enten $(c+a)/2$ eller $(c-a)/2$. Heraf følger, at hvert af tallene $(c + a)/2$ og $(c - a)/2$ er kvadrattal.
4) Sæt nu

$$\frac{c + a}{2} = s^2 \quad \text{og} \quad \frac{c - a}{2} = t^2 \quad .$$

Så fås let $a = s^2 - t^2$, $b = 2st$ og $c = s^2 + t^2$. Da $(s^2, t^2) = 1$, må også $(s, t) = 1$. Da c er ulige, må s og t have modsat paritet. $\diamond$

Svar på øvelser

Øv.1.1. Ialt 24 divisorer, nemlig 1; 2, 2^2, 3, 5, 19; $2\cdot 3$, $2^2\cdot 3$, $2\cdot 5$, $2^2\cdot 5$, $2\cdot 19$, $2^2\cdot 19$, $3\cdot 5$, $3\cdot 19$, $5\cdot 19$; $2\cdot 3\cdot 5$, $2^2\cdot 3\cdot 5$, $2\cdot 3\cdot 19$, $2^2\cdot 3\cdot 19$, $2\cdot 5\cdot 19$, $2^2\cdot 5\cdot 19$, $3\cdot 5\cdot 19$;$2\cdot 3\cdot 5\cdot 19$, $2^2\cdot 3\cdot 5\cdot 19 = 1140$.
Øv.1.2. $2\cdot 3\cdot 11^2\cdot 19$.
Øv.1.3. $2\cdot 3\cdot 19$.
Øv.1.4. $2^2\cdot 3\cdot 5\cdot 11^2\cdot 19$.
Øv.1.5. Nej, da 19 ikke går op i 81, 2 eller 60.
Øv.1.6. 4 nuller (idet hvert nul hidrører fra kombinationen af en faktor 5 og en faktor 2 i primfaktoropløsningen af 20!).
Øv.1.7. 1) Udnyt entydigheden: primfaktoropløsningen af produktet fremkommer ud fra primfaktoropløsningerne af faktorerne. 2) Eks.: $6|3\cdot 4$.
Øv.1.8. Bemærk, at vi kan skrive tallet som $n(n+1)(n-1)$; her er faktorerne tre på hinanden følgende tal, og derfor vil et af dem være deleligt med 3 og mindst et af dem lige. Altså går $3\cdot 2 = 6$ op i deres produkt.
Øv.1.9. At d er divisor i $n = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot ...\cdot p_r^{\alpha_r}$ er ensbetydende med, at d kan skrives $p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot ...\cdot p_r^{\beta_r}$, $0\le\beta_i\le\alpha_i$, $i = 1, ..., r$. Det ønskede følger da umiddelbart af multiplikationsprincippet, idet β_i kan vælges på netop $\alpha_i + 1$ måder.
Øv.2.1. For $..., -11, -4, 3, 10, 17, ...$.
Øv.2.2. At a og b har samme *paritet* (dvs. er enten begge lige eller begge ulige).
Øv.2.3. Denne relation er altid opfyldt.
Øv.2.4. De er kongruente, netop hvis de ender på samme ciffer.
Øv.2.5. $..., -8, -2, 4, 10, 16, ...$ og $..., -1, 4, 9, ...$
Øv.2.6. 8.
Øv.2.7. Ved brug af regnereglerne ses, at $x\equiv 0 \pmod 5$ medfører $x^2\equiv 0 \pmod 5$, $x\equiv 1 \pmod 5$ medfører $x^2\equiv 1 \pmod 5$, $x\equiv 2 \pmod 5$ medfører $x^2\equiv 4 \pmod 5$, $x\equiv 3 \pmod 5$ medfører $x^2\equiv 9\equiv 4 \pmod 5$, $x\equiv 4 \pmod 5$ medfører $x^2\equiv 16\equiv 1 \pmod 5$. Kongruensen $x^2\equiv 3 \pmod 5$ har altså ingen løsninger, og $x^2\equiv 4 \pmod 5$ har løsningerne $x\equiv 2 \pmod 5$ og $x\equiv 3 \pmod 5$. På tilsvarende måde findes ved gennemgang af 6 tilfælde modulo 6 , at $x^2\equiv 3 \pmod 6$ har løsningerne $x\equiv 3 \pmod 6$, og $x^2\equiv 4 \pmod 6$ har løsningerne $x\equiv 2 \pmod 6$ og $x\equiv 4 \pmod 6$.
Øv.2.8. Jf. øvelse 1.7.
Øv.2.9. 1) Da $ca\equiv cb \pmod p \Rightarrow c(b-a)\equiv 0 \pmod p$, følger resultatet af nulreglen (øv.2.8). 2) Eks.: $2\cdot 2\equiv 2\cdot 3 \pmod 6$, men $2\not\equiv 3 \pmod 6$.
Øv.2.10. 1) og 2): Ved brug af nulreglen giver $x^2-1\equiv 0 \pmod p (\Rightarrow (x-1)(x+1)\equiv 0 \pmod p)$, at $x\equiv -1 \pmod p \vee x\equiv 1 \pmod p$. For

