Mårten Wadenbäck

# Fortsättning om primtal

Definition: Ett heltal $a>1$ sägs vara ett primtal om de enda delarna till $a$ är $\pm 1$ och $\pm a$. Om $a>1$ inte är ett primtal är $a$ ett sammansatt tal.

Notera att om $a$ är ett primtal och $a \nmid b$ så är $\operatorname{sgd}(a,b)=1$.

Sats: Om $a$ och $b$ är heltal med $\operatorname{sgd}(a,b)=1$ och $c$ är ett heltal så gäller det att

$$a \mid bc \Rightarrow a \mid c.$$

Bevis: Enligt Bezouts identitet finns det heltal $u$ och $v$ sådana att $au+bv=1$, så $acu+bcv=c$. Eftersom $a \mid bc$ delar $a$ vänsterledet, och därför måste $a \mid c$.

Följdsats: Om $p$ är ett primtal och $a,b \in \mathbb{Z}$ så gäller det att $p \mid ab \Leftrightarrow p \mid a \vee p \mid b$.

Sats: Om $p$ är ett primtal och $a_1, \dots, a_n$ är heltal sådana att $p \mid a_1 a_2 \cdots a_n$ så gäller det att $p \mid a_k$ för minst ett $k \in \{1, 2, \dots, n\}$.

Bevis: Om $n = 2$ är vi redan klara (följdsatsen ovan).

Antag att satsen gäller för $n = r$, och betrakta fallet $n = r+1$. Om $p \mid a_1 \cdots a_r a_{r+1}$ så gäller det att $p \mid a_1 \cdots a_r \vee p \mid a_{r+1}$. Om $p \mid a_1 \cdots a_r$ gäller enligt induktionsantagandet att $p \mid a_k$ för något $k \in \{1, 2, \dots, r\}$. Alltså gäller det att $p \mid a_k$ för något $k \in \{1, 2, \dots, r, r+1\}$, och satsen följer nu genom induktion.

Följdsats: Om $p$ och $q_1, q_2, \dots, q_n$ alla är primtal och $p \mid q_1 \cdots q_n$ så gäller att $p$ är lika med något av talen $q_1, q_2, \dots, q_n$.

Bevis: Vi vet att $p \mid q_k$ för något $k \in \{1, \dots, n\}$, men enda talen som delar $q_k$ är $\pm q_k$ och $\pm 1$.

Sats (Aritmetikens fundamentalsats): Varje heltal $a > 1$ kan skrivas som en produkt av primtal. Bortsett från ordningen bland faktorerna kan detta endast göras på ett sätt.

Bevis: Vi börjar med att visa existensen av primtalsfaktoriseringen med hjälp av induktion. Talet 2 är ett primtal, så vi har ett basfall. Anlag nu att varje tal upp till och med $a$ har en primtalsfaktorisering. Nästa tal, $a+1$, är antingen ett primtal (då är vi klara) eller ett sammansatt tal. Om $a+1$ är sammansatt är det produkten av två tal $b$ och $c$, som båda är större än ett och mindre än $a+1$, och alltså har primtalsfaktoriseringar. Detta ger en primtalsfaktorisering av $a+1 = bc$, och induktion ger att alla heltal $a > 1$ har en primtalsfaktorisering.

För att bevisa entydigheten, antag motsatsen, dvs att $a = p_1 \cdots p_m = q_1 \cdots q_n$ är två olika primtalsfaktoriseringar. Vi kan utan vidare antaga att $m \leq n$ och att primfaktorerna står i växande storleksordning. Det minsta av $p_1$ och $q_1$ delar ju $a$. Om $p_1 \leq q_1$ måste $p_1 = q_1$, eftersom $p_1 | q_1 \cdots q_n$, och om $q_1 \leq p_1$ måste $q_1 = p_1$ då $q_1 | p_1 \cdots p_m$. Detta leder till att $p_2 \cdots p_m = q_2 \cdots q_n$, och vi kan upprepa samma argument för $q_2$. På detta sätt får vi att $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_m = q_m$, och $1 = q_{m+1} \cdots q_n$. Då måste $q_{m+1}, \ldots, q_n$ alla vara lika med 1, och är inte primtal. Alltså är $m = n$.

Exempel: Primtalsfaktoriseringen av 511 är $511 = 7 \cdot 73$, och primtalsfaktoriseringen av 824 är $824 = 2 \cdot 2 \cdot 2 \cdot 103$.

Anmärkning: Att hitta primtalsfaktoriseringen till ett givet tal $n$ anses vara ett "svårt" problem, och för riktigt stora tal finns ingen känd metod som inte tar orimligt lång tid.

# Diofantiska ekvationer

En diofantisk ekvation är en ekvation till vilken vi söker heltalslösningar.

Exempel: Fermats ekvation $x^n+y^n=z^n$, där $n\in\mathbb{N}$ är ett givet tal, är en diofantisk ekvation i $x$, $y$, och $z$. Om $n=1$ eller $n=2$ finns det oändligt många lösningar, men om $n>2$ finns det inga lösningar utom när något av talen är noll.

Vi skall titta närmre på ekvationer av typen

$ax+by=c$, där $a,b,c\in\mathbb{Z}$ är givna.

Exempel: Antag att blyertspennor kostar 6 kr/st och suddgummin kostar 7 kr/st. En person som köpte blyertspennor och suddgummin betalade 32 kr. Hur många pennor respektive suddgummin kan vederbörande ha köpt? Vi kan enkelt testa alla möjligheter, och ser att enda möjligheten är tre pennor och två suddgummin.

Om personen tidigare hade köpt pennor och suddgummin på öppet köp, och kunde lämna till baka saker, då hade även $-4$ pennor och 8 suddgummin varit en möjlighet. Finns det fler?

Sats: Den diofantiska ekvationen $ax+by=c$ är lösbar om och endast om $sgd(a,b) \mid c$.

Bevis: Om $d=sgd(a,b)$ gäller att $d \mid ax+by$ för alla heltal $x$ och $y$, så då gäller att $d \mid c$. Om $sgd(a,b) \mid c$ kan vi dela båda sidor med $sgd(a,b)$ och få $a'x+b'y=c'$, där $sgd(a',b')=1$. Enligt Bezouts identitet finns det heltal $u$ och $v$ sådana att $a'u+b'v=1$, så $a'(uc')+b'(vc')=c'$.

Ur beviset får vi en metod för att hitta en lösning. Vi kan bestämma $u$ och $v$ med "bakländesversionen" av Euklides algoritm, och sedan sätta $x=uc$ och $y=vc$.

Finns det fler lösningar? Ja, för varje heltal $n$ fungerar även $x = uc - bn$ och $y = vc + an$, eftersom

$$ax + by = a(uc - bn) + b(vc + an) = auc - abn + bvc + abn =$$

$$= (au + bv)c = c.$$

Finns det ännu fler lösningar? Nej, för om $(x, y)$ och $(x', y')$ är lösningar så är

$$ax + by = c \quad \text{och} \quad ax' + by' = c,$$

så $\quad ax + by - ax' - by' = c - c = 0 \iff a(x - x') + b(y - y') = 0 \iff$

$a(x - x') = b(y' - y)$. Men detta betyder att $b \mid a(x - x')$, och då $\text{sgd}(a, b) = 1$ gäller det att $b \mid x - x'$, dvs $x - x' = nb \iff x' = x - nb$, och på samma sätt får vi $y' = y + na$.