Øvingsforelesning 4

TMA4140 Diskret Matematikk

September 2019

"Modulo—hva er nå det for no'?"

Dagen i dag

- Repetere kongruensregning og annet underveis
- **H11.3a**: Inverser og kongruensligninger
- **H12.1**: Kinesiske restteorem
- **MS12.10 & MS15.6**: Gcd som lineærkombinasjon
- **MS17.12**: Generell tallteori
- **MS14.14, MS10.11 & MS11.1**: 2, 8, 10 og 16-tallsystemene

Kongruensregning I

Husk: $a \equiv b \mod m$ hviss $m|(a-b)$.
Eksempel:

- $17 \equiv 12 \mod 5$ siden $5|(17-12) = 5$

Kongruensregning I

Husk: $a \equiv b \mod m$ hviss $m|(a-b)$.
Eksempel:

- $17 \equiv 12 \mod 5$ siden $5|(17-12) = 5$
- $100^{100} \equiv 1^{100} \mod 99$ siden $100 \equiv 1 \mod 99$

Kongruensregning II

Husk: Ligner veldig på å regne med likninger

- Vi kan addere kongruenser med samme modulus(!)

Kongruensregning II

Husk: Ligner veldig på å regne med likninger

- Vi kan addere kongruenser med samme modulus(!)
- Multiplisere sammen kongruenser med samme modulus

Kongruensregning II

Husk: Ligner veldig på å regne med likninger

- Vi kan addere kongruenser med samme modulus(!)
- Multiplisere sammen kongruenser med samme modulus
- Men vi kan ikke alltid dele med samme tall på begge sider: $6 \equiv 3 \mod 3$ men $2 \not\equiv 1 \mod 3$.

Kongruensregning II

Husk: Ligner veldig på å regne med likninger

- Vi kan addere kongruenser med samme modulus(!)
- Multiplisere sammen kongruenser med samme modulus
- Men vi kan ikke alltid dele med samme tall på begge sider: $6 \equiv 3 \mod 3$ men $2 \not\equiv 1 \mod 3$.
- Ikke bare å dele på "null", også: $2 \cdot 1 \equiv 8 \mod 6$ men $1 \not\equiv 4 \mod 6$.

Kongruensregning II

Husk: Ligner veldig på å regne med likninger

- Vi kan addere kongruenser med samme modulus(!)
- Multiplisere sammen kongruenser med samme modulus
- Men vi kan ikke alltid dele med samme tall på begge sider: $6 \equiv 3 \mod 3$ men $2 \not\equiv 1 \mod 3$.
- Ikke bare å dele på "null", også: $2 \cdot 1 \equiv 8 \mod 6$ men $1 \not\equiv 4 \mod 6$.
- Problemet i forrige er at $2 \cdot 3 = 6 \equiv 0 \mod 6$.

Kongruensregning II

Husk: Ligner veldig på å regne med likninger

- Vi kan addere kongruenser med samme modulus(!)
- Multiplisere sammen kongruenser med samme modulus
- Men vi kan ikke alltid dele med samme tall på begge sider: $6 \equiv 3 \mod 3$ men $2 \not\equiv 1 \mod 3$.
- Ikke bare å dele på "null", også: $2 \cdot 1 \equiv 8 \mod 6$ men $1 \not\equiv 4 \mod 6$.
- Problemet i forrige er at $2 \cdot 3 = 6 \equiv 0 \mod 6$.
- Eller: $\gcd(2, 6) \neq 1$

Lineære kongruenser

Theorem

Hvis a og b er relativt primiske heltall og $m > 1$, finnes det en invers av a modulo m. I tillegg er denne inversen unik modulo m.

Lineære kongruenser

Theorem

Hvis a og b er relativt primiske heltall og $m > 1$, finnes det en invers av a modulo m. I tillegg er denne inversen unik modulo m.

M.a.o. finnes det et unikt heltall $\bar{a}$ mindre enn m som er en invers av a modulo m og alle andre inverser av a modulo m er kongruente til $\bar{a}$ modulo m.

Lineære kongruenser

Theorem

Hvis a og b er relativt primiske heltall og $m > 1$, finnes det en invers av a modulo m. I tillegg er denne inversen unik modulo m.

