Matematik baskurs, med diskret matematik

SF1671

Föreläsare: Petter Brändén

Föreläsning 10

Primtal

- Ett **primtal** är ett heltal $p > 1$ vars enda positiva delare är p och 1.
- $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots$

Aritmetikens fundamentalsats

Varje heltal $a \geq 2$ kan entydigt skrivas som en produkt av primtal

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m},$$

där $p_1 < p_2 < \cdots < p_m$ är primtal och $\alpha_1, \ldots, \alpha_m$ är positiva heltal.

Viktigt i tillämpning som tex
RSA-krypto.

Primtal

- Ett **primtal** är ett heltal $p > 1$ vars enda positiva delare är p och 1.
- $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots$

Aritmetikens fundamentalsats

Varje heltal $a \geq 2$ kan entydigt skrivas som en produkt av primtal

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m},$$

där $p_1 < p_2 < \cdots < p_m$ är primtal och $\alpha_1, \ldots, \alpha_m$ är positiva heltal.

- $150 = 2 \cdot 3 \cdot 5^2$ och $140 = 2^2 \cdot 5 \cdot 7$.

Motsägelsebevis.

- Antag att vi vill bevisa att ett påstående P.

Motsägelsebevis.

- Antag att vi vill bevisa att ett påstående P.
- Ett vanligt förfarande är att antaga att P är falskt och ur det antagandet härleda något som är uppenbart falskt.

Tex $0 = 1$

Motsägelsebevis.

- Antag att vi vill bevisa att ett påstående P.
- Ett vanligt förfarande är att antaga att P är falskt och ur det antagandet härleda något som är uppenbart falskt.
- Då måste P vara sann.

Motsägelsebevis.

- Antag att vi vill bevisa att ett påstående P.
- Ett vanligt förfarande är att antaga att P är falskt och ur det antagandet härleda något som är uppenbart falskt.
- Då måste P vara sann.
- Sats (Euklides). "Det finns oändligt många primtal." P

Bevis: Antag att P är falsk, dvs det finns bara ändligt många primtal, säg $p_1, p_2, p_3, \ldots, p_N$

Bilda ett nytt tal $m = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$

m lämnar resten 1 vid division med alla primtal, så m är inte delbart med något primtal.

Detta är en motsägelse, eftersom alla tal är delbara med primtal.

Så därför är P sann.

Motsägelsebevis.

- Antag att vi vill bevisa att ett påstående P.
- Ett vanligt förfarande är att antaga att P är falskt och ur det antagandet härleda något som är uppenbart falskt.
- Då måste P vara sann.
- Sats (Euklides). Det finns oändligt många primtal.

Kontrapositivt bevis.

- Antag att vi vill bevisa en implikation av påståenden: $P \implies Q$.

Motsägelsebevis.

- Antag att vi vill bevisa att ett påstående P.
- Ett vanligt förfarande är att antaga att P är falskt och ur det antagandet härleda något som är uppenbart falskt.
- Då måste P vara sann.
- Sats (Euklides). Det finns oändligt många primtal.

Kontrapositivt bevis.

- Antag att vi vill bevisa en implikation av påståenden: $P \implies Q$.
- Då kan vi istället bevisa

$$(Q \text{ är falsk}) \implies (P \text{ är falsk})$$

Bevis av Aritmetikens fundamentalsats.

Existens.

Vill visa att varje tal $n \geq 2$ kan skrivas som produkt av primtal.

Bevis av Aritmetikens fundamentalsats.

Existens.

Vill visa att varje tal $n \geq 2$ kan skrivas som produkt av primtal.

- Tag godtyckligt $n \geq 2$.
- Är n ett primtal?

Bevis av Aritmetikens fundamentalsats.

Existens.

Vill visa att varje tal $n \geq 2$ kan skrivas som produkt av primtal.

- Tag godtyckligt $n \geq 2$.
- Är n ett primtal?
- Om svaret är ja, så är vi klara.

Bevis av Aritmetikens fundamentalsats.

Existens.

Vill visa att varje tal $n \geq 2$ kan skrivas som produkt av primtal.

