

'n Faktoriseringsmetode gegrond op 'n additiewe eienskap

B. de la Rosa*, H. du T. Mouton, A. van der Westhuizen, D. van Deventer en J.P.H. Wessels
Departement Wiskunde, Universiteit van die Oranje-Vrystaat, Posbus 339, Bloemfontein 9300

Onvang 2 Augustus 1991; aanvaar 22 April 1992

UITTREKSEL.

Die doel van hierdie artikel is om 'n faktoriseringsmetode te ontwikkel deur van 'n additiewe eienskap van die positiewe heelgetalle gebruik te maak. Aan die hand van bekende resultate word beklemtoon dat die saamgestelde, onewe positiewe heelgetalle presies daardie onewe getalle is wat as somme van drie of meer opeenvolgende, positiewe heelgetalle voorgestel kan word. Die direk geïmpliseerde algoritmebasis word in hierdie artikel verfyn tot op 'n gewenste peil van optimaliteit. Die resultaat is 'n additief-multiplikatiewe basis vir 'n algoritme wat gedeeltelik op die genoemde additiewe eienskap en gedeeltelik op langdeling (of alternatiewelik die ggd) berus.

ABSTRACT

A factorisation method based on an additive property

The purpose of this article is to develop a method of factorisation based on an additive property of the positive integers. Using known results it is emphasised that the composite odd positive integers are precisely those odd numbers that can be represented as sums of three or more consecutive positive integers. The obviously implied algorithm basis is refined in this paper up to a desired level of optimality. The result is an additive-multiplicative basis for an algorithm that is based partly on the said additive property and partly on long division (or alternatively the gcd).

1. Inleiding

Faktoriseringsmetodes vorm 'n vrugbare bron vir teoretiese besinning sowel as praktiese toepassings. Hierdie stelling word bewys in onder ander die uitstekende oorsig deur Dixon.¹ Die doel hier is die toevoeging van 'n verdere metode tot die bestaande lys, gegrond op 'n additiewe eienskap van die positiewe heelgetalle.²

2. Somme van opeenvolgende positiewe heelgetalle

Vir die *som* in 'n voorstelling van die vorm

$$t = \sum_{r=1}^n (a + r - 1)$$

waar $a \geq 1$ en $n \geq 3$ heelgetalle is, word die term δ -partisie van t gebruik, en word $\delta(t, a, n)$ daarvoor geskryf. Voorbeeld van δ -partisies is $45 = \delta(45, 5, 6)$ en $45 = \delta(45, 14, 3)$. Twee bekende resultate² word hier as grondslag vir die verdere aanbieding aangehaal.

STELLING 1: Elke saamgestelde, onewe positiewe heelgetal besit 'n δ -partisie. \square

Dit volg maklik (as bewys vir hierdie stelling) dat vir enige faktorisering $t = kg$ ($3 \leq k \leq g$) geld dat

$$t = \delta(t, g - \frac{1}{2}(k - 1), k).$$

Vir enige gegewe faktorisering $t = kg$ ($3 \leq k \leq g$) volg ook direk dat

$$t = \delta(t, k - \frac{1}{2}(g - 1), g) \text{ as } g < 2k + 1$$

en

$$t = \delta(t, \frac{1}{2}(g + 1) - k, 2k) \text{ as } g \geq 2k + 1;$$

en in die geval $g < 2k + 1$ geld dat

$$\delta(t, g - \frac{1}{2}(k - 1), k) \equiv \delta(t, k - \frac{1}{2}(g - 1), g) \Leftrightarrow k = g.$$

Die volgende omgekeerde van *STELLING 1* toon dat die pasbespreekte drie vorms van δ -partisies die enigste is wat 'n onewe positiewe heelgetal kan hê.

STELLING 2: Laat $\delta(t, a, n)$ 'n δ -partisie van 'n onewe positiewe heelgetal t wees, dan geld minstens een van die volgende twee uitkomste:

(1) Daar bestaan 'n faktorisering $t = kg$ ($3 \leq k \leq g$, $g < 2k + 1$) en ooreenstemmend hiermee die versameling δ -partisies

$$\Delta(1) = \{\delta(t, g - \frac{1}{2}(k - 1), k), \delta(t, k - \frac{1}{2}(g - 1), g)\};$$

en $\delta(t, a, n) \in \Delta(1)$.

