PRIMTAL

Ett primtal är ett heltal som är större än 1 och som ej kan skrivas som en produkt av två eller flera mindre heltal, d.v.s. talet saknar äkta delare. T.ex. är $3, 5, 7, 11, 13$ primtal, medan 4 eller 12 inte är primtal (eftersom $4 = 2 \cdot 2$ och $12 = 2 \cdot 2 \cdot 3$). Alla positiva heltal som inte är primtal går att dela upp i primtalsfaktorer.

Exempel: $100 = 2 \cdot 50 = 2 \cdot 2 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5$, där 2 och 5 är primtalsfaktorer.

Det finns oändligt många primtal. Det första beviset gavs av Euklides för 2300 år sen. Kort förklaring av beviset:

1. Enligt Aritmetikens fundamentalsats gäller att alla tal kan delas upp i primtalsfaktorer, utom primtalen. (Måste bevisas för sig)
2. Vi antar att det finns ändligt många primtal och därmed ett största. Vi kallar detta för n.
3. I så fall, om vi multiplicerar alla kända primtal ($2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot \ldots \cdot n$) och sedan adderar 1 får vi ett tal, p.
4. p är nu inte delbart med något primtal:

    a) det är inte delbart med 2 (om vi delar med 2 får vi resten 1)
    b) ej heller med 3 (samma resonemang som för 2 ovan)
    c) ej heller med något av de andra primtalen (samma resonemang)
    d) alltså är inte p delbart med något tal

5. alltså är p självt ett primtal
6. p är större än n och därmed är vårt antagande, att n är det största primtalet, felaktigt.
7. Motsägelsen implicerar att det finns oändligt många primtal.

Aritmetikens fundamentalsats säger att varje positivt heltal kan skrivas i form av en produkt av primtal på ett (och endast ett sätt), om man ej tar hänsyn till primfaktorernas ordning. T.ex. är $12 = 2 \cdot 2 \cdot 3$, då man har tre primfaktorer. Primfaktorernas antal kan också vara ett, när talet självt är ett primtal såsom 5, och t.o.m. noll, när talet är 1 varvid det är frågan om den s.k. tomma produkten.

Bevis av satsen:

1. Lemma 1

Om heltalet *a* är större än eller lika med 2och om *a* inte är ett primtal, så är den minsta positiva äkta delaren till *a* ett primtal.

Bevis av Lemma 1:

Om a inte är ett primtal så måste det (enligt definitionen av primtal) ha *någon* positiv äkta delare och något måste vara minst.
Vi kallar det tal för *p*.

Eftersom *p* delar *a* så gäller $a = p \cdot c$, där *c* är ett heltal, och framförallt $1 < \mathrm{p} < \mathrm{a}$.
Om *p* inte är ett primtal så måste *p* självt ha *någon* positiv äkta delare. Låt oss kalla denna delare för *d* och precis som ovan måste $p = d \cdot e$, där *e* är ett heltal. Även här gäller att $1 < \mathrm{d} < \mathrm{p}$. Men då är ju $a = p \cdot c = d \cdot e \cdot c$. Det betyder att *d* delar *a* och vidare vet vi att $1 < \mathrm{d} < \mathrm{p}$.

Att *d* är positiv äkta delare till *a* och dessutom mindre än *p* är en motsägelse eftersom vi antagit att *p* är den minsta äkta delaren till *a*.

Alltså måste *p* (den minsta positiva delaren till *a*) vara ett primtal.

2. Lemma 2

Varje heltal större än eller lika med 2 kan skrivas som en produkt av primtal.

Bevis av Lemma 2

Låt a vara ett heltal större än eller lika med 2.

Om a är ett primtal så håller *Lemma 2*. (a:s primtalsfaktorer är a, som 5 ovan.) Annars så har *a* en äkta delare som är ett primtal. (Enligt *Lemma 1*.) Detta primtal kallar vi p_1. Då gäller att $a = p_1 \cdot a_1$.

Om a_1 är ett primtal så håller *Lemma 2*. (Då har vi delat in *a* i dess primtalsfaktorer p_1 och a_1.) Annars måste *a1*, enligt *Lemma 1* ha en äkta delare som är ett primtal. Detta tal kallas för p_2. Då är $a_1 = p_2 \cdot a_2$, så att $a = p_1 \cdot p_2 \cdot a_2$.

Är nu a_2 ett primtal så håller *Lemma 2*. Om inte upprepas proceduren och eftersom $a > a1 > a2 > \ldots > 2$ så måste något $a[k]$ vara ett primtal. Därmed är *a* uppdelat i sina primtalsfaktorer.

Enligt *Lemma 2* så *kan* varje positivt heltal större än eller lika med 2 delas in i primtalsfaktorer. Nu ska det bevisas att det bara finns en uppdelning (bortsett ordning). Anta att det finns två *olika* primtalsfaktoriseringar. Vi kan skriva dem som:
$a = p_1 \cdot p_2 \cdot \ldots \cdot p[i] = q_1 \cdot q_2 \cdot \ldots \cdot q[j]$

Vi vet att p_1 delar *a* och då måste p_1 dela $q_1 \cdot q_2 \cdot \ldots \cdot q[j]$. Men då måste$p_1$ dela $q[k]$ för något k, men då $q[k]$ är ett primtal måste p_1 vara lika med $q[k]$. Vi kan då dela båda led med p_1. Proceduren kan upprepas tills vi kommer till ett av tre fall.

- $1 = 1$, Satsen bevisad. Alla *p[l]* är lika med något *q[k]*.
- $1 = q[a] \cdot q[b] \cdot \ldots \cdot q[n]$. Men eftersom samtliga *q* är primtal är de större än eller lika med två och detta fall blir en omöjlighet.
- $p[a] \cdot p[b] \cdot \ldots \cdot p[n] = 1$. Som fall 2.

Alltså kommer vi till fall ett och satsen gäller, det finns bara en primtalsfaktorisering.