Talteori-workshop

UNF København

Ungdommens Naturvidenskabelige Forening

23. maj 2023

Program

1. Delelighed og primtal
2. Euklids algoritme
3. Modulær aritmetik
4. Perspektivering og anvendelser af modulær aritmetik
5. Tak for denne gang

Program

Hvad er talteori?

Talteori er studiet af heltallene, dvs

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

Hvad er talteori?

Talteori er studiet af heltallene, dvs

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

Talteori er en meget gammel gren af matematikken, som stammer helt tilbage til oldtiden.

Delelighed

Definition

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 $d \mid a$.

Delelighed

Definition

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 $d \mid a$.

Eksempel

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 $7 = 2 \cdot n$.

Regneregler for delelighed

Regneregler for delelighed

Definition

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. $a_k - a_{k-1} + a_{k-2} - ....$

Regneregler for delelighed

Definition

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. $a_k - a_{k-1} + a_{k-2} - ....$

Eksempel

Tværsummen af 123 er $1 + 2 + 3 = 6$. Den alternerende tværsum er $1 - 2 + 3 = 2$.
Tværsummen af 9416 er $9 + 4 + 1 + 6 = 20$, og den alternerende tværsum er $9 - 4 + 1 - 6 = 0$.

Regneregler for delelighed

Proposition

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.*

Primtal

Definition

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

Primtal

Definition

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

De første primtal er

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

En simpel primtalstest

Proposition

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).

En simpel primtalstest

Proposition

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.

En simpel primtalstest

Proposition

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.

En simpel primtalstest

Proposition

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 $a, b > 1$.

En simpel primtalstest

Proposition

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 $\sqrt{p} < a, b$.

En simpel primtalstest

Proposition

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! Ergo må p være et primtal. ■

Primtalsfaktoriseringer

En ret fascinerende egenskab ved primtal er, at de udgør "byggeklodserne" for alle andre heltal.

Primtalsfaktoriseringer

En ret fascinerende egenskab ved primtal er, at de udgør "byggeklodserne" for alle andre heltal.

Definition

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.

Primtalsfaktoriseringer

En ret fascinerende egenskab ved primtal er, at de udgør "byggeklodserne" for alle andre heltal.

Definition

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

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 $-122 = -2 \cdot 61$.

Primtalsfaktoriseringer

Sætning (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.

Primtalsfaktoriseringer

Sætning (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.

Beviset for denne sætning findes i materialet og er baseret på følgende hjælperesultat:

Lemma (Euklids lemma)

Lad a og b være heltal og p et primtal, som deler $a \cdot b$. Da deler p a eller b.

Hvor mange primtal?

Hvor mange primtal?

Sætning

Der findes uendeligt mange primtal.

Hvor mange primtal?

Sætning

Der findes uendeligt mange primtal.

Lad os tage beviset på tavlen.

Opgaver

Opgave 1.1 til 1.4 er øvelse af regnereglerne for delelighed. Opgave 1.5 og 1.6 skal bruges til senere beviser og er derfor gode at lave.

Opgave 1.9 er en sjov øvelse i at finde primtal. Diskutér gerne fremgangsmåder med hinanden! Opgave 1.10 til 1.13 er øvelse i primtalsfaktorisering. Opgave 1.14 til 1.16 omhandler forskellige typer primtal.

Program

Største fælles divisorer

Største fælles divisorer

Definition

Lad a og b være heltal. Den *største fælles divisor* af a og b er det største heltal d, som deler både a og b.

Største fælles divisorer

Definition

Lad a og b være heltal. Den *største fælles divisor* af a og b er det største heltal d, som deler både a og b.

Bemærkning

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

Største fælles divisorer

Største fælles divisorer

Eksempel

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.

Største fælles divisorer

Eksempel

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.

Lemma

For to heltal a og b gælder:

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

Euklidisk division

Følgende sætning er måske bekendt fra grundskolen.

Sætning (**Euklidisk division**)

Lad a og $b \neq 0$ være heltal. Da eksisterer der unikke heltal q og r, der opfylder $a = qb + r$ og $0 \leq r < |b|$.