(2) Daar bestaan 'n faktorisering $t = kg$ ($3 \leq k \leq g$, $g \geq 2k + 1$) en ooreenstemmend hiermee die versameling δ -partisies

$$\Delta(2) = \{\delta(t, g - \frac{1}{2}(k - 1), k), \delta(t, \frac{1}{2}(g + 1) - k, 2k)\};$$

en $\delta(t, a, n) \in \Delta(2)$. \square

GEVOLG: 'n Onewe getal is saamgestel as, en slegs as dit 'n δ -partisie besit. \square

OPMERKINGS: (1) 'n Onewe getal t wat m faktoriserings van die vorm $t = kg$, $3 \leq k \leq g$ het, het $2m$ δ -partisies, behalwe in die geval waar t 'n vierkant is, in welke geval

*Outeur aan wie korrespondensie gerig kan word.

die aantal δ -partisies gegee word deur $2m - 1$. (2) In enige δ -partisie $\delta(t, a, n)$ is $a \leq \frac{1}{2}(t - 3)$, want $a + (a + 1) + (a + 2) = 3a + 3 \leq t$.

Die *GEVOLG* hierbo word nou eksplisiet geformuleer as:

ALGORITMEBASIS I: 'n Onewe getal t is saamgesteld as, en slegs as daar positiewe heelgetalle $a \leq \frac{1}{2}(t - 3)$ en $n \geq 3$ bestaan sodanig dat $t = \sum_{r=1}^n (a + r - 1)$. (In hierdie situasie is $t = \frac{1}{2}n(2a + n - 1)$, en: as n onewe is, dan is n 'n faktor van t ; en as n ewe is, dan is $\frac{1}{2}n$ 'n faktor van t .) \square

Die doel is om hierdie algoritmebasis tot op 'n gewenste peil van optimaliteit te verfyn.

3. Verfyning van die algoritmebasis

Uit §2 volg dat met elke faktorisering $t = kg$ ($3 \leq k \leq g$) van 'n onewe positiewe heelgetal t presies twee δ -partisies ooreenstem, naamlik

$$(1) \delta(t, g - \frac{1}{2}(k - 1), k)$$

en dan nog presies één van

$$(2) \delta(t, k - \frac{1}{2}(g - 1), g), \text{ (as } g < 2k + 1\text{)}$$

en

$$(3) \delta(t, \frac{1}{2}(g + 1) - k, 2k), \text{ (as } g \geq 2k + 1\text{);}$$

behalwe in die geval waar $k = g$, waar daar slegs die δ -partisie (1) \equiv (2) is. Vir die aanvangsterme in hierdie partisies volg dat

$$(4) (g - \frac{1}{2}(k - 1)) - (k - \frac{1}{2}(g - 1)) = \frac{1}{2}(g - k) \geq 0$$

en

$$(5) (g - \frac{1}{2}(k - 1)) - (\frac{1}{2}(g + 1) - k) = \frac{1}{2}(g + k) > 0.$$

Die volgende notasie is vir die aanvangsterme van die δ -partisies in (1) - (3) gebruik; vir (1): $a(kg, k) := g - \frac{1}{2}(k - 1)$; vir (2): $a(kg, g) := k - \frac{1}{2}(g - 1)$; vir (3): $a(kg, 2k) := \frac{1}{2}(g + 1) - k$. In hierdie notasie geld nou op grond van STELLING 2, en (4) en (5):

STELLING 3: Laat $t = kg$ ($3 \leq k \leq g$) 'n faktorisering van 'n onewe getal t wees.

(1) As $g < 2k + 1$ word die ooreenstemmende δ -partisies van t gegee deur

$$\delta(t, a(kg, k), k) \text{ en } \delta(t, a(kg, g), g),$$

en geld dat $a(kg, k) \geq a(kg, g)$.