- Tag godtyckligt $n \geq 2$.
- Är n ett primtal?
- Om svaret är ja, så är vi klara.
- Annars är $n = ab$ där $1 < a < n$ och $1 < b < n$.

Bevis av Aritmetikens fundamentalsats.

Existens.

Vill visa att varje tal $n \geq 2$ kan skrivas som produkt av primtal.

- Tag godtyckligt $n \geq 2$.
- Är n ett primtal?
- Om svaret är ja, så är vi klara.
- Annars är $n = ab$ där $1 < a < n$ och $1 < b < n$.
- Fortsätt att fråga a och b är primtal o.s.v.

Bevis av Aritmetikens fundamentalsats.

Existens.

Vill visa att varje tal $n \geq 2$ kan skrivas som produkt av primtal.

- Tag godtyckligt $n \geq 2$.
- Är n ett primtal?
- Om svaret är ja, så är vi klara.
- Annars är $n = ab$ där $1 < a < n$ och $1 < b < n$.
- Fortsätt att fråga a och b är primtal o.s.v.
- Algoritmen resulterar i en faktorisering av n i primtal.

12

$12 = 3 \cdot 4$

Ja

Nej

$4 = 2 \cdot 2$

Ja

ja

$12 = 3 \cdot 2 \cdot 2$

Bevis av Aritmetikens fundamentalsats.

Unikhet. (Dvs att vi bara skriva på ett sätt)

Kom ihåg

Korollarium

Om $d \mid ab$ och $\mathrm{sgd}(a, d) = 1$, så $d \mid b$.

Bevis av Aritmetikens fundamentalsats.

Unikhet.

Kom ihåg

Korollarium

Om $d \mid ab$ och $\mathrm{sgd}(a, d) = 1$, så $d \mid b$.

$$\Downarrow$$

Lemma (Hjälpsats)

Låt a, b vara heltal och p ett primtal.

$$p \mid ab \implies p \mid a \text{ eller } p \mid b.$$

Bevis av Aritmetikens fundamentalsats.

Unikhet.
Kom ihåg

Korollarium

Om $d \mid ab$ och $\mathrm{sgd}(a, d) = 1$, så $d \mid b$.

Lemma (Hjälpsats)

Låt a, b vara heltal och p ett primtal.

$$p \mid ab \implies p \mid a \text{ eller } p \mid b.$$

Lemma A

Låt $a_1, a_2, \ldots, a_k$ vara heltal och p ett primtal.

$$p \mid (a_1 a_2 \cdots a_k) \implies p \mid a_i \text{ för något } i.$$

Bevis av Aritmetikens fundamentalsats.

Unikhet.

Motsägelsebevis.

Bevis av Aritmetikens fundamentalsats.

Unikhet.

Motsägelsebevis. Antag falskt.

- Antag att det finns ett tal med två olika faktoriseringar:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell},$$

där vi har förkortat bort gemensamma primtalsfaktorer.

$\Rightarrow p_i \neq q_j$ för alla i, j

Bevis av Aritmetikens fundamentalsats.

Unikhet.

Motsägelsebevis.

- Antag att det finns ett tal med två olika faktoriseringar:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell},$$

  där vi har förkortat bort gemensamma primtalsfaktorer.
- Eftersom p_1 delar n, så delar p_1 högerledet.

Bevis av Aritmetikens fundamentalsats.

Unikhet.

Motsägelsebevis.

- Antag att det finns ett tal med två olika faktoriseringar:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell},$$

  där vi har förkortat bort gemensamma primtalsfaktorer.
- Eftersom p_1 delar n, så delar p_1 högerledet.
- Från Lemma A följer att $p_1 \mid q_j$ för något j, dvs $p_1 = q_j$.

(eftersom p_1 är primtal)

Bevis av Aritmetikens fundamentalsats.

Unikhet.

Motsägelsebevis.

- Antag att det finns ett tal med två olika faktoriseringar:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell},$$

  där vi har förkortat bort gemensamma primtalsfaktorer.
- Eftersom p_1 delar n, så delar p_1 högerledet.
- Från Lemma A följer att $p_1 \mid q_j$ för något j, dvs $p_1 = q_j$.
- Detta är en motsägelse eftersom vi antog att vi hade förkortat bort gemensamma primtalsfaktorer.

