Algebraiska strukturer, 30 januari

Låt a och b vara heltal. Med **största gemensamma delaren** till a och b ($a \neq 0$ eller $b \neq 0$) menar man ett positivt heltal d så att

1) $d|a$ och $d|b$;

2) d är delbart med varje gemensam delare till a och b.

Betecknas $SGD(a,b)$ eller (a,b). $SGD(0,0) = 0$.

$SGD(a,b)$ är definierad entydigt, ty om både d och d' uppfyller villkoren ovan så gäller $d|d'$ och $d'|d$ vilket innebär att $d = \pm d'$.

Om $SGD(a,b) = 1$ så säger man att a och b är **relativt prima**.

$SGD(a,b)$ kan beräknas med hjälp av **Euklides algoritm**: Man bildar en divisionkedja

$$
\begin{aligned}
&a = bq_1 + r_1, \quad 0 \leq r_1 < |b|,\\
&b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1,\\
&r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2,\\
&\ldots\\
&r_{n-2} = r_{n-1} q_n + r_n, \quad 0 \leq r_n < r_{n-1},\\
&r_{n-1} = r_n q_{n+1}.
\end{aligned}
$$

Vi påstår att $r_n = SGD(a,b)$. $r_n|a$ och $r_n|b$, ty från likheterna följer att $r_n|r_{n-1} \Rightarrow r_n|r_{n-2} \Rightarrow \ldots r_n|b \Rightarrow r_n|a$.

Om g nu är en godtycklig gemensam delare till a och b så visar den första likheten att $g|r_1$. Alltså ger den andra att $g|r_2$, osv, $g|r_n$. Detta visar påståendet.

Proposition. För varje par av heltal a och b finns det två heltal m och n sådana att $SGD(a,b) = am + bn$.

m och n kan beräknas med hjälp av Euklides algoritm.

Med **minsta gemensamma multipeln** till a och b menar man ett positivt heltal m som är delbart med a och b och som delar varje gemensam multipeln av a och b. Minsta gemensamma multipeln av a och b definieras entydigt av dessa tal (varför?). Betecknas $MGM(a,b)$.

Man säger att ett positivt heltal p är ett **primtal** om p har exakt två olika positiva delare: 1 och p.

Aritmetikens fundamentalsats. Varje heltal $n > 1$ är en entydig produkt av primtal dvs om

$$n = p_1 p_2 \ldots p_m = p'_1 p'_2 \ldots p'_n,$$

där p_i och p'_j är primtal så är $m = n$ och vid lämplig numrering av faktorerna är $p_i = p'_i$.

Lemma 1. Låt p vara ett primtal, $a, b \in \mathbb{Z}$. Om $p|ab$ så gäller $p|a$ eller $p|b$.

Bevis av Lemma 1. Antag att $p \not| a$. Då är $SGD(p,a) = 1$ och det finns m, $n \in \mathbb{Z}$ så att $1 = pm + an$. Detta ger $b = pbm + abn$. Eftersom $p|pbm$ och $p|abn$, får vi $p|b$.

Lemma 2. Låt p vara ett primtal $a_1, \ldots, a_k \in \mathbb{Z}$. Om $p|a_1 \ldots a_k$ så gäller $p|a_i$ för något i.

Bevis av Lemma 2. Vi visar påståendet med induktion med avseende på antalet faktorer k i produkten. Fallet $k = 1$ är klart. Låt $k > 1$ och antag att $p|a_1 \dots a_{k-1}$ medför $p|a_i$ för något $i \in \{1, \dots, k-1\}$. Låt $p|a_1 \dots a_k$. Enligt Lemma 1, $p|a_k$ eller $p|a_1 \dots a_{k-1}$. Om $p|a_k$ så] är vi klara. I annat fall ger induktionsantagandet att $p|a_i$ för något $i \in \{1, \dots, k-1\}$. Beviset är klart.

Bevis av satsen. Först visar vi med induktion att varje heltal $n > 1$ är en produkt av primtal. $n = 2$ är klart. Låt $n > 2$ och antag att varje heltal k, $1 < k < n$, är en produkt av primtal. Låt p vara minsta äkta delaren till n ($p \neq 1$). Då är p ett primtal, ty annars har p en äkta delare som är automatiskt en delare till n. Vi har $n = pq$, där $1 \leq q < n$. Enligt antagandet är q en produkt av primtal vilket visar att n är en sådan produkt.

Entydigheten. Låt

$$p_1 p_2 \dots p_m = p'_1 p'_2 \dots p'_n, \tag{1}$$

där p_i och p'_j är primtal. Primtalet p_1 delar $p_1 \dots p_m$. Detta ger $p_1 | p'_1 p'_2 \dots p'_n$. Enligt Lemma 2 $p_1 | p'_k$ för något k och därmed $p_1 = p'_k$. Vi eliminerar p_1 från vänster och p'_k från höger i likheten (1) och får

$$p_2 \dots p_m = p'_1 \dots p'_{k-1} p'_{k+1} \dots p'_n.$$

Vi upprepar samma argumenter och får $m = n$, varje p_i är lika med något p'_j, ty vi inte kan ha alla primtal borttagna på en av sidorna och ha några kvar på den andra.