M.a.o. finnes det et unikt heltall $\bar{a}$ mindre enn m som er en invers av a modulo m og alle andre inverser av a modulo m er kongruente til $\bar{a}$ modulo m.

Eksempler:

- $5 \cdot 3 \equiv 1 \mod 7$ siden $15 - 14 = 1$.

Lineære kongruenser

Theorem

Hvis a og b er relativt primiske heltall og $m > 1$, finnes det en invers av a modulo m. I tillegg er denne inversen unik modulo m.

M.a.o. finnes det et unikt heltall $\bar{a}$ mindre enn m som er en invers av a modulo m og alle andre inverser av a modulo m er kongruente til $\bar{a}$ modulo m.

Eksempler:

- $5 \cdot 3 \equiv 1 \mod 7$ siden $15 - 14 = 1$.
- $5 \cdot 10 \equiv 1 \mod 7$ siden $50 - 49 = 1$.

Lineære kongruenser

Theorem

Hvis a og b er relativt primiske heltall og $m > 1$, finnes det en invers av a modulo m. I tillegg er denne inversen unik modulo m.

M.a.o. finnes det et unikt heltall $\bar{a}$ mindre enn m som er en invers av a modulo m og alle andre inverser av a modulo m er kongruente til $\bar{a}$ modulo m.

Eksempler:

- $5 \cdot 3 \equiv 1 \mod 7$ siden $15 - 14 = 1$.
- $5 \cdot 10 \equiv 1 \mod 7$ siden $50 - 49 = 1$.
- $1601 \cdot 101 \equiv 1 \mod 4620$

H11.3a

Finn $0 < x < 273$ slik at

$$100x \equiv 157 \pmod{273}.$$

Kinesisk restteorem I

Theorem

La $m_1, m_2, \ldots, m_n$ være parvis relativt primiske positive heltall mindre enn en og $a_1, a_2, \ldots, a_n$ vilkårlige heltall. Da har systemet

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n \end{aligned}$$

en unik løsning modulo $m_1 m_2 \cdots m_n$.

Kinesisk restteorem I

Theorem

La $m_1, m_2, \ldots, m_n$ være parvis relativt primiske positive heltall mindre enn en og $a_1, a_2, \ldots, a_n$ vilkårlige heltall. Da har systemet

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n \end{aligned}$$

en unik løsning modulo $m_1 m_2 \cdots m_n$.

Merk: Som med forrige resultat, finnes det en unik x slik at $0 \leq x < m$ og alle andre løsninger er kongruente modulo m til denne.

Kinesisk restteorem II

Husk at $m = m_1 \cdot m_2 \cdot \cdots \cdot m_n$.
Løsningen man lager er

$$x = a_1 \cdot m/m_1 \cdot y_1 + a_2 \cdot m/m_2 \cdot y_2 + \cdots + a_n \cdot m/m_n \cdot y_n$$

hvor y_1 er en invers av m/m_1 modulo m_1, y_2 er en invers av m/m_2 modulo m_2 og så videre.

Kinesisk restteorem II

Løsningen man lager er

$$x = a_1 \cdot m/m_1 \cdot y_1 + a_2 \cdot m/m_2 \cdot y_2 + \cdots + a_n \cdot m/m_n \cdot y_n$$

hvor y_1 er en invers av m/m_1 modulo m_1, y_2 er en invers av m/m_2 modulo m_2 og så videre.

Eksempler:

- $x \equiv 5 \mod 7$ og $x \equiv 3 \mod 5$ har løsning
  $x = 5 \cdot 5 \cdot 3 + 3 \cdot 7 \cdot 3 = 138 \equiv 33 \mod 35$.

Kinesisk restteorem II

Løsningen man lager er

$$x = a_1 \cdot m/m_1 \cdot y_1 + a_2 \cdot m/m_2 \cdot y_2 + \cdots + a_n \cdot m/m_n \cdot y_n$$