$p > 2$ er der altså de to løsninger 1 og $p-1$. For $p = 2$ er der kun en løsning (idet $1 = p - 1$). 3) $x^2 \equiv 1 \pmod 8$ har løsningerne 1, 3, 5, 7.
Øv.2.11. For $p > 2$: 0, 1 eller 2 løsninger. For $p = 2$: 1 løsning.
Øv.2.12. b) Nej.
Øv.2.13. Beviset kan ordret bruges.
Øv.2.14. a) $T(r) \equiv r = n \cdot m \equiv T(n) \cdot T(m) \pmod 9$. b) Nej. c) Eks.: $3 \cdot 8 = 60$?! d) Ja.
Øv.2.15. Kopiér beviset for sætn.2.4 med passende modifikationer: af $10 \equiv -1 \pmod{11}$ fås $10^i \equiv (-1)^i \pmod{11}$ for alle $i = 1, ..., k$.
Øv.2.16. Lige. Med 2 og med 3. Med 3 og med 5. Med 2 og med 9. Se om 25 går op i tallet skrevet med de to sidste cifre.
Øv.2.17. Nej. Nej. For $a \equiv 1 \pmod 3$.
Øv.2.18. Ja, da 14 går op i differensen.
Øv.2.19. 2, 4, 0, 4.
Øv.3.1. $13794 = 12 \cdot 1140 + 114$; $1140 = 10 \cdot 114 + 0$. Altså 114.
Øv.3.2. For $c =$ et multiplum af (a, b). (Betingelsen er nødvendig, da (a, b) går op i ligningens venstre side; og den er tilstrækkelig, da enhver løsning til $xa+yb = (a, b)$ ved multiplikation med k giver en løsning til $xa+yb = k(a, b)$).
Øv.3.3. Af $628 = 3 \cdot 209 + 1$ fås $1 = -3 \cdot 209 + 628$ og dermed $13 = -39 \cdot 209 + 13 \cdot 628$.
Øv.4.1. Primiske rester: 1, 2, 4, 7, 8, 11, 13, 14; deres inverse hhv. 1, 8, 4, 13, 2, 11, 7, 14.
Øv.4.2. Ja. Med notationen fra øv.2.12 gælder, at hvis f.eks. c_6 mangler, skal kongruensen $5c_6 \equiv -(4c_1 + 3c_2 + 2c_3 + 7c_4 + 6c_5 + 4c_7 + 3c_8 + 2c_9 + c_{10}) \pmod{11}$ løses mht. c_6, og da 5 er primisk med 11, har kongruensen en entydigt bestemt løsning pånær kongruens modulo 11. Løsningen findes ved multiplikation med det inverse element 9 til 5.
Øv.4.3. 8 (idet $1 = -3 \cdot 85 + 8 \cdot 32$).
Øv.4.4. 1) $1^2 \equiv 1 \pmod n$; $(n-1)^2 \equiv (-1)^2 \equiv 1 \pmod n$. 2) Se øv.2.10.
Øv.5.1. 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8.
Øv.5.3. $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.
Øv.5.4. Det er 7 (da $\varphi(16) = \varphi(2^4) = 2^3 \cdot \varphi(2) = 8$ og $7^{8-1} \equiv 7^7 \equiv 7 \cdot 49^3 \equiv 7 \pmod{16}$.)

Blandede opgaver

Opgave 1. Vis, at hvis et ulige tal n kan skrives som sum af to kvadrattal, da er $n \equiv 1 \pmod 4$.

Opgave 2. For hvilke tal $n \in N$ gælder det, at $\varphi(n) = 4$?