(2) As $g \geq 2k + 1$ word die ooreenstemmende δ -partisies van t gegee deur

$$\delta(t, a(kg, k), k) \text{ en } \delta(t, a(kg, 2k), 2k),$$

en geld dat $a(kg, k) > a(kg, 2k)$. \square

Vervolgens word die faktorisings van 'n willekeurige gegewe onewe positiewe heelgetal t , $\{t = kg : 3 \leq k \leq g\}$ beskou, en word vir die doel van rekenaarsoktote die gunstigste grense vir die aanvangsterme van die ooreenstemmende δ -partisies as funksies van die toetsgetal t bepaal. Eerstens is opgelet dat $a(kg, l) \leq \frac{1}{2}(l - 3)$ vir $l = k, g, 2k$. Verder is:

$$\begin{aligned} a(kg, k) &= g - \frac{1}{2}(k - 1) \geq \sqrt{t} - \frac{1}{2}(\sqrt{t} - 1) = \frac{1}{2}(\sqrt{t} + 1) \\ a(kg, g) &= k - \frac{1}{2}(g - 1) \leq \sqrt{t} - \frac{1}{2}(\sqrt{t} - 1) = \frac{1}{2}(\sqrt{t} + 1) \\ a(kg, 2k) &= \frac{1}{2}(g + 1) - k = \frac{1}{2}(\frac{1}{2}k + 1) - k \leq \frac{1}{2}(\frac{1}{2}k + 1) - 3 = \frac{1}{6}(t - 15). \end{aligned}$$

Die twee *bogrens* (in die laasgenoemde twee gevalle) is eerste suksesse in die gevalle waar die toetsgetal 'n vierkant van 'n priemgetal of van die vorm $3p$ (p priem, $p \geq 7$) onderskeidelik is.

Die gestelde grensafskattings saam met *STELLING 2* gee nou:

ALGORITMEBASIS II: Die volgende drie voorwaardes op 'n onewe positiewe heelgetal t is ekwivalent:

- (1) t is 'n saamgestelde getal.
- (2) Daar bestaan 'n δ -partisie $\delta(t, a, n)$ met $\frac{1}{2}(\sqrt{t} + 1) \leq a \leq \frac{1}{2}(t - 3)$.
- (3) Daar bestaan
 - (3.1) 'n δ -partisie $\delta(t, a, k)$ met $a \leq \frac{1}{2}(\sqrt{t} + 1)$ óf
 - (3.2) 'n δ -partisie $\delta(t, a, g)$ met $a \leq \frac{1}{2}(\sqrt{t} + 1)$.

Die δ -partisie in (2) is van die vorm $\delta(kg, a(kg, k), k)$, en dié in (3.1) en (3.2) van die vorms $\delta(kg, a(kg, g), g)$ en $\delta(kg, a(kg, 2k), 2k)$ onderskeidelik. Voorwaarde II(2) is duidelik 'n verbetering op die "rou" *ALGORITMEBASIS I*. En hierdie basis II(2) word op sy beurt oortref deur die basis II(3) – in (3.1) weens die kort interval $[1, \frac{1}{2}(\sqrt{t} + 1)]$ teenoor $[\frac{1}{2}(\sqrt{t} + 1), \frac{1}{2}(t - 3)]$, en in (3.2) weens die kleiner bogrens $\frac{1}{6}(t - 15)$, sowel as *STELLING 3(2)* vir gevalle waar $a(kg, 2k) > \frac{1}{2}(\sqrt{t} + 1)$. Verder word dus op *ALGORITMEBASIS II(3)* gekonsentreer.

Vir groot toetsgetalle t wat slegs oor faktorisings van die vorm kg met $g \geq 2k + 1$ beskik, kan die soektote na aanvangsterme $a(kg, 2k)$ oor die (heelgetalle in die) eerste komponent van die toetsinterval

$$[1, \frac{1}{6}(t - 15)] = [1, \frac{1}{2}(\sqrt{t} + 1)] \cup (\frac{1}{2}(\sqrt{t} + 1), \frac{1}{6}(t - 15)]$$

faal, en in die tweede komponent steeds relatief lank duur. Om hierdie probleem te akkommodeer, sal die additiewe basis II(3) vervang word met 'n additief-multiplikatiewe basis waardeur alle soektote dan binne die interval $[1, \frac{1}{2}(\sqrt{t} + 1)]$ sal plaasvind. Hiertoe is nodig:

STELLING 4: As $t = kg$ ($3 \leq k \leq g$) 'n faktorisering met $g \geq 2k + 1$ is, dan is $k < \frac{1}{2}\sqrt{t}$.