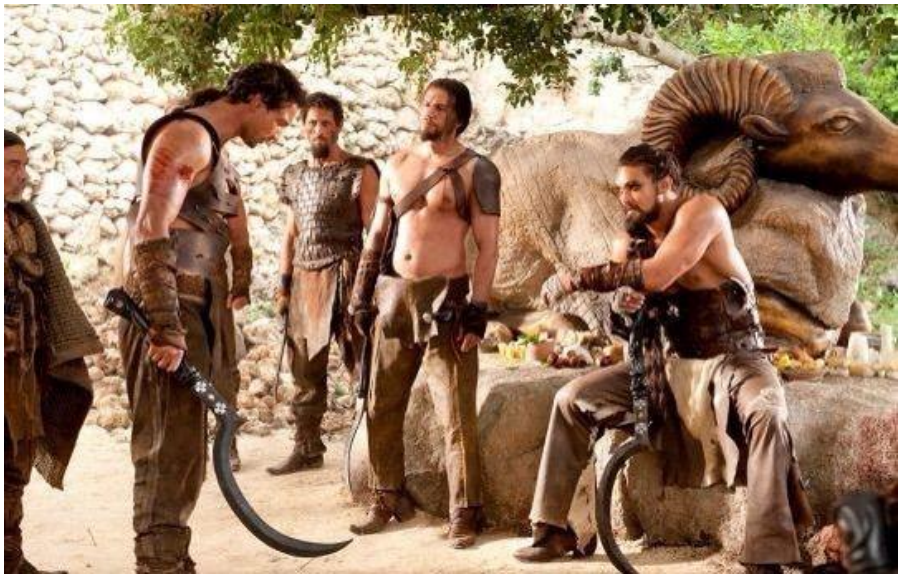
hvor y_1 er en invers av m/m_1 modulo m_1, y_2 er en invers av m/m_2 modulo m_2 og så videre.

Eksempler:

- $x \equiv 5 \mod 7$ og $x \equiv 3 \mod 5$ har løsning
  $x = 5 \cdot 5 \cdot 3 + 3 \cdot 7 \cdot 3 = 138 \equiv 33 \mod 35$.

H12.1

En bande Dothrakier plyndret med seg en sekk med gull fra Casterly Rock. Til å begynne med var det 59 dothrakier, men da de forsøkte å dele gullmyntene seg i mellom ble det 28 mynter til overs. Som seg hør og bør brøt det ut et slagsmål hvor 40 av dem døde. Når de deretter forsøkte å dele gullmyntene ble det 6 mynter til overs. Men de var nå lei av å sloss og lederen fikk de siste 6 myntene selv. Hvor mange gullmynter var det i sekken? (Gitt at sekken ikke rommer mer enn 1200 mynter.)



Største felles divisor og Bezout

Theorem

Hvis a og b er positive heltall, finnes det heltall s og t slik at $\gcd(a, b) = sa + tb$.

Største felles divisor og Bezout

Theorem

Hvis a og b er positive heltall, finnes det heltall s og t slik at $\gcd(a, b) = sa + tb$.

Merk: Hvis $sa + tb = 1$ for noen $s, t \in \mathbb{Z}$, kan man ikke ha $gcd(a, b) > 1$. Hvorfor ikke?

Største felles divisor og Bezout

Theorem

Hvis a og b er positive heltall, finnes det heltall s og t slik at $\gcd(a, b) = sa + tb$.

- **Merk:** Hvis $sa + tb = 1$ for noen $s, t \in \mathbb{Z}$, kan man ikke ha $gcd(a, b) > 1$. Hvorfor ikke?
- Likningen gir en øvre grense for gcd!
- $6 - 5 = 1$
- $4 \cdot 252 - 5 \cdot 198 = 18$

Største felles divisor og Bezout

Theorem

Hvis a og b er positive heltall, finnes det heltall s og t slik at $\gcd(a, b) = sa + tb$.

- **Merk:** Hvis $sa + tb = 1$ for noen $s, t \in \mathbb{Z}$, kan man ikke ha $gcd(a, b) > 1$. Hvorfor ikke?
- Likningen gir en øvre grense for gcd!
- $6 - 5 = 1$
- $4 \cdot 252 - 5 \cdot 198 = 18$

MS12.10

For hvilke av følgende ligninger eksisterer det $s, t \in \mathbb{Z}$ slik at ligningen er tilfredsstilt?

Alt 1) $490256s + 337t = 5$

Alt 2) $825s + 315t = 5$

Alt 3) $33649s + 3059t = 1$

Alt 4) $2695s + 4199t = 1$

MS12.10

For hvilke av følgende ligninger eksisterer det $s, t \in \mathbb{Z}$ slik at ligningen er tilfredsstilt?