Opgave 3. Tallet a har den principale rest 1 ved division med 3.
1) Bestem de mulige principale rester af a ved division med 6.
2) Bestem de mulige principale rester af a^2 ved division med 12.

Opgave 4. 1) Vis, at hvis p er et primtal med $p \equiv 1 \pmod 4$, da vil

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

2) Vis, at hvis p er et primtal med $p \equiv 3 \pmod 4$, da vil

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

Opgave 5. Lad tallet n have primfaktoropløsningen

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r} \ .$$

Vis, at summen af samtlige divisorer i n er

$$\frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot ... \frac{p_r^{\alpha_r+1}-1}{p_r-1} \ .$$

Opgave 6. Vis, at $\varphi(n^\alpha) = n^{\alpha-1} \cdot \varphi(n)$, $\alpha, n \in N$.

Opgave 7. Vis, at tallet $\frac{1}{6}n^3 - \frac{3}{2}n^2 + \frac{7}{3}n$ er et helt tal for alle værdier af det hele tal n.

Opgave 8. Wilson's sætning sagde, at hvis p er et primtal, så gælder $(p-1)! \equiv -1 \pmod p$. Vis, at det omvendte også gælder, altså at hvis $(p-1)! \equiv -1 \pmod p$, så er p et primtal.

Opgave 9. Vis, at der for alle $a, m, n \in N$ gælder:

$$a^m \equiv 1 \pmod n \quad \Rightarrow \quad (a, n) = 1 \ .$$

Opgave 10. Lad $n \in N$, og lad $m \in N$ være det mindste naturlige tal, således at $a^m \equiv 1 \pmod{n}$. Vis, at hvis $a^k \equiv 1 \pmod{n}$, $k \in N$, da vil $m|k$.

Opgave 11. 1) Vis, at $\varphi(n)$ er et lige tal, når $n \geq 3$.
2) Find det mindste lige tal, som *ikke* tilhører værdimængden for φ. (Og det næstmindste).

Opgave 12. 1) Find alle tal $n \in N$, så $2^n - 1$ er delelig med 7.
2) Find alle tal $n \in N$, så $2^n + 1$ er delelig med 7.

Opgave 13. Vis, at $a^{13} \equiv a \pmod{2730}$ for alle $a \in N$.

Opgave 14 . Bevis, at i ethvert pythagoræisk talsæt er mindst et af tallene deleligt med 5.

Opgave 15. (Fermats store sætning for $n = 4$). Antag, at $u, v, w \in N$ så $u^4 + v^4 = w^2$. Vi skal i en serie skridt vise umuligheden af en sådan fremstilling. Heraf følger også umiddelbart, at ligningen $x^4 + y^4 = z^4 = (z^2)^2$ ikke har nogen heltallige løsninger. Vi antager indledningsvis w valgt, således at ingen heltalsligning $\alpha^4 + \beta^4 = \gamma^2$ har $\gamma < w$.
(i) Vis, at $(u, v) = (v, w) = (w, u) = 1$.
(ii) Vis, at man uden indskrænkning kan antage, at u er ulige og v lige.
(iii) Vis, at der findes $a, b \in N$, så $u^2 = a^2 - b^2$, $v^2 = 2ab$ og $w = a^2 + b^2$.
(iv) Vis, at a må være ulige og b lige, samt at $(a, b) = 1$.
(v) Vis, at der findes indbyrdes primiske $k, m \in N$ med $u = k^2 - m^2$, $b = 2km$ og $a = k^2 + m^2$.
(vi) Vis, at hvert af tallene k, m og $k^2 + m^2$ er kvadrattal, og udled heraf modstrid med de gjorte antagelser om u, v og w.

Løsningsforslag til opgaver

Opgave 1. Vi antager, at n kan skrives $a^2 + b^2$. Da n er ulige, må det ene af tallene a og b være ulige og det andet lige, f. eks. $a = 2m$ og $b = 2k + 1$. Så er $a^2 + b^2 = 4m^2 + 4k^2 + 4k + 1 \equiv 1 \pmod{4}$.

Opgave 2. Lad $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ være primfaktoropløsningen af n, hvor $p_1 < p_2 < \ldots < p_r$. Da er $\varphi(n) = 4 = p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot \ldots \cdot p_r^{\alpha_r - 1} \cdot (p_r - 1)$.