Euklidisk division

Følgende sætning er måske bekendt fra grundskolen.

Sætning (**Euklidisk division**)

Lad a og $b \neq 0$ være heltal. Da eksisterer der unikke heltal q og r, der opfylder $a = qb + r$ og $0 \leq r < |b|$.

Eksempel

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

Euklids algoritme

Den primære ide til Euklids algoritme er dette resultat.

Lemma

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

Euklids algoritme

Den primære ide til Euklids algoritme er dette resultat.

Lemma

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

Dette giver os en idé til at udregne største fælles divisorer effektivt. Vi kan udregne største fælles divisorer ved blot at anvende Euklidisk division nok gange!

Euklids algoritme

Lad heltallene a og b være givet. Vi kan fjerne eventuelle fortegn på a og b, så de bliver positive. Vi omdøber $a = r_0$ og $b = r_1$. Skriv $r_0 = q_1 r_1 + r_2$ med $0 \leq r_2 < r_1$.

Euklids algoritme

Lad heltallene a og b være givet. Vi kan fjerne eventuelle fortegn på a og b, så de bliver positive. Vi omdøber $a = r_0$ og $b = r_1$. Skriv $r_0 = q_1 r_1 + r_2$ med $0 \leq r_2 < r_1$. Gentag på følgende måde:

- $r_0 = q_1 r_1 + r_2 \quad$ hvor $0 \leq r_2 < r_1$

Euklids algoritme

Lad heltallene a og b være givet. Vi kan fjerne eventuelle fortegn på a og b, så de bliver positive. Vi omdøber $a = r_0$ og $b = r_1$. Skriv $r_0 = q_1 r_1 + r_2$ med $0 \leq r_2 < r_1$. Gentag på følgende måde:

- $r_0 = q_1 r_1 + r_2 \quad$ hvor $0 \leq r_2 < r_1$
- $r_1 = q_2 r_2 + r_3 \quad$ hvor $0 \leq r_3 < r_2$

Euklids algoritme

Lad heltallene a og b være givet. Vi kan fjerne eventuelle fortegn på a og b, så de bliver positive. Vi omdøber $a = r_0$ og $b = r_1$. Skriv $r_0 = q_1 r_1 + r_2$ med $0 \leq r_2 < r_1$. Gentag på følgende måde:

- $r_0 = q_1 r_1 + r_2 \quad$ hvor $0 \leq r_2 < r_1$
- $r_1 = q_2 r_2 + r_3 \quad$ 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 $\gcd(r_0, r_1) = \gcd(a, b)$.

Eksempel

Vi ønsker at finde $\gcd(336, 148)$. Vi følger proceduren ovenover:

$$\begin{aligned} 336 &= 2 \cdot 148 + 40 \\ 148 &= 3 \cdot 40 + 28 \\ 40 &= 1 \cdot 28 + 12 \\ 28 &= 2 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 \end{aligned}$$

Det ses, at den sidste rest forskellig fra 0 er 4. Ergo er $\gcd(336, 148) = 4$.

Opgaver

Regn som udgangspunkt opgave 2.1 og 2.2. Derfra udvælger i bare, hvad I finder interessant.

Program

Modulær aritmetik

Vi skal nu indføre en ny form for regning med heltal.

Modulær aritmetik

Vi skal nu indføre en ny form for regning med heltal.

Definition

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

Modulær aritmetik

Vi skal nu indføre en ny form for regning med heltal.

Definition

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

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.

Regning med modulær aritmetik

Hvordan bestemmer vi, om $a \equiv b \pmod{n}$?

Regning med modulær aritmetik

Hvordan bestemmer vi, om $a \equiv b \pmod{n}$?

Proposition

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.*

Regning med modulær aritmetik

Hvordan bestemmer vi, om $a \equiv b \pmod{n}$?

Proposition

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.*

Korollar

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* $a \equiv r \pmod{n}$.

