LEKTION 03-05

Vi börjar med lite terminologi om heltal.

Definition 0.1. Låt a, b vara två heltal. Man säger att b *delar* a eller att b är en *delare* till a om det finns ett heltal n sådan att

$$a = nb$$

Man skriver $b|a$ när b delar a och $b \not| a$ när så inte är fallet. Exempelvis $4|16$, $3 \not| 8$.
Exempel:

- $\pm a|a$ och $\pm 1|a$ för varje $a \in \mathbb{Z}$. Man säger att b är en äkta delare till a om $b|a$ och $b \neq \pm a, \pm 1$.
- $b|0$ för varje heltal b, eftersom $0 = 0b$; Om $0|a$ så gäller $a = 0$.
- visa att om $a|b$ och $b|a$ då $a = \pm b$.
  Om $a = 0$ är också $b = 0$ så vi kan anta att $a \neq 0$. Eftersom $a|b$ och $b|a$ så är $b = na$ och $a = mb$. Detta ger att $a = mna$ och därmed $mn = 1$. Eftersom $m, n \in \mathbb{Z}$ så har vi att $m = n = 1$ eller $m = n = -1$.
- Visa att $a|b$ och $b|c$ ger $a|c$.
  Eftersom $b = na$ och $c = mb$ har vi att $c = mna$ och $mn \in \mathbb{Z}$. Alltså är a en delare till c.

Övning.

(1) Visa att om $c|a$ och $c|b$ då gäller $c|xa + yb$ för alla heltal x och y.
(2) Visa att om $b|a$ och $a > 0$ då är $b \leq a$.

Definition 0.2. Ett heltal $p > 1$ kallas att *primtal* om det saknar äkta delare.

Man ska tänka på primtalen som "byggstenar" för heltalen, på grund av:

Aritmetikens fundamentalsats(AFS). Varje heltal $n > 1$ kan skrivas som en produkt av primtal:

$$n = p_1 p_1 ... p_k$$

Den kallas en *primfaktorisering*.

BEVIS. Om n är ett primtal då är primfaktorisering $n = n$. Antar att n inte är ett primtal och låt b vara en äkta delare till n. Det betyder att $n = bm$ där $m \in \mathbb{Z}$. Om b eller m , säg b, är ett primtal, sätt $b = p_1$ och fortsätt på samma sätt med m. Efter ett ändligt antal steg får man en primfaktorisering av n.

Exempel Talet 16170 primfaktoriseras som

$$1610 = 3 \cdot 5 \cdot 7^2 \cdot 11$$

NOTERA att primfaktoriseringen är inte entydig. Den blir så om man bortser från ordningen mellan faktorer!

Nu kan vi visa en mycket viktig sats:

EUKLIDES SATS. Det finns oänligt många primtal.

BEVIS Antag motsatsen, dvs antag att det finns k stycker primtal: $p_1, p_2, ..., p_k$. Bilda talet:

$$n = p_1 p_2 ... p_k + 1$$

Enligt (AFS) är n en produkt att primtal $q_1, ..., q_j$ så vihar att:

$$n = q_1 q_2 ... q_j = p_1 p_2 ... p_k + 1$$

Eftersom $q_1 | n$ och $q_1, p_1, ..., p_k$ är alla primtal så måsta $q_1 | 1$. Detta innebär en motsägelse eftersom $q_1 > 1$.

En mycket viktig egenskap hos de positiva tal är den så kallade *välordningsprincipen* som säger att:

Varje icke-tom delmängd av $\mathbb{Z}^+$ har ett minsta element.

Det betyder att det finns ett element som är mindre än alla andra element i mängden. Vi ska visa det lite senare!

Vi behöver välordningsprincipen för att visa den så kallade *divisionsalgoritmen*:

EUKLIDESALGORITEN. Låt a, b vara heltal och $b > 0$. Då finns entyga heltal q, r sådan att:

$$a = bq + r \qquad\qquad 0 \leq r < b$$

BEVIS. Satsen är trivial om $a = 0$, så antag att $a > 0$. Betrakta mängden:

$$S = \{a - bt \text{ där } t \in \mathbb{Z}, a - tb \geq 0\}$$

S är en icke-tom ($a \in S$) delmängd av $\mathbb{Z}^+$ och enligt välordningsprincipen har S ett minsta element $r = a - bq$. Då är $a = bq + r$ och $0 \leq r < b$. Nu ska vi visa att q, r är entydiga. Antag att det finns Q, R sådan att $a = bQ + R$, med $0 \leq R < b$. Då är

$$a = bq + r = bQ + R \qquad \text{och därmed}$$

$$(q - Q)b = R - r$$

Eftersom $R - r < b$ så måste $q - Q = 0$ och därmed $R - r = 0$.

