Föreläsning 8

Talteori
Primtal
Aritmetikens fundamentalsats
Största gemensamma delare
Minsta gemensamma multipel
Euklides algoritm

Om a och b är heltal, $a \neq 0$ säger vi att b delar a
$b \mid a$ om det finns ett heltal q så att $a = qb$. dvs $\frac{a}{b}$ är ett heltal.

Definition

Ett heltal $p > 1$ är ett *primtal* om de enda tal som delar p är $\pm p$ och ± 1. Ett heltal $n > 1$ som inte är ett primtal kallas för ett sammansatt tal.

Sats Om n är ett sammansatt tal så har n en delare $d \mid n$ så att $1 < d \leq \sqrt{n}$.

Om man skall kontrollera om ett tal n är primtal behöver man alltså bara kolla att inget d, $1 < d \leq \sqrt{n}$ delar n. Jfr Algoritm 5.1.8 i kursboken.

Bevis Antag att n är sammansatt. Låt d vara en delare till n så att $1 < d < n$. Vet att sån finns annars vore n ett primtal. Om $d \leq \sqrt{n}$ är vi klara. Annars utnyttjar vi att $n = qd$ där $q \in \mathbb{Z}$. Men då måste $q \leq \sqrt{n}$ för annars vore $n = qd > \sqrt{n}\sqrt{n} = n$. Motsägelse. $\square$

Aritmetikens fundamentalsats Varje heltal $n > 1$ kan skrivas som en produkt av primtal $n = p_1 \dots p_k$. Denna s.k. primtalsfaktorisering är unik, så när som på vilken ordning primtalen skrivs.

Om man t ex kräver att primtalen skall stå i icke-avtagande ordning, så får vi alltså en unik faktorisering.

Exempel:
$15 = 3 \cdot 5$
$33 = 3 \cdot 11$
$56 = 2 \cdot 2 \cdot 2 \cdot 7$

För att visa satsen ska vi använda oss av följande

Lemma Varje heltal $n \geq 2$ har åtminstone en delare som är ett primtal.

Bevis av Lemmat Låt $n \geq 2$ vara ett heltal. Vi vet att n har minst en delare som är > 1, nämligen n självt.

Låt p vara det minsta heltal så att $p \geq 2$ och $p \mid n$.

Visar att p är ett primtal.

Antag att p inte är ett primtal. Då är $p = km$, k, m heltal $1 < k < p$ och $1 < m < p$.

Men då är ju $n = pq = kmq$. Dvs $k \mid n$ och $1 < k < p$. Detta är en motsägelse! Alltså p är ett primtal, och minst ett primtal delar varje heltal $n > 1$ □

Bevis av aritmetikens fundamentalsats Visar först *existens* av en primtalsfaktorisering mha av stark induktion.

Grundsteg $n = 2$:

2 är ett primtal så det 'är sin egen primtalsfaktorisering'

Induktionssteg: Antag sant för $2 \leq k < n$ Visar sant för n.

Om n är ett primtal är vi klara.

Om n är sammansatt så vet vi enligt lemmat att n delas av minst ett primtal p_1. Då är $n = p_1 k$, med $2 < k < n$. Enligt induktionsantagandet har k en primtalsfaktorisering $k = p_2 \dots p_m$. Men då är $n = p_1 p_2 \dots p_m$ en primtalsfaktorisering av n.

Beviset av *entydighet* återkommer vi eventuellt till senare. □

Med hjälp av Lemmat ovan kan man också visa följande:

Sats Det finns oändligt många primtal.

Bevis Gör ett motsägelse bevis. Antag att det finns ett ändlligt antal primtal $p_1, \dots, p_m$. Låt $n = p_1 p_2 \dots p_m + 1$.

Enligt Lemmat måste n delas av något av primtalen $p_1, \dots, p_n$. Men det gör det inte eftersom

$$\frac{n}{p_k} = p_1 \dots p_{k-1} p_{k+1} \dots p_m + \frac{1}{p_k}$$

inte är ett heltal. □

Definition En *gemensam delare* till två heltal m och n är ett tal som delar både m och n.

m och n har alltid 1 som gemensam delare.

Den största (positiva) gemensamma delaren till m och n skriver vi
$\text{sgd}(m, n)$ – Största Gemensamma Delare.
i kursboken skriver man $\gcd(m, n)$ – Greatest Common Divisor.

Exempel: $m = 42$, $n = 70$
Delare till m: 1, 2, 3, 6, 7, 14, 21, 42
Delare till n: 1, 2, 5, 7, 10, 14, 35, 70
Gemensamma delare: 1, 2, 7, 14
$\text{sgd}(42, 70) = 14$

Definition En *gemensam multipel* till två heltal m och n är ett tal som delas av både m och n.

mn är alltid en gemensam multipel till m och n.

Den minsta (positiva) gemensamma multipeln till m och n skriver vi
$\text{mgm}(m, n)$ – Minsta Gemensamma Multipel
I kursboken används $\text{lcm}(m, n)$ – Least Common Multiple

Sats Antag att
$m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ och
$n = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$
där $p_1, \dots, p_k$ är primtal och $a_i = 0$ om p_i inte är en faktor av m oc $b_i = 0$ om p_i inte är en faktor av n.

Då är

$\text{sgd}(m,n) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_k^{\min(a_k,b_k)}$ och
$\text{mgm}(m,n) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_k^{\max(a_k,b_k)}$
Följdsats $\text{sgd}(m,n) \cdot \text{gcd}(m,n) = mn$

Exempel från ovan
$42 = 2 \cdot 3 \cdot 7 (= 2^1 3^1 5^0 7^1)$
$70 = 2 \cdot 5 \cdot 7 (= 2^1 3^0 5^1 7^1)$
$\text{sgd}(42,70) = 2 \cdot 7 = 14.$
$\text{mgm}(42,70) = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

Euklides algoritm Används till att bestämma sgd av två tal, på ett mycket snabbare sätt än att använda primtalsfaktoriseringen av talen. Den bygger på följande
Sats Om $r = a \mod b$ (dvs $a = qb + r$, $0 \leq r < b$) så är $\text{sgd}(a,b) = \text{sgd}(b,r)$

Bevis
Vi visar att a, b har samma gemensamma delare som b, r.
Antag att c delar a och b. Visar att c delar r.
c delar också bq, och alltså delar c även $r = a - bq$

På samma sätt Antag att c delar b och r Visar att c delar a.
c delar också bq och alltså även $a = bq + r$.

Rekommenderade uppgifter:
§5.1: 12, 15, 18, 21, 24, 25, 28, 31
§5.3: 1-4, 6, 11 (för dessa), 15, 16, 23, 32-38
§5.4: 7-16