Regning med modulær aritmetik

$\equiv$ har nogle egenskaber lig dem for $=$:

Proposition

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).*

Regning med modulær aritmetik

$\equiv$ har nogle egenskaber lig dem for $=$:

Proposition

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).*

Dette skal I bevise som en øvelse!

Regneregler for modulær aritmetik

Spørgsmål: Kan vi bruge $+$ og $\cdot$ som sædvanligt med $\equiv$?

Regneregler for modulær aritmetik

Spørgsmål: Kan vi bruge $+$ og $\cdot$ som sædvanligt med $\equiv$?

Proposition

Lad a, b, c, d være heltal med $a \equiv c \pmod{n}$ og $b \equiv d \pmod{n}$. Da gælder:

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

Regneregler for modulær aritmetik

Spørgsmål: Kan vi bruge $+$ og $\cdot$ som sædvanligt med $\equiv$?

Proposition

Lad a, b, c, d være heltal med $a \equiv c \pmod{n}$ og $b \equiv d \pmod{n}$. Da gælder:

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

Dette betyder, at svaret er ja! Vi siger, at $+$ og $\cdot$ er *veldefinerede* regneregler.

Opgaver

Lav opgave 3.1 til 3.6.

Når I er ved at være i bund, ser vi på nogle interessante anvendelser af modulær aritmetik!

Program

ISBN

Et *ISBN* (International Standard Book Number) er en serie af tal, der står i (næsten) alle bøger, som identificerer netop den bog. Vi skal i denne opgave kigge 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:

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

ISBN

I eksemplet 978-0-471-43334-7 er 7 tjek-cifferet. Lad os verificere dette. Vi udregner:

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

ISBN

I eksemplet 978-0-471-43334-7 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.

Løsninger til heltalsligninger

Ligninger kan se ud på mange måder, f.eks. $x^2 + y^2 = 1$ (enhedscirklen), $3x + 4y + 6z = 2$ osv. Lad os se på ligninger, hvor alle variable kun kan være heltal.

Løsninger til heltalsligninger

Ligninger kan se ud på mange måder, f.eks. $x^2 + y^2 = 1$ (enhedscirklen), $3x + 4y + 6z = 2$ osv. Lad os se på ligninger, hvor alle variable kun kan være heltal.

Spørgsmål: Findes metoder til at bestemme, om en ligning har heltalsløsninger eller ej?

Lokale obstruktioner

Sætning (**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.

Lokale obstruktioner

Sætning (**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. ■

Eksempel

Betragt $3x^2 + 4y^2 = 98$.

Eksempel

Betragt $3x^2 + 4y^2 = 98$. Lad os reducere denne ligning modulo 3, da fås $y^2 \equiv 2 \pmod 3$. Findes der et y, som opfylder dette?

Eksempel

Betragt $3x^2 + 4y^2 = 98$. Lad os reducere denne ligning modulo 3, da fås $y^2 \equiv 2 \pmod 3$. Findes der et y, som opfylder dette? y kan have tre mulige rester ved division med 3, nemlig 0, 1 og 2.

Eksempel

Betragt $3x^2 + 4y^2 = 98$. Lad os reducere denne ligning modulo 3, da fås $y^2 \equiv 2 \pmod 3$. Findes der et y, som opfylder dette? y kan have tre mulige rester ved division med 3, nemlig 0, 1 og 2. Vi har

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

Eksempel

Betragt $3x^2 + 4y^2 = 98$. Lad os reducere denne ligning modulo 3, da fås $y^2 \equiv 2 \pmod 3$. Findes der et y, som opfylder dette? y kan have tre mulige rester ved division med 3, nemlig 0, 1 og 2. Vi har

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

Vi ser, at $y^2 \equiv 2 \pmod 3$ ingen løsninger har. Dermed har $3x^2 + 4y^2 = 98$ heller ingen heltalsløsninger!

Program

Tak for denne gang

Andre arrangementer (foredrag, workshops og andet) i UNF København kan ses her: https://unf.dk/aktiviteter/?department=kbh

Information om vores sommer-sciencecamps kan ses her: https://unf.dk/sciencecamps/