STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1956-013

Bespreking van het manuscript

Een methode voor het ontbinden van getallen van

Frater Edwardo Smits

H.J.A. Duparc

1956
ZW

Rapport ZW 1956-013
(Intern)

Bespreking van het manuscript

Een methode voor het ontbinden van getallen van Frater Edwardo Smits,

door H.J.A. Duparc

De schrijver geeft, toegelicht met veel voorbeelden, een methode waarmee het hem, geroutineerd als hij is in den door hem ontworpen gedachtengang, gelukt om sommige getallen in priemfactoren te ontbinden. Het essentiële van zijn methode is dat hij om factoren van een getal te vinden zowel gebruik maakt van hun grootte als van hun resten bij deeling door allerlei deelers. Zijn methode is het eenvoudigste te illustreeren aan een voorbeeld.

Zij het te ontbinden getal $g=100895598169$. Zij $g=pq$. Dan is mod 10 gerekend hetzij $p\equiv 3$, $q\equiv 3$, hetzij $p\equiv 1$, $q\equiv 9$, hetzij $p\equiv 7$, $q\equiv 7$. Beschouwen wij eerst het eerste geval. Zij $p<q$. Dan heeft men voor p slechts die tienvouden +3 te probeeren die $<\sqrt{g}$ zijn. Dit onderzoek wordt nu vereenvoudigd door te bedenken dat $[\sqrt{g}] = 317640$ en dan te stellen

$$p = 317633 - 10a, \quad q = 317633 + 10b.$$

Voor a heeft men dan $0<a<\frac{\sqrt{g}}{10}$. Uit $pq=g$ leidt de schrijver nu af

$$317633(b-a)-10ab = 487548.$$

Lettende op het karakter mod 10 der diverse hier optredende grootheden vindt men

(1) $\qquad b-a=6+10K$; dus $ab=141825 + 317633\,K$,

waaruit nog volgt dat

(2) $\qquad (b+a)^2=567336 + 1270652\,K + 100\,K^2$.

De bepaling van de getallen a en b en de hulpgrootheid k geschiedt door (2) op te vatten als Diophantische vergelijking voor a+b en K en door voor K de diverse restklassen modulo allerlei getallen te probeeren, waarbij steeds de helft van het aantal van alle mogelijke restklassen uitvalt. Hier wordt natuurlijk de theorie der quadraatresten ingeschakeld. Na veel en handig probeeren komt de schrijver zoo òf tot de gewenschte waarde van K, a en b òf tot de onmogelijkheid van een dergelijke ontbinding. Daarna probeert hij eventueel een ontbinding waarbij $p\equiv 1 \pmod{10}$ is en dus $q\equiv 9 \pmod{10}$. Dit doet hij door 9g te nemen en daarvoor te schrijven

$$9g = (952899 - 10a)(952899 + 10b)$$

en verder volgens bovengenoemd procédé te werken. Zoo nodig is ook nog te probeeren het geval dat $p\equiv q\equiv 7 \pmod{10}$ is, maar dit kan op het eerstgegeven deel van het onderzoek worden teruggebracht, waarbij nu a en b aan andere ongelijkheden hebben te voldoen, zooals b.v. $a>31763{,}3$; $b<-31763{,}3$.