lcm en gcd

stelling van Bézout

Als a en b gehele getaleln zijn die niet beide nul zijn en dat d =gcd(a,b). dan bestaan er gehele getallen m en n zodanig dat am+bn=d

gevolgen stelling bézout

als voor drie gehele getallen a,b,c met (b,c)≠(0,0) geldt dat c|ab en dat gcd(b,c)=1, dan is c|a

bewijs
uit gcd(b,c)=1 volgt dat er m,n ∈ Z bestaan zodat mb+nc=1; hieruit volgt dat mab +nac=a. Aangezien c|ab per veronderstelling, is ook c |mab , en uiteraard ook c|nac, zodat c|mab+nac en bijgevolg c|a

---

indien p een priemgetal is en indien x_1, x_2, ... ,x_n gehele getallen zijn zodanig dat p een deler is van hun product,
p | x_1 x_2 ... x_n
dan is p een deler van ten minste één x_i (i ∈ N[1,n])

bewijs
Indien p | ab met a,b ∈ Z, dan p|a of p|b het algemene resultaat volgt dan per inductie op n.
Stel dus dat p | ab, en veronderstel dat p ∤ b; we moeten bewijzen dat dan p|a. Merk op dat p ∤ b impliceert dat gcd(b, p)=1. We kunnen dus de vorige stelling toepassen met c=p, en we besluiten dat p | a.

De ontbinding van een natuurlijk getal n>= 2 in priemfactoren is uniek op de volgorde van de factoren na

bewijs
we gebruiken het principe van het kleinste tegenvoorbeeld. veronderstel dus dat er een kleinste natuurlijke getal >=2 bestaat waarvoor dit niet waar is, daarom is

$$n_0 = \prod_{i=1}^{k} p_i = \prod_{j=1}^{\ell} p'_j,$$

waarbij p_i (i ∈ N[1,k]), evenals p'_j (j ∈ N[2,l]) (niet noodzakelijk onderling verschillende) priemgetallen zijn. Hieruit volgt dat

$$p_1 \mid \prod_{j=1}^{\ell} p'_j$$

en dus wegens voorgaande stelling dat p_1 ten minste één van de getallen p'_j deelt.
Zonder de algemeenheid te schaden, mogen we veronderstellen dat $p_1 \mid p'_1$,
Aangezien beide getallen echter priemgetallen zijn, volgt hieruit dat $p_1 = p'_1$

$$\frac{n_0}{p_1} = n_1 = \prod_{i=2}^{k} p_i = \prod_{j=2}^{\ell} p'_j.$$

dit is echter in strijd met de veronderstelling dat n_0 het kleinste getal is dat 2 verschillende ontbindingen in priemfactoren bezit. bijgevolg bestaat n_0 niet en mogen we besluiten dat de stelling bewezen is voor elke n>=2