Antag $p_1 = 2$; vi kan da have $\alpha_1 - 1 = 2$ og dermed løsningen $n = 2^3 = 8$, eller vi kan have $\alpha_1 - 1 = 1$ og $p_2 - 1 = 2$ og $\alpha_2 - 1 = 0$, som giver løsningen $n = 2^2 \cdot 3 = 12$, eller vi kan endelig have $\alpha_1 - 1 = 0$, som tvinger $p_2 - 1 = 4$ og $\alpha_2 - 1 = 0$, altså løsningen $n = 2 \cdot 5 = 10$. Antag $p_1 = 3$, så må $\alpha_1 = 1$, da 34, men så mangler vi mindst én faktor $p_2 - 1 \geq 4$, og så bliver produktet for stort, og $p_1 = 3$ er altså umuligt. Antag $p_1 = 5$, så må $\alpha_1 = 1$ og $n = 5$ være en løsning. Da n oplagt ikke kan indeholde nogen primfaktor større end 5, er $\{n|\varphi(n) = 4\} = \{5, 8, 10, 12\}$.

Opgave 3. Vi har $a = 3k + 1$ for et helt tal k . Hvis a er lige, må k være ulige; vi skriver $k = 2n + 1$ og finder $a = 6n + 4 \equiv 4 \pmod 6$ og $a^2 = 36n^2 + 48n + 16 \equiv 4 \pmod{12}$. Hvis a er ulige, er k lige, dvs. $k = 2n$ og dermed $a = 6n+1 \equiv 1 \pmod 6$ og $a^2 = 36n^2+12n+1 \equiv 1 \pmod{12}$. Hermed er begge opgavens spørgsmål besvaret.

Opgave 4. 1) Skriv $p = 4n + 1$; så er $(p - 1)/2 = 2n$ og $(((p - 1)/2)!)^2 = ((2n)!)^2$. Ifølge Wilson's sætning er $(p - 1)! = (4n)! \equiv -1 \pmod p$. Nu er $(4n)! = (2n)! \cdot (2n + 1) \cdot (2n + 2) \cdot ... \cdot (2n + 2n)$. Hver af faktorerne $2n + i$, $i = 1, 2, ..., 2n$, omskrives: $2n + i = 4n + 1 - (2n - (i - 1)) = p - (2n - (i - 1))$, hvor $p - (2n - (i - 1)) \equiv (-1) \cdot (2n - (i - 1)) \pmod p$, og hvor $2n - (i - 1)$ gennemløber tallene $2n, 2n - 1, ..., 1$. Altså bliver $(-1) \equiv (4n)! \equiv (2n)! \cdot (-1)^{2n} \cdot (2n)! = ((2n)!)^2 \pmod p$.
2) Ovenstående ændres til: $p = 4n+3$, $(p - 1)/2 = 2n+1$, $(((p - 1)/2)!)^2 = ((2n + 1)!)^2$. Wilson's sætning giver: $(4n + 2)! = (2n + 1)! \cdot (2n + 1 + 1) \cdot ... \cdot (2n + 1 + 2n + 1)$. Vi omskriver: $2n + 1 + i = 4n + 3 - (2n + 1 - (i - 1)) = p - (2n + 1 - (i - 1)) \equiv (-1) \cdot (2n + 1 - (i - 1)) \pmod p$, hvor $2n + 1 - (i - 1)$ gennemløber tallene $2n + 1, 2n, ..., 1$. Altså bliver $-1 \equiv (4n+2)! \equiv (2n+1)! \cdot (-1)^{2n+1} \cdot (2n+1)! = -((2n+1!)$, som giver det ønskede: $((2n + 1)!)^2 \equiv 1 \pmod p$.

Opgave 5. Vi får her brug for kvotientrækkeformlen: $1+q+q^2+...+q^k = (q^{k+1} - 1)/(q - 1)$. Ved udregning af produktet $(1 + p_1 + ... + p_1^{\alpha_1}) \cdot ... \cdot (1 + p_r + ... + p_r^{\alpha_r})$ vil nemlig enhver af ovenstående divisorer i $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r}$ optræde netop én gang som addend. Altså er summen af alle divisorer i n lig med det anførte produkt, og så er vi færdige via kvotientrækkeformlen.