$\square$

Polynom

- Mängden av alla polynom i variabeln x med reella koefficienter betecknas $\mathbb{R}[x]$.

x är den obekanta variabeln

$$p(x) = 2x^2 - 3x + 2$$

$$= -\sqrt{3}\, x^7 + 6x^3 - 2 \cdot e$$

Polynom

- Mängden av alla polynom i variabeln x med reella koefficienter betecknas $\mathbb{R}[x]$.
- Ett polynom är **moniskt** om ledande koefficienten är lika med ett.

moniskt: $x^7 - \sqrt{2}\, x^3 + 8$

ej moniskt: $8x^3 + 2$

Polynom

- Mängden av alla polynom i variabeln x med reella koefficienter betecknas $\mathbb{R}[x]$.
- Ett polynom är **moniskt** om ledande koefficienten är lika med ett.

Om $f(x) = d(x) \cdot q(x)$ så säger vi att $d(x)$ är en delare till $f(x)$.

Största gemensamma delare

Låt $f, g \in \mathbb{R}[x]$, inte båda lika med 0. **Största gemensamma delare** till f och g är det unika moniska polynom d s.a.

$d(x) \mid f(x)$

1. $d \mid f$ och $d \mid g$, (gemensam delare)
2. Om $c \mid f$ och $c \mid g$, så $c \mid d$ (största) (d delas av alla andra gemensamma delare)

$d = d(x)$

(spara plats)

Polynom

- Mängden av alla polynom i variabeln x med reella koefficienter betecknas $\mathbb{R}[x]$.
- Ett polynom är **moniskt** om ledande koefficienten är lika med ett.

Största gemensamma delare

Låt $f, g \in \mathbb{R}[x]$, inte båda lika med 0. **Största gemensamma delare** till f och g är det unika moniska polynom d s.a.

1. $d \mid f$ och $d \mid g$, (gemensam delare)
2. Om $c \mid f$ och $c \mid g$, så $c \mid d$ (största)

- $d = \mathrm{sgd}(f, g)$ existerar och är unik eftersom vi har en Euklides algoritm för polynom. Följer av divisionsalg. (liggande stolen)
- Funkar precis likadant som för heltal pga satsen om polynomdivision.

- **Sats** (Polynomdivision). Antag att f och d är polynom och $d \neq 0$. Då finns **unika** polynom r och q s.a.

$$f = d \cdot q + r, \qquad \text{och } \deg r < \deg d.$$

"liggande stolen"

graden

- **Sats** (Polynomdivision). Antag att f och d är polynom och $d \neq 0$. Då finns **unika** polynom r och q s.a.

$$f = d \cdot q + r, \qquad \text{och } \deg r < \deg d.$$

- **Exempel**. Bestäm $\operatorname{sgd}(\underbrace{x^4 - x^3 - x^2 + 1}_{=f}, \underbrace{x^3 - 1}_{=g})$.

mha Euklides alg. Dela f med g

$$\begin{array}{l|l}
\multicolumn{1}{l}{x - 1} & \\
\hline
x^4 - x^3 - x^2 + 1 & \underline{x^3 - 1} \\
-(x^4 - x) & \\
\hline
-x^3 - x^2 + x + 1 & \\
-(-x^3 + 1) & \\
\hline
-x^2 + x &
\end{array}$$

$f = (x-1)g + -x^2 + x$

$x^3 - 1 = (-x-1)(-x^2+x) + (x-1)$

(liggande stolen)

$-x^2 + x = (-x)(x-1) + 0$

$\operatorname{sgd}(f, g) = x - 1$

sista nollskilda resten, vilket ger sgd enligt Euklides alg.