Alt 1) $490256s + 337t = 5$

Alt 2) $825s + 315t = 5$

Alt 3) $33649s + 3059t = 1$

Alt 4) $2695s + 4199t = 1$

MS12.10

For hvilke av følgende ligninger eksisterer det $s, t \in \mathbb{Z}$ slik at ligningen er tilfredsstilt?

Alt 1) $490256s + 337t = 5$

Alt 2) $825s + 315t = 5$

Alt 3) $33649s + 3059t = 1$

Alt 4) $2695s + 4199t = 1$

MS12.10

For hvilke av følgende ligninger eksisterer det $s, t \in \mathbb{Z}$ slik at ligningen er tilfredsstilt?

Alt 1) $490256s + 337t = 5$

Alt 2) $825s + 315t = 5$

Alt 3) $33649s + 3059t = 1$

Alt 4) $2695s + 4199t = 1$

MS15.6

Hvilke av følgende utsagn er garantert riktige?

Alt 1) La q være et primtall og la $b \in \mathbb{Z}^+$ slik at q ikke er divisor i b. Det finnes $s, t \in \mathbb{Z}$ slik at $sq + tb = 13$.

Alt 2) La q være et primtall. Det finnes $s, t \in \mathbb{Z}$ slik at $s(q+1) + t(q+2) = 2$.

Alt 3) La q være et primtall. Det finnes $s, t \in \mathbb{Z}$ slik at $s(q+1) + t(q+3) = 1$.

Alt 4) La a, b være naturlige tall ≥ 5 slik at $\gcd(a, b) = 1$. Det finnes $s, t \in \mathbb{Z}$ slik at $s(a-1) + t(b-2) = 1$.

MS15.6

Hvilke av følgende utsagn er garantert riktige?

Alt 1) La q være et primtall og la $b \in \mathbb{Z}^+$ slik at q ikke er divisor i b. Det finnes $s, t \in \mathbb{Z}$ slik at $sq + tb = 13$.

Alt 2) La q være et primtall. Det finnes $s, t \in \mathbb{Z}$ slik at $s(q+1) + t(q+2) = 2$.

Alt 3) La q være et primtall. Det finnes $s, t \in \mathbb{Z}$ slik at $s(q+1) + t(q+3) = 1$.

Alt 4) La a, b være naturlige tall ≥ 5 slik at $\gcd(a, b) = 1$. Det finnes $s, t \in \mathbb{Z}$ slik at $s(a-1) + t(b-2) = 1$.

MS15.6

Hvilke av følgende utsagn er garantert riktige?

Alt 1) La q være et primtall og la $b \in \mathbb{Z}^+$ slik at q ikke er divisor i b. Det finnes $s, t \in \mathbb{Z}$ slik at $sq + tb = 13$.

Alt 2) La q være et primtall. Det finnes $s, t \in \mathbb{Z}$ slik at $s(q+1) + t(q+2) = 2$.

Alt 3) La q være et primtall. Det finnes $s, t \in \mathbb{Z}$ slik at $s(q+1) + t(q+3) = 1$.

Alt 4) La a, b være naturlige tall ≥ 5 slik at $\gcd(a, b) = 1$. Det finnes $s, t \in \mathbb{Z}$ slik at $s(a-1) + t(b-2) = 1$.

MS15.6

Hvilke av følgende utsagn er garantert riktige?

Alt 1) La q være et primtall og la $b \in \mathbb{Z}^+$ slik at q ikke er divisor i b. Det finnes $s, t \in \mathbb{Z}$ slik at $sq + tb = 13$.

Alt 2) La q være et primtall. Det finnes $s, t \in \mathbb{Z}$ slik at $s(q+1) + t(q+2) = 2$.

Alt 3) La q være et primtall. Det finnes $s, t \in \mathbb{Z}$ slik at $s(q+1) + t(q+3) = 1$.

Alt 4) La a, b være naturlige tall ≥ 5 slik at $\gcd(a, b) = 1$. Det finnes $s, t \in \mathbb{Z}$ slik at $s(a-1) + t(b-2) = 1$.

MS17.12

Hvilke av følgende utsagn er garantert riktige?