Opgave 6. Hvis $n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r}$, er $n^\alpha = (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r})^\alpha$, og $\varphi(n^\alpha) = (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r})^\alpha \cdot (1 - \frac{1}{p_1}) \cdot ... \cdot (1 - \frac{1}{p_r})$, mens $n^{\alpha-1} \cdot \varphi(n) = (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r})^{\alpha-1} \cdot (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r})^\alpha \cdot (1 - \frac{1}{p_1}) \cdot ... \cdot (1 - \frac{1}{p_r})$; opgaven er altså helt oplagt via forskriften for φ-funktionen.

Opgave 7. For at vise det ønskede skal vi vise, at det hele tal n^3-9n^2+14n er deleligt med 6. Dette følger af, at $n^3 - 9n^2 + 2n \equiv n^3 - 3n^2 + 2n = n(n-1)(n-2) \pmod 6$, og det sidste tal er oplagt deleligt med 6.

Opgave 8. Antag $(p-1)! \equiv -1 \pmod p$, og lad d være en ægte divisor i p. Af antagelsen får vi, at d går op i $(p-1)!+1$ (det gør p jo), men da d jo må være en af faktorerne i $(p-1)!$, gælder også $d|(p-1)!$; heraf følger, at $d|1$, og så er det bevist, at p er et primtal.

Opgave 9. Med d betegnes største fælles divisor for a og n . Af $a^m \equiv 1 \pmod n$ fås $n|a^m-1$ og dermed $d|a^m-1$; endvidere har vi $d|a^m$. Vi slutter, at $d|1$, altså $d=1$ som ønsket.

Opgave 10. Skriv $k = qm + r$, $0 \le r < m$. Så er $a^k \equiv (a^m)^q \cdot a^r \equiv a^r \pmod n$ og dermed $a^r \equiv 1 \pmod n$, og så må $r=0$ ifølge definitionen af m.

Opgave 11. 1) Lad $n \ge 3$. Enten er n en 2-tals-potens, eller også har n en ulige primdivisor. I det første tilfælde har vi $n = 2^k$, $k \ge 2$, og så er $\varphi(n) = \varphi(2^k) = 2^{k-1} \cdot \varphi(2) = 2^{k-1}$, som er lige. I det andet tilfælde skrives $n = p^k \cdot m$, p ulige primtal med $(p,m)=1$; da φ er multiplikativ, fås $\varphi(n) = \varphi(p^k) \cdot \varphi(m)$ med $\varphi(p^k) = p^{k-1} \cdot \varphi(p) = p^{k-1} \cdot (p-1)$. Da $p-1$ er lige, er $\varphi(n)$ lige.
2) Vi udregner først et par φ-værdier : $2 = \varphi(3)$, $4 = \varphi(8)$, $6 = \varphi(9)$, $8 = \varphi(16)$, $10 = \varphi(11)$, $12 = \varphi(13)$, $14 =$???, $16 = \varphi(17)$, $18 = \varphi(19)$, ... Et kvalificeret gæt må da være, at 14 er det mindste lige tal, som ikke tilhører værdimængden for φ. Dette eftervises nu. Beviset føres indirekte. Vi antager altså, at der findes et $n \in N$ med $\varphi(n) = 14$. Tallet n kan ikke være et primtal, for så ville jo $\varphi(n) = n-1 = 14$, dvs. $n = 15$, men 15 er jo ikke et primtal. Vi kan heller ikke have $n = p^k$, $k > 1$, p primtal, for så var $\varphi(n) = p^{k-1}(p-1) = 2 \cdot 7$, og det er oplagt umuligt. Tilbage står muligheden, at $n = a \cdot b$, $1 < a, b < n$, $(a,b) = 1$. I så fald var $\varphi(n) = \varphi(a) \cdot \varphi(b) = 2 \cdot 7$, hvilket er umuligt, da såvel $\varphi(a)$ som $\varphi(b)$ er lige tal (jf. 1)).
(Vedr. det næstmindste tal : vi finder videre $20 = \varphi(25)$, $22 = \varphi(23)$, $24 = \varphi(39)$, men $26 \notin Vm(\varphi)$, vises helt analogt).

Opgave 12. Løsningen af både 1) og 2) ligger i udnyttelsen af observationen $2^3 = 8 \equiv 1 \pmod 7$. Skriv $n = 3k + r$ med $0 \le r \le 2$. Vi har $2^n - 1 = 2^r \cdot (2^3)^k - 1 \equiv 2^r - 1 \pmod 7$ og på tilsvarende måde $2^n + 1 \equiv 2^r + 1 \pmod 7$. (i) Ved at prøve $r = 0, 1, 2$ ses, at $2^r - 1 \equiv 0 \pmod 7$ hvis og kun hvis $r = 0$, dvs. netop når n er delelig med 3. 2) Ved at prøve de tre

muligheder ses, at $2^r + 1$ aldrig giver resten 0, dvs. $2^n + 1$ er aldrig delelig med 7.