- På samma sätt som för heltal (baklänges i Euklides) får vi
- Bezouts sats. Låt $f, g \in \mathbb{R}[x]$, inte båda lika med 0. Det finns polynom a, b s.a.

$$\mathrm{sgd}(f, g) = a \cdot f + b \cdot g.$$

- På samma sätt som för heltal (baklänges i Euklides) får vi
- Bezouts sats. Låt $f, g \in \mathbb{R}[x]$, inte båda lika med 0. Det finns polynom a, b s.a.

$$\mathrm{sgd}(f, g) = a \cdot f + b \cdot g.$$

- Exempel. $\mathrm{sgd}(\underbrace{x^4 - x^3 - x^2 + 1}_{=f}, \underbrace{x^3 - 1}_{=g})$.

$$x^4 - x^3 - x^2 + 1 = (x-1)(x^3-1) + (-x^2+x)$$

$$x^3 - 1 = (-x-1)(-x^2+x) + (x-1)$$

$$\mathrm{sgd} = x-1 = g - (-x-1)(-x^2+x) = g + (x+1)\Big(f - (x-1)\overbrace{(x^3-1)}^{g=}\Big)$$

$$= \big(1 - (x+1)(x-1)\big)g + (x+1)f$$

$$= (x+1)f + (-x^2+2)g$$

- Ett polynom f är **reducibelt** om $f = d \cdot q$, där d, q är polynom som inte är konstanter.

- Ett polynom f är **reducibelt** om $f = d \cdot q$, där d, q är polynom som inte är konstanter.
- Ett polynom som inte är konstant eller reducibelt kallas för **irreducibelt**.
- (Motsvarigheten till primtal)

- Ett polynom f är **reducibelt** om $f = d \cdot q$, där d, q är polynom som inte är konstanter.
- Ett polynom som inte är konstant eller reducibelt kallas för **irreducibelt**.
- (Motsvarigheten till primtal)
- Genom att använda sig av Bezouts sats, som för heltalen, får vi:

Motsvarigheten till Aritmetikens fund. sats.

- Sats. Varje polynom $f \neq 0$ kan entydigt skrivas på formen

$$f = \lambda \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

där $p_1, \dots, p_n$ är irreducibla moniska polynom, $\alpha_1, \dots, \alpha_n$ är positiva heltal och λ är en konstant.

- Ett polynom f är **reducibelt** om $f = d \cdot q$, där d, q är polynom som inte är konstanter.
- Ett polynom som inte är konstant eller reducibelt kallas för **irreducibelt**.

  • Alla pol. av grad 1 är irred.
  • Polynom av grad 2 utan nollställen är irreducibla.
- (Motsvarigheten till primtal)
- Genom att använda sig av Bezouts sats, som för heltalen, får vi:
- Sats. Varje polynom $f \neq 0$ kan entydigt skrivas på formen

$$f = \lambda \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

  där $p_1, \ldots, p_n$ är irreducibla moniska polynom, $\alpha_1, \ldots, \alpha_n$ är positiva heltal och λ är en konstant.
- Exempel. $4x^6 - x^2$. $= 4 \cdot x^2 (x^4 - \frac{1}{4}) = 4 \cdot x^2 (x^2 - \frac{1}{2})(x^2 + \frac{1}{2})$

$$= 4 \cdot x^2 \cdot (x - \tfrac{1}{\sqrt{2}})(x + \tfrac{1}{\sqrt{2}})\underbrace{(x^2 + \tfrac{1}{2})}_{\text{irreducibel}}$$

- Man definierar $\mathrm{mgm}(f,g)$ som för heltal.

Minsta gemensamma multipel

Låt $f,g \in \mathbb{R}[x]$ vara två nollskilda polynom. Den **minsta gemensamma multipel** till f och g är det unika moniska polynom $h = \mathrm{mgm}(f,g)$ s.a.

1. $f \mid h$ och $g \mid h$, (gemensam multipel)
2. Om $f \mid s$ och $c \mid s$, så $h \mid s$ (minsta)

- Som för heltal följer att

$$\mathrm{mgm}(f,g) \cdot \mathrm{sgd}(f,g) = f \cdot g.$$

Modulär aritmetik

- Utvecklades av Carl Friedrich Gauss (1777–1855) vid 24 års ålder.

Modulär aritmetik

- Vi lär oss tidigt att skilja på jämna och udda tal.

Modulär aritmetik

- Vi lär oss tidigt att skilja på jämna och udda tal.
- Även räkneregler för dem.

jämn + udda = udda

udda + udda = jämn

...

