Diskret matematik 2018-03-23 #3

Idag
- Aritmetikens fundamentalsats & hur många primtal?
- Modulär aritmetik

Def^n Kvot, rest
Sats (Division med kvot och rest/divisionsalgoritmen)

Def^n gcd
Sats Euklides algoritm: kan skriva $\gcd(a,b) = am + bn$

Sats Om $\gcd(a,b)=1$ & $a \mid bn$, då $a \mid n$
Följd Om p är ett primtal och $p \mid mn$ då $p \mid m$ eller $p \mid n$

Sats Alla tal ≥ 2 kan primfaktoriseras på ~~ett~~ unikt sätt

<u>Sats</u> (Primfaktoriseringens nyckellemma)

Låt p vara ett primtal. Om $p \mid mn$ gäller att $p \mid m$ eller $p \mid n$ (eller båda)

<u>Bevis</u> Om $p \mid m$ är vi klara. Annars, om $p \nmid m$, är $\gcd(p,m)=1$. Varför?
Därför, enl. "delbarhet hos prod" gäller $p \mid n$ ∎

p har endast p och 1 som positiva delare. Och $p \nmid m$.

<u>Sats</u> (Aritmetikens fundamentalsats)
Varje heltal större än 1 kan skrivas som en produkt av primtal på ett <u>och endast ett</u> sätt (bortsett från ordningen).

<u>Bevis</u> Att det finns ≥ 1 sätt vet vi från förra gången. Varför unikt.
Anta att $m \geq 2$ kan skrivas som

$m = p_1 p_2 \cdots p_k$
& $m = q_1 q_2 \cdots q_n$ där p_i och q_j är primtal

Detta innebär att $p_1 \mid q_1 \cdots q_n$
Enligt nyckellemmat gäller då att $p_1 \mid q_1$ eller $p_1 \mid q_2 \cdots q_n$
Återupprepar flera gånger för att se att

$p_1 \mid q_1$ eller $p_1 \mid q_2$ eller ... eller $p_1 \mid q_n$

Men eftersom varje q_j är ett primtal måste

$p_1 = q_j$ för något $j = 1, 2, \ldots, n$

Alltså är

$$p_2 \cdots p_k = \frac{m}{p_1} = \frac{m}{q_j} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_n$$

Enligt samma resonemang, med p_2 istället för p_1, så är $p_2 = q_i$ för något $i = 1, 2, \ldots, n$ $(i \neq j)$.

Till slut ser vi att alla p_x-faktorer kan matchas upp med en egen q_y-faktor (och vice versa).

Detta är precis det vi ville visa. ∎

2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Euklides ∞ många primtal

Euklides metod tar en ändlig lista primtal och visar att det finns ett annat primtal (utan att säga vad det är)

Säg att vår lista består av $p_1, p_2, \dots p_k$

Titta på talet

$m = p_1 p_2 \cdots p_k + 1.$

Enligt aritmetikens fundamentalsats har detta tal en primfaktorisering, så det är delbart med ett primtal. Detta primtal kan inte vara p_1, för när vi delar m med p_1 får vi resten 1.
Inte heller kan det vara p_2, för $\frac{m}{p_2}$ har rest 1. o.s.v.
Så inget av primtalen $p_1, \cdots p_k$ delar m.
Alltså måste vår primtalsfaktor till m vara ett annat primtal
$\Rightarrow$ det finns ett annat primtal. ∎

Def$^{\underline{n}}$ (Kongruens) Låt $d \neq 0$ vara ett heltal, och låt a, b vara heltal.
Vi skriver

$a \equiv b \pmod d$

och säger a är kongruent med b modulo d, om a och b skiljer sig med en multipel av d, dvs om $d \mid a-b$.

Ex

$24 \equiv 0 \pmod{24}$ $\quad$ $49 \equiv 1 \pmod{24}$
$48 \equiv 0 \pmod{24}$ $\quad$ $13 \equiv 1 \pmod 4$
$365 \equiv 1 \pmod 7$ $\quad$ $4 \equiv 14 \pmod{10}$
$35 \equiv 25 \pmod{10}$ $\quad$ $-2 \equiv 8 \pmod{10}$

Sats (Modulär addition, subtraktion, multiplikation)

Om $a \equiv b \pmod d$ och $m \equiv n \pmod d$ gäller

i) $a + m \equiv b + n \pmod d$
ii) $a - m \equiv b - n \pmod d$
iii) $a \cdot m \equiv b \cdot n \pmod d$

T.ex $\quad 11 \cdot 13 \equiv -1 \pmod{12}$
$11 \equiv -1 \pmod{12}$ $\quad$ $11 = 1 \cdot 12 - 1$
$13 \equiv 1 \pmod{12}$ $\quad$ $13 = 1 \cdot 12 + 1$

Bevis Vi har som antagande att $d \mid a-b$ och $d \mid m-n$

i) Vi vill visa att $d \mid a+m-(b+n)$.
Men $a+m-(b+n) = (a-b)+(m-n)$ och detta är en summa av multiplar av d, så den är en multipel av d.
ii) Liknande

iii) Vi vill visa att $am-bn$ är en multipel av d.:

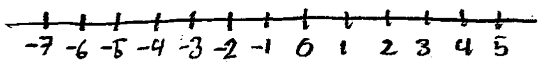
$am - bn = am - bm + bm - bn = m(a-b) + b(m-n)$

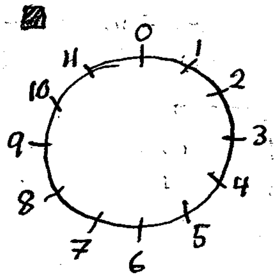
och

är multiplar av d, så hela uttrycket är det. ∎

Ex Eftersom $13 \equiv 3 \pmod{10}$
& $25 \equiv 5 \pmod{10}$
så gäller $13 \cdot 25 \equiv 3 \cdot 5 \pmod{10} \equiv 15 \pmod{10} \equiv 5 \pmod{10}$

- och $113 \cdot 395 \equiv 3 \cdot 5 \pmod{10} \equiv 5 \pmod{10}$
- Och modulo 17 har vi
  $16 \cdot 16 \equiv (-1)\cdot(-1) \equiv 1 \pmod{17}$. ∎





Heltalen modulo 12

Def^n Låt $n \geq 1$ vara ett heltal
Med $\mathbb{Z}_n$ menar vi heltalen modulo n där alla tal som är kongurenta mod n anses lika, och där vi har modulär addition & multiplikation. Vanligtvis använder vi talen $0, 1, 2, \ldots, (n-1)$ för att representera dessa, men även $-1, -2, \ldots, -(n-1)$.

Ex. (Additionstabell & multiplikationstabell)

$\mathbb{Z}_6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\mathbb{Z}_6$:

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Division & ekvationer

Vad menar vi med $\frac{3}{2}$?

Vi vill ha lösningen till $2x = 3$
och $\frac{1}{2}$ motsvarar att lösa $2x = 1$.

I $\mathbb{Z}_6$, kan vi lösa $2x = 3$?
Det finns ingen 3:a i rad 2 av multiplikationstabellen i $\mathbb{Z}_6$,
så det går inte att lösa i $\mathbb{Z}_6$

Sats Låt a, d vara heltal. Ekvationen $ax \equiv d \pmod{n}$ går att lösa omm $\gcd(a,n) \mid d$.

Bevis $ax \equiv d \pmod{n}$ motsvarar att $ax + ny = d$ för något y.