Opgave 13. Vi opløser 2730 i primfaktorer: $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. For hvert $p \in \{2, 3, 5, 7, 13\}$ gælder nu ifølge Fermats lille sætning for a med $(a, p) = 1$ at $a^{p-1} \equiv 1 \pmod{p}$. Ved at skrive $12 = (p-1) \cdot s$ (muligt for hver af de omtalte værdier af p) fås heraf, at $a^{12} = (a^{p-1})^s \equiv 1^s = 1 \pmod{p}$. For a med $(a, p) = 1$ har vi altså $p | a^{12} - 1$; for a med $(a, p) \neq 1$ gælder $p | a$. For alle a har vi da $p | a(a^{12} - 1) = a^{13} - a$. Tallet $a^{13} - a$ er altså deleligt med hver af primfaktorerne i 2730 og dermed med 2730, hvilket skulle vises.

Opgave 14. Antag $a^2 + b^2 = c^2$. Ved kvadrering fås $a^4 + b^4 + 2a^2b^2 = c^4$. Vi skal vise, at a, b eller $c \equiv 0 \pmod{5}$. Antag, at dette ikke tilfældet. Så gælder if. Fermat (eller ved gennemgang af de fire tilfælde), at a^4, b^4 og $c^4 \equiv 1 \pmod{5}$, og vi får $1 + 1 + 2a^2b^2 \equiv 1 \pmod{5}$. Dette giver $2(ab)^2 \equiv 4 \pmod{5}$. Ved forkortningsreglen fås $(ab)^2 \equiv 2$. Men dette er umuligt, da ethvert kvadrat er $\equiv 1$ eller $4 \pmod{5}$. (Ses ved gennemgang af tilfældene).

Opgave 15. (i) Hvis $(u, v) > 1$, har u og v en fælles primfaktor p. Af $p^4 | w^2$ følger $p^2 | w$, og vi får en ny ligning $u_1^4 + v_1^4 = w_1^2$, hvor $u = pu_1$, $v = pv_1$, $w = p^2 w_1$. Tilsvarende ses, at $(v, w) = (w, u) = 1$.
(ii) Ifølge (i) kan u og v ikke begge være lige. De kan heller ikke begge være ulige, for så ville $w^2 \equiv 2 \pmod{4}$, men ethvert kvadrattal er modulo 4 kongruent med enten 0 eller 1 (da $(2n)^2 = 4n^2 \equiv 0 \pmod{4}$ og $(2n+1)^2 = 4n^2 + 4n + 1 \equiv 1 \pmod{4}$).
(iii) (u^2, v^2, w) er et pythagoræisk talsæt.
(iv) Af $u^2 = a^2 - b^2$ og u ulige følger, at a må være ulige og b må være lige; de kan nemlig ikke begge være enten lige eller ulige (for så ville u^2 være lige), og hvis a var lige og b ulige, så ville $a^2 - b^2 \equiv -1 \pmod{4}$ (hvorimod $u^2 \equiv 1 \pmod{4}$). At $(a, b) = 1$ går som ovenfor.
(v) (u, b, a) er et pythagoræisk talsæt. At $(k, m) = 1$ går som ovenfor.
(vi) Vi har $v^2 = 2ab = 4km(k^2+m^2)$; følgelig er også produktet $k \cdot m \cdot (k^2+m^2)$ et kvadrattal, og da alle parrene (k, m), (m, k^2+m^2), (k^2+m^2, k) er 1 (følger let af $(k, m) = 1$), ses umiddelbart (ved betragtning af primfaktoropløsningen af hvert af tallene k, m og $k^2 + m^2$), at hver af de tre faktorer k, m og $k^2 + m^2$ selv må være kvadrattal: $k = r^2$, $m = s^2$ og $k^2 + m^2 = t^2$. Nu fås den ønskede modstrid ved: $r^4 + s^4 = k^2 + m^2 = t^2$ med $t < w$ (da $t < t^2 = k^2 + m^2 = a < a^2 < w$).