Modulär aritmetik

- Vi lär oss tidigt att skilja på jämna och udda tal.
- Även räkneregler för dem.
- Vi lär oss också att räkna med klockan:
- Om klockan är 21, dvs 9 på kvällen. Vad är då klockan 56 timmar senare. Jo

$$21 + 56 = 77 = 3 \cdot 24 + 5$$

- Så klockan är 5 på morgonen.

Modulär aritmetik

- Låt $m \geq 2$ vara ett heltal.

Modulär aritmetik

- Låt $m \geq 2$ vara ett heltal.
- Om x, y är heltal så säger vi att x är **kongruent** med y **modulo** m om $m \mid (x - y)$,

Modulär aritmetik

- Låt $m \geq 2$ vara ett heltal.
- Om x, y är heltal så säger vi att x är **kongruent** med y **modulo** m om $m \mid (x - y)$,
- dvs omm x och y lämnar samma rest vid division med m.

Modulär aritmetik

- Låt $m \geq 2$ vara ett heltal.
- Om x, y är heltal så säger vi att x är **kongruent** med y **modulo** m om $m \mid (x - y)$,
- dvs omm x och y lämnar samma rest vid division med m.
- Vi skriver $x \equiv y \mod m$, eller $x \equiv_m y$.

Modulär aritmetik

- Låt $m \geq 2$ vara ett heltal.
- Om x, y är heltal så säger vi att x är **kongruent** med y **modulo** m om $m \mid (x - y)$,
- dvs omm x och y lämnar samma rest vid division med m.
- Vi skriver $x \equiv y \mod m$, eller $x \equiv_m y$.
- $77 \equiv_{24} 5$, eftersom $77 = 3 \cdot 24 + 5$.

$77 \equiv_{24} 29 \qquad 29 = 1 \cdot 24 + 5$

Modulär aritmetik

- Låt $m \geq 2$ vara ett heltal.
- Om x, y är heltal så säger vi att x är **kongruent** med y **modulo** m om $m \mid (x - y)$,
- dvs omm x och y lämnar samma rest vid division med m.
- Vi skriver $x \equiv y \mod m$, eller $x \equiv_m y$.
- $77 \equiv_{24} 5$, eftersom $77 = 3 \cdot 24 + 5$.
- $1038 \equiv_9 1020$, eftersom $1020 - 1038 = -18 = (-2) \cdot 9$.

Modulär aritmetik

- Låt $m \geq 2$ vara ett heltal.
- Om x, y är heltal så säger vi att x är **kongruent** med y **modulo** m om $m \mid (x - y)$,
- dvs omm x och y lämnar samma rest vid division med m.
- Vi skriver $x \equiv y \mod m$, eller $x \equiv_m y$.
- $77 \equiv_{24} 5$, eftersom $77 = 3 \cdot 24 + 5$.
- $1038 \equiv_9 1020$, eftersom $1020 - 1038 = -18 = (-2) \cdot 9$.
- $\equiv_m$ är en ekvivalensrelation på $\mathbb{Z}$. Visades förra veckan.
- De olika ekvivalensklasserna är $[0], [1], \ldots, [m-1]$, dvs en klass för varje möjlig rest: $[x] = \{ y \in \mathbb{Z} \mid y \equiv_m x \}$

$$[r] = \{\ldots, r - 3m, r - 2m, r - m, r, r + m, r + 2m, r + 3m, \ldots\}.$$

alla som ger resten r vid division med m

Sats (Räkna med rester)

Om $x_1 \equiv_m x_2$ och $y_1 \equiv_m y_2$, så

$$x_1 + y_1 \equiv_m x_2 + y_2 \quad \text{och}$$
$$x_1 y_1 \equiv_m x_2 y_2.$$

Bevis:

$x_1 \equiv_m x_2 \iff m \mid (x_1 - x_2) \iff x_1 - x_2 = km$ ngt k

$y_1 \equiv_m y_2 \iff m \mid (y_1 - y_2) \iff y_1 - y_2 = l \cdot m$ ngt l

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = k \cdot m + lm$$
$$= (k + l) \cdot m$$

