



Universiteit
Leiden
The Netherlands

On the amount of sieving in factorization methods

Ekkelkamp, W.H.

Citation

Ekkelkamp, W. H. (2010, January 20). *On the amount of sieving in factorization methods*. Retrieved from <https://hdl.handle.net/1887/14567>

Version: Corrected Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/14567>

Note: To cite this publication please use the final published version (if applicable).

Stellingen

behorende bij het proefschrift

“On the Amount of Sieving in Factorization Methods”

door W.H. Ekkelkamp

1. De in hoofdstuk 3 beschreven experimenten geven aan dat het vooralsnog voor de praktijk niet nuttig is om de derde orde term in beschouwing te nemen.
2. Het is aannemelijk dat de foutterm van stelling 7 in hoofdstuk 2 verbeterd kan worden door gebruik te maken van de door Tenenbaum in [1] toegepaste methode.
[1] *Tenenbaum, G.: A rate estimate in Billingsley's theorem for the size distribution of large prime factors. Quart. J. Math. 51 (2000) 385–403*
3. Het simuleren van relaties in de number field sieve, zoals beschreven in sectie 4.2, is betrekkelijk eenvoudig aan te passen in het geval meer grote priemenvrijdelingen worden toegelaten dan in dit proefschrift.
4. Het valt te verwachten dat bij het gebruik van relaties met drie grote priemenvrijdelingen de keuze van verschillende grenzen een tijdswinst oplevert ten opzichte van gelijke grenzen en dat deze tijdswinst procentueel groter is dan in het geval van twee grote priemenvrijdelingen.
5. De generieke Painlevé equations I t/m VI hebben alleen triviale Lie symmetrieën [2].
[2] *Ekkelkamp, W.H.: On the computation of Lie symmetries. MSc.thesis, Rijksuniversiteit Groningen (2004)*
6. Het fibonacciwoord is de limiet van de fibonaccirij, die wordt voortgebracht door de substitutie $0 \rightarrow 01, 1 \rightarrow 0$, met $F_2 = 0, F_3 = 01$ en $F_{i+1} = F_i \circ F_{i-1}$ voor $i = 3, 4, \dots$ ($\circ$ is concatenatie). Een woord $w_1 w_2 \dots w_n$ is een palindroom als geldt $w_1 \dots w_n = w_n \dots w_1$, en een prefix is een eerste deel van een woord, oftewel $w_1 \dots w_k, k \leq n$. Er geldt: u en v zijn palindromic prefixes van een fibonacciwoord met $|u| < |v|$ dan en slechts dan als $|v| - |u|$ een periode is van v .
7. De in dit proefschrift behandelde methode om het aantal relaties te schatten voor het factoriseren van grote getallen met de Number Field Sieve kan ook toegepast worden voor het vinden van de discrete logaritme met de index calculus methode [3].
[3] *Gaudry, P., Thomé, E., Thériault, N., Diem, C.: A double large prime variation for small genus hyperelliptic index calculus. Math. Comp. 76 (2007) 457–492*
8. Zij $\sigma(m)$ de som van alle delers van het natuurlijke getal m . Een paar (m, n) , met $m < n$, heet een bevriend getallenpaar als $\sigma(m) - m = n$ en $\sigma(n) - n = m$. Kleinste voorbeeld: $(m, n) = (220, 284)$. Zij $A(x)$ het aantal bevriende getallenparen

(m, n) met $1 \leq m \leq x$. Voor $x = 10^4, 10^5, \dots, 10^{14}$ weten we uit [4] dat, respectievelijk, $A(x) = 5, 13, 42, 108, 236, 586, 1427, 3340, 7642, 17519, 39374$. Table 4 in [5] laat zien dat $A(x) = O(\sqrt{x}/\log^i x)$ voor $x \rightarrow \infty$ geen goede asymptotische schatting is voor $A(x)$ ($i = 1, 2, 3, 4$). Een betere schatting wordt gegeven door $A(x) = O(x^\alpha)$ voor $x \rightarrow \infty$, met $\alpha \approx 0.33$, misschien wel $\alpha = 1/3$.

[4] <http://amicable.homepage.dk/knwn2.htm>

[5] Garcia, M., Pedersen, J.M., Te Riele, H.: *Amicable Pairs – a Survey*. In: Alf van der Poorten and Andreas Stein (eds.), *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications, AMS, Providence RI (2004) 179–196

9. De aanname dat dieren dezelfde gevoelens hebben als mensen is geen goede leidraad voor een optimale behandeling van dieren.
10. Niet alleen kan een dubbele ontkenning een bevestiging zijn, een dubbele bevestiging kan ook een ontkenning inhouden.
11. De auto doet zijn naam steeds meer eer aan.