Bewys: $a(kg, 2k) > \frac{1}{2}(\sqrt{t} + 1)$

$$\begin{aligned} &\Leftrightarrow g + 1 - 2k > \sqrt{t} + 1 \\ &\Leftrightarrow t + k - 2k^2 > k\sqrt{t} + k \end{aligned}$$

$$\begin{aligned} &\Leftrightarrow 2k^2 + \sqrt{t} \cdot k - t < 0 \\ &\Leftrightarrow (k + \sqrt{t})(2k - \sqrt{t}) < 0 \\ &\Leftrightarrow k < \frac{1}{2}\sqrt{t}. \quad \square \end{aligned}$$

ALGORITME BASIS II(3) kan dus vervang word met:

ALGORITME BASIS III: Die volgende twee voorwaardes op 'n onewe positiewe heelgetal t is ekwivalent:

- (1) t is 'n saamgestelde getal.
- (2) Daar bestaan 'n δ -partisie $\delta(t, a, n)$ met $a \leq \frac{1}{2}(\sqrt{t} + 1)$, of daar bestaan 'n onewe heelgetal k met $3 \leq k < \frac{1}{2}\sqrt{t}$ sodanig dat k 'n faktor van t is. \square

Die kragpunt van die multiplikatiewe gedeelte van die basis *III(2)* lê (natuurlik) by toetsgetalle met (onder andere) *klein* priemfaktore, terwyl dié van die additiewe gedeelte lê by toetsgetalle met faktorisering van (onder andere) die vorm kg met k in die "omgewing" van $\frac{1}{2}g$. Laasgenoemde word bevestig in:

STELLING 5: Laat $t = kg$ ($3 \leq k \leq g$) 'n faktorisering van 'n onewe positiewe heelgetal t wees, en η 'n positiewe heelgetal. Dan is $a \leq \eta$ vir enige δ -partisie $\delta(t, a, n)$ van t as en slegs as $|2k - g| \leq 2\eta - 1$.

Bewys: As $g < 2k + 1$, dan is $a = a(kg, g) = k - \frac{1}{2}(g - 1) = \frac{1}{2}(2k - g + 1)$ en

$$|2k - g| = 2k - g, \text{ sodat}$$

$$|2k - g| \leq 2\eta - 1 \Leftrightarrow 2k - g \leq 2\eta - 1 \Leftrightarrow a \leq \eta.$$

As $g \geq 2k + 1$, dan is $a = a(kg, 2k) = \frac{1}{2}(g + 1) - k = \frac{1}{2}(g - 2k + 1)$ en $|2k - g| = g - 2k$, sodat

$$|2k - g| \leq 2\eta - 1 \Leftrightarrow g - 2k \leq 2\eta - 1 \Leftrightarrow a \leq \eta. \quad \square$$

Die gunstigste toetsgetalle vir die additiewe gedeelte van die algoritmebasis is inderdaad dié van die vorm $k(2k+1)$ self, want hierin is $a(kg, 2k) = 1$. Die ongunstigste toetsgetalle vir die basis as geheel is die priemgetalle: die basis *faal* met 'n getal t as en slegs as t 'n priemgetal is! En vlak naas die priemgetalle (in hierdie verband) lê die vierkante van priemgetalle, $t = p^2$, want hierin is 'n faktor $k < \frac{1}{2}\sqrt{t}$ nie ter sprake nie, en $a(p^2, g) = \frac{1}{2}(\sqrt{t} + 1)$.

LITERATUURVERWYSINGS

1. Dixon, J.D. (1984). Factorization and primality tests, *Amer. Math. Monthly*, 91: 333-352.
2. De la Rosa, B. (1978). Primes, powers and partitions, *The Fibonacci Quarterly*, 16: 518-522.