Så $m \mid [(x_1 + y_1) - (x_2 + y_2)]$ dvs $x_1 + y_1 \equiv_m x_2 + y_2$

- Alltså kan man “räkna” med resterna (ekvivalensklasserna).
- Man skriver $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. $\Leftarrow$ alla möjliga rester.
- Om $x, y \in \mathbb{Z}_m$:

$$x + y = \text{ resten av } x + y \text{ vid division med } m$$
$$x \cdot y = \text{ resten av } x \cdot y \text{ vid division med } m.$$

$\underline{m = 3}$

$\mathbb{Z}_3 = \{0, 1, 2\}$

$0+0=0$, $0+2=2$

$1+1=2$, $1+2=3 \equiv_3 0$

$2+2=4 \equiv_3 1$

$2 \cdot 2 = 4 \equiv_3 1$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$$1+3=4 \equiv_4 0$$

$$2+3=5 \equiv_5 1$$

$$3 \cdot 3 = 9 \equiv_4 1$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- De vanliga räknereglerna gäller i $\mathbb{Z}_m$:

$$x + y = y + x \text{ och } xy = yx$$ kommutativ

$$x + (y + z) = (x + y) + z \text{ och } x(yz) = (xy)z$$ associativ

$$x(y + z) = xy + xz$$ distribut~~a~~tiv

- De vanliga räknereglerna gäller i $\mathbb{Z}_m$:

$$x + y = y + x \text{ och } xy = yx \qquad \text{kommutativ}$$

$$x + (y + z) = (x + y) + z \text{ och } x(yz) = (xy)z \qquad \text{associativ}$$

$$x(y + z) = xy + xz \qquad \text{distributativ}$$

- "räkna som vanligt och ta resten modulo m närsomhelst".

Ex: $x = 234072$ delbart med 9?
$2+3+4+0+7+2 = 18 = 2\cdot 9$
Ja!

- De vanliga räknereglerna gäller i $\mathbb{Z}_m$:

$$x + y = y + x \text{ och } xy = yx \qquad \text{kommutativ}$$
$$x + (y + z) = (x + y) + z \text{ och } x(yz) = (xy)z \qquad \text{associativ}$$
$$x(y + z) = xy + xz \qquad \text{distributativ}$$

- "räkna som vanligt och ta resten modulo m närsomhelst".
- Exempel. Ett tal $x = r_n r_{n-1} \cdots r_0$ skrivet på decimalform är delbart med 3 (eller 9) omm $r_n + r_{n-1} + \cdots + r_1 + r_0$ är delbart med 3 (eller 9).

$10 \equiv_3 1$
"$10 = 1$ i $\mathbb{Z}_3$"
$10^k = 1^k = 1$
i $\mathbb{Z}_3$

$x = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + r_1 \cdot 10 + r_0$
$= r_n \cdot 1 + r_{n-1} \cdot 1 + \cdots + r_1 \cdot 1 + r_0$
$= r_n + r_{n-1} + \cdots + r_1 + r_0$ i $\mathbb{Z}_3$
(och i $\mathbb{Z}_9$)

$3 \mid x \iff 3 \mid (r_0 + r_1 + \cdots + r_n)$

▶ Exempel. Visa att talet $x = (104600120)_8$ är delbart med 56.

$56 = 7 \cdot 8$. Visa att $7 \mid x$ o $8 \mid x$

$8 \mid x$? Ja, ty sista siffran är noll.

$7 \mid x$? $x = 1 \cdot 8^8 + 4 \cdot 8^6 + 6 \cdot 8^5 + 1 \cdot 8^2 + 2 \cdot 8^1 + 0 \cdot 8^0$

$8 \equiv_7 1 \quad 8^k \equiv_7 1$

$\boxed{\begin{array}{l} 8 = 1 \cdot 7 + 1 \\ 8 \equiv_7 1 \end{array}}$

I $\mathbb{Z}_7$ har vi $x = 1 + 4 + 6 + 1 + 2 = 14 = 2 \cdot 7$

$= 0$ i $\mathbb{Z}_7$

dvs $7 \mid x$

$\therefore \quad 7 \mid x$ o $8 \mid x$, så $56 \mid x$.