Alt 1) La p være et odde primtall og la $a \geq 2$ være et partall. Da vil $a^{(p-1)} \equiv 1 \mod p$.

Alt 2) La $a, b \in \mathbb{Z}^+$ dele 2341. Da finnes $s, t \in \mathbb{Z}$ slik at $sa + tb = 4862$.

Alt 3) La $a, b \in \mathbb{Z}^+$, $a, b \geq 2$, være relativt primiske. Da finnes $s, t \in \mathbb{Z}$ slik at $s(a+1) + t(b+2) = 1$.

Alt 4) $23939^{419} \equiv -1 \mod 420$

MS17.12

Hvilke av følgende utsagn er garantert riktige?

Alt 1) La p være et odde primtall og la $a \geq 2$ være et partall. Da vil $a^{(p-1)} \equiv 1 \mod p$.

Alt 2) La $a, b \in \mathbb{Z}^+$ dele 2341. Da finnes $s, t \in \mathbb{Z}$ slik at $sa + tb = 4862$.

Alt 3) La $a, b \in \mathbb{Z}^+$, $a, b \geq 2$, være relativt primiske. Da finnes $s, t \in \mathbb{Z}$ slik at $s(a+1) + t(b+2) = 1$.

Alt 4) $23939^{419} \equiv -1 \mod 420$

MS17.12

Hvilke av følgende utsagn er garantert riktige?

Alt 1) La p være et odde primtall og la $a \geq 2$ være et partall. Da vil $a^{(p-1)} \equiv 1 \mod p$.

Alt 2) La $a, b \in \mathbb{Z}^+$ dele 2341. Da finnes $s, t \in \mathbb{Z}$ slik at $sa + tb = 4862$.

Alt 3) La $a, b \in \mathbb{Z}^+$, $a, b \geq 2$, være relativt primiske. Da finnes $s, t \in \mathbb{Z}$ slik at $s(a+1) + t(b+2) = 1$.

Alt 4) $23939^{419} \equiv -1 \mod 420$

MS17.12

Hvilke av følgende utsagn er garantert riktige?

Alt 1) La p være et odde primtall og la $a \geq 2$ være et partall. Da vil $a^{(p-1)} \equiv 1 \mod p$.

Alt 2) La $a, b \in \mathbb{Z}^+$ dele 2341. Da finnes $s, t \in \mathbb{Z}$ slik at $sa + tb = 4862$.

Alt 3) La $a, b \in \mathbb{Z}^+$, $a, b \geq 2$, være relativt primiske. Da finnes $s, t \in \mathbb{Z}$ slik at $s(a+1) + t(b+2) = 1$.

Alt 4) $23939^{419} \equiv -1 \mod 420$

Binære, oktale og heksidesimale representasjoner av heltall

Husk: For å bruke heksidesimale representasjoner utvider vi mengden med siffer på kanskje den enkleste tenkelige måten:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$$

.

Eksempler:

- $(B2B)_{16} = 11 \cdot 16^2 + 2 \cdot 16^1 + 11 \cdot 16^0$
- $(10110010101011)_2 = 1 \cdot 2^{11} + 0 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 0 \cdots + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$
- $(5453)_8 = 5 \cdot 8^3 + 4 \cdot 8^2 + 5 \cdot 8^1 + 3 \cdot 8^0$

Binære, oktale og heksidesimale representasjoner av heltall

Husk: For å bruke heksidesimale representasjoner utvider vi mengden med siffer på kanskje den enkleste tenkelige måten:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$$

.

Eksempler:

- $(B2B)_{16} = 11 \cdot 16^2 + 2 \cdot 16^1 + 11 \cdot 16^0$
- $(101100101011)_2 =$
  $1 \cdot 2^{11} + 0 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 0 \cdot \cdots + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$
- $(5453)_8 = 5 \cdot 8^3 + 4 \cdot 8^2 + 5 \cdot 8^1 + 3 \cdot 8^0$

Binære, oktale og heksidesimale representasjoner av heltall

Husk: For å bruke heksidesimale representasjoner utvider vi mengden med siffer på kanskje den enkleste tenkelige måten:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$$

.