Exempel. Om 125 divideras med 12 har vi att:

$$125 = 12 \cdot 10 + 5$$

TALBASEN

Om man skriver ett tal som 12345 så är det förstått att talet är givet i *talbasen* **10**, dvs

$$12345 = 1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0$$

Inom datorområdet använder man ofta det *binära talsystemet*, där ett tal skrivas som en sekvens av "0" och "1", dvs

$$77 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 10011010$$

Man kan konvertera ett tal från basen 10 till basen 2 med hjälp av Euklidens algoritmen:

$$\begin{array}{rcll} 77 & = & 2 \cdot 38 & + \ 1 \\ 38 & = & 2 \cdot 19 & + \ 0 \\ 19 & = & 2 \cdot 9 & + \ 1 \\ 9 & = & 2 \cdot 4 & + \ 1 \\ 4 & = & 2 \cdot 2 & + \ 0 \\ 2 & = & 2 \cdot 1 & + \ 0 \\ 1 & = & 2 \cdot 0 & + \ 1 \end{array}$$

Så vi har:

$$77 = 2(2 \cdot (2 \cdot 9 + 1)) + 1 = 2(2(2(2 \cdot 4 + 1))) + 2^2 + 1 = 2^6 + 2^3 + 2^2 + 2^0$$

På samma sätt konverterar man ett tal från basen 10 till en annan bas. Till exempel kan talet 777 skrivas "i basen 8" som (en sekvens av tal mellan 0 och 7):

$$\begin{array}{rcll} 777 & = & 8 \cdot 97 & + \ 1 \\ 97 & = & 8 \cdot 12 & + \ 1 \\ 12 & = & 8 \cdot 1 & + \ 4 \\ 1 & = & 8 \cdot 0 & + \ 1 \end{array}$$

Så vi har $777 = 8(8(8 + 4) + 1) + 1 = 8^3 + 4 \cdot 8^2 + 8 + 8^0 = 1411$.

STÖRSTA GEMENSAM DELARE

Naturigtvis kan två heltal a, b ha gemensamma delare. Eftersom bara ett änligt antal delare är möijlgt så det måste finnas en största delare.

Definition 0.3. Låt a, b vara heltal, inte båda noll. Det positiva talet d kallas *den största gemensamma delaren*(sgd) till a och b om:

(1) $d|a$ och $d|b$;
(2) om $c|a$ och $c|b$ då $c|d$.

Den $sgd(a, b)$ brukar betecknas också (a, b).
Man säger att a, b är relativt prima om $sgd(a, b) = 1$.
Det kan vara komplicerat att hitta sgd av två störa tal, men det finns ett systematiskt sätt att hitta sgd tackvare Euklides algoritm.

Exampel Bestäm $sgd(252, 111)$.

$$\begin{array}{lcll} 252 & = & 111 \cdot 2 & + \ 30 \\ 111 & = & 30 \cdot 3 & + \ 21 \\ 30 & = & 21 \cdot 1 & + \ 9 \\ 21 & = & 9 \cdot 2 & + \ \mathbf{3} \\ 9 & = & 3 \cdot 3 & \end{array}$$

Så sgd är den icke-försvinnande resten: $sgd(252, 111) = 3$

Notera att på grund av övning (2), om $d|252$ och $d|111$ då $d|252 - 2 \cdot 111 = 30$, då $d|111 - 3 \cdot 3 = 21$, $d|30 - 21 = 9$ och $d|3$. Det följer att $sgd(252, 111) = 3$.

Notera dessutom att man kan följa algoritm från slutet till början och få $3 = 21 - 2(30 - 21) = 3 \cdot 21 - 2 \cdot 30 = 3(111 - 3 \cdot 30) - 2 \cdot 30 = 3 \cdot 111 - 11 \cdot (252 - 2 \cdot 111) = 25 \cdot 111 - 11 \cdot 252$ så att

$$3 = 25 \cdot 111 - 11 \cdot 252$$

Man kan på samma sätt visa att:

SATS. Om $d = (a, b)$ så finns två heltal N och M så att:

$$d = Na + Mb$$

DIOFANTISKA EKNATIONER

Alla ni vet att när man löser en bråkaddition och vill skriva svaret som ett bråk, behöver man räkna ut den *minsta gemensamma multipel* mellan nämnarna. Ofta kallas det *lcd* från det engelska ordet "list common divisor". Man Kan beräkna $lcm(a, b)$ med hjälp av primtal faktoriseringen. Om $a = p_1 \cdot ... \cdot p_r$ och $b = q_1 \cdot ... \cdot q_l$ är $lcd(a, b)$ "unionen" av den. Till exmpel:
$60 = 2 \cdot 2 \cdot 3 \cdot 5$, $36 = 2 \cdot 2 \cdot 3 \cdot 3$ så är $lcm(60, 36) = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 180$

Övning. Visa att:

$$lcm(a, b) = \frac{ab}{sgd(a, b)}$$

Exempel. Bestämm $lcd(4711, 777)$.

Med hjälp av Euklides algoritm hittar man att $(4711, 777) = 7$. Eftersom är

$$4711 \cdot 777 = lcd(4711, 777) \cdot sgd(4711, 777)$$

har vi att $lcd(4711, 777) = 522921$.

Vi har sett att man kan skriva $sgd(n, m)$ som en linjära kombination av n och m : $sgd(n, m) = an + bm$, där $m, n \in \mathbb{Z}$. Till exempel är

$$7 = 16 \cdot 4711 - 97 \cdot 777$$

Finns den ett entydigt sätt att göra så? Eftersom $4711 \cdot 111 = 673 \cdot 777$ ser man att

$$7 = 16 \cdot 4711 - 97 \cdot 777 + k(4711 \cdot 111 - 673 \cdot 777) = (16 + 111k) \cdot 4711 - (97 + 673k) \cdot 777$$

Så det finns oändligt många sätt(ett för varje k).

Låt $a, b, c \in \mathbb{Z}$ och x, y vara obekanta heltal.
Betrackta den *diofantiska ekvationen*:

$$ax + by = c$$

Antag att ekvationen är lösbar och låt $d = sgd(a, b)$. Det följer att $d|ax+by$ och därmed att $d|c$. Antag omvänt att $d|c$ så att $c = dm$ för något heltal m. Eftersom $d = sgd(a, b)$ finns det $M, N \in \mathbb{Z}$ sådan att $d = Na+bM$. Då är $x = M$ och $y = N$ en lösning till ekvationen $d = xa + by$ och $x = mM$, $y = mN$ är en lösning till ekvationen $c = md = xa + by$. Vi har visat att:

SATS. Ekvationen $ax + by = c$ är lösbar om och endast om $(a, b)|c$.

Detta ger en algoritm för att lösa ekvationen $ax + by = c$:

- bestäm $d = (a, b)$
- om $c \not| (a, b)$ då är ekvationen ej-lösbar;
- om $c = md$ låt $h = lcm(a, b)$ där $h = Aa = Bb$. Hitta heltal N, M sådan att $d = Na + Mb$. Den allmänna lösning är $x = mN + kA, y = mM - kB$.

Exempel Vid en idrottstävling kostade biljetter 175 SEK för vuxna och 145 för barn. De totala intäkterna var 10000 kronor. Hur många barn köpte biljett?

Antag att det kom x barn och y vuxna, dvs: $175y+145x = 10000$. Här är $sgd(145, 175) = 5$ och $5|10000$. Observera att man kan dela hela ekvationen med 5:

$$29x + 35y = 2000 \qquad \text{då är } (29, 35) = 1$$

På grund av Euklides algoritm har vi:

$$\begin{array}{rcl} 35 & = & 29 \cdot 1 + 6 \\ 29 & = & 4 \cdot 6 + 5 \\ 6 & = & 5 \cdot 1 + 1 \end{array}$$

och $1 = 6 - 5 = 6 - 29 + 4 \cdot 6 = 5 \cdot 6 - 29 = 5(35 - 29) - 29 = 5 \cdot 35 - 6 \cdot 29$. Eftersom $x = -6, y = 5$ är en lösning till $29x + 35y = 1$ så är $x = -12000, y = 10000$ en lösning till $29x + 35y = 2000$. Eftersom $lcm(29, 35) = 29 \cdot 35$ blir den almänna lösningen:

$$x = -12000 + 35k \qquad y = 10000 - 29k$$

Klart att vi ska kräva att $x = -12000 + 35k \geq 0$ och $y = 10000 - 29k \geq 0$. Det följer att $343 \leq k \leq 344$. Svaret ër:

- $-1200 + 35 \cdot 343 = 5$ barn eller
- $-1200 + 35 \cdot 344 = 40$ barn.