Eksempler:

- $(B2B)_{16} = 11 \cdot 16^2 + 2 \cdot 16^1 + 11 \cdot 16^0$
- $(101100101011)_2 =$
  $1 \cdot 2^{11} + 0 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 0 \cdot \cdots + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$
- $(5453)_8 = 5 \cdot 8^3 + 4 \cdot 8^2 + 5 \cdot 8^1 + 3 \cdot 8^0$

Finne binær og oktal representasjon av et heksidesimaltall

Vi kan oversette til binær og så til oktal.

Eksempler:

- $(CB)_{16} = (11001011)_2 = (313)_8$

For multiple choice oppgaver er ikke dette alltid nødvendig: kan bruke kongruenser.

Summer og produkt av binær, oktal, og heksidesimaltall

- For sum er det greit å bruke algoritmen vi er vant til: $(ABC)_{16} + (DE)_{16} = (B9A)_{16}$
- For produkt er det greit å oversette til desimaltall, gjøre beregningen der, og så oversette tilbake

Summer og produkt av binær, oktal, og heksidesimaltall

- For sum er det greit å bruke algoritmen vi er vant til: $(ABC)_{16} + (DE)_{16} = (B9A)_{16}$
- For produkt er det greit å oversette til desimaltall, gjøre beregningen der, og så oversette tilbake

MS14.14

Hva er den hexadesimale (dvs. grunntall 16) fremstillingen av $(ABCD)_{16} + (F5E)_{16}$?

Alt 1) $(AB2B)_{16}$

Alt 2) $(BB2B)_{16}$

Alt 3) $(BC2B)_{16}$

Alt 4) $(BB1B)_{16}$

Finne heksidesimalrepresentasjon av desimaltall

- Hvordan finner vi den binære, oktale, eller heksidesimale representasjonen av et desimaltall?
- Vi gjennomfører divisjon med rest med divisor henholdsvis 2, 8, 16 på kvotientene vi får til det stopper opp.
- Hvorfor? Vi ønsker å få et utrykk bestående av ledd som involverer divisoren og rester under divisjon med divisoren.

Eksempel: $(14)_{10} = (1110)_2$

$$14 = 2 \cdot 7 + 0$$
$$7 = 2 \cdot 3 + 1$$
$$3 = 2 \cdot 1 + 1$$
$$1 = 2 \cdot 0 + 1$$

Finne heksidesimalrepresentasjon av desimaltall

- Hvordan finner vi den binære, oktale, eller heksidesimale representasjonen av et desimaltall?
- Vi gjennomfører divisjon med rest med divisor henholdsvis 2, 8, 16 på kvotientene vi får til det stopper opp.
- Hvorfor? Vi ønsker å få et utrykk bestående av ledd som involverer divisoren og rester under divisjon med divisoren.

Eksempel: $(14)_{10} = (1110)_2$

$$14 = 2 \cdot 7 + 0$$
$$7 = 2 \cdot 3 + 1$$
$$3 = 2 \cdot 1 + 1$$
$$1 = 2 \cdot 0 + 1$$

Finne heksidesimalrepresentasjon av desimaltall

- Hvordan finner vi den binære, oktale, eller heksidesimale representasjonen av et desimaltall?
- Vi gjennomfører divisjon med rest med divisor henholdsvis 2, 8, 16 på kvotientene vi får til det stopper opp.
- Hvorfor? Vi ønsker å få et utrykk bestående av ledd som involverer divisoren og rester under divisjon med divisoren.

Eksempel: $(14)_{10} = (1110)_2$

$$
\begin{aligned}
14 &= 2 \cdot 7 + 0 \\
7 &= 2 \cdot 3 + 1 \\
3 &= 2 \cdot 1 + 1 \\
1 &= 2 \cdot 0 + 1
\end{aligned}
$$

MS10.11: Direkte oversettelse og kongruenser.

Oppgave 11: Hvilke tall er lik $(ABCD)_{16}$?

Alt 1) $(1010101111001101)_2$

Alt 2) $(43982)_{10}$

Alt 3) $(43981)_8$

Alt 4) $(47342)_8$

MS11.1

Hva er $(213986)_{10}$ i det hexadesimale tallsystemet?

Alt 1) $(344F2)_{16}$

Alt 2) $(343F2)_{16}$

Alt 3) $(344E2)_{16}$

Alt 4) $(343E2)_{16}$