



Universiteit
Leiden
The Netherlands

Mersenne primes and class field theory

Jansen, B.J.H.

Citation

Jansen, B. J. H. (2012, December 18). *Mersenne primes and class field theory*. Number Theory, Algebra and Geometry, Mathematical Institute, Faculty of Science, Leiden University. Retrieved from <https://hdl.handle.net/1887/20310>

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/1887/20310>

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

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/20310> holds various files of this Leiden University dissertation.

Author: Jansen, Bas

Title: Mersenne primes and class field theory

Date: 2012-12-18

Samenvatting

Priemgetallen

Op de middelbare school leer je dat alle materie is opgebouwd uit atomen. Zo bestaat een watermolecuul (H_2O) uit twee waterstofatomen en één zuurstofatoom. De atomen kun je daarom zien als de bouwstenen van de materie. Binnen de verzameling van de natuurlijke getallen

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \dots\}$$

heb je ook bouwstenen waaruit je alle natuurlijke getallen kunt maken. Zo is 45 “opgebouwd” uit twee 3’en en één 5, want $45 = 3 \cdot 3 \cdot 5$. De getallen 3 en 5 zijn voorbeelden van priemgetallen. Priemgetallen zijn de bouwstenen van de natuurlijke getallen.

In het scheikundelokaal hangt een poster van het periodiek systeem der elementen. Hierop staan alle atomen afgebeeld gerangschikt naar hun chemische eigenschappen. In het wiskundelokaal zie je geen poster met daarop alle priemgetallen afgebeeld. Dit komt niet omdat zo’n poster niet interessant zou zijn. Integendeel, één van de belangrijkste problemen in de wiskunde (de Riemann hypothese) gaat over de priemgetallen. Rond 300 voor Christus bewees Euclides echter dat er oneindig veel priemgetallen zijn. Dus alle priemgetallen passen niet op een poster. Als je de priemgetallen rangschikt van klein naar groot, dan ziet de verzameling van de priemgetallen er als volgt uit

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \dots\}.$$

Perfekte getallen

Een ander onderwerp dat Euclides bestudeerde waren de zogenaamde perfecte getallen. Aan de hand van het volgende voorbeeld wordt duidelijk wat een perfect getal is.

De delers van 6 zijn 1, 2 en 3 (de deler 6 doet niet mee). De som $1 + 2 + 3$ van deze delers is weer gelijk aan het oorspronkelijke getal 6. Als een getal deze bijzondere eigenschap heeft dan noemen het getal een perfect getal. Ook het getal 28 is perfect, want de delers van 28 zijn 1, 2, 4, 7, 14 en

$$1 + 2 + 4 + 7 + 14 = 28.$$

De volgende twee perfecte getallen zijn 496 en 8128. Er geldt

$$1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496 \text{ en}$$

$$1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064 = 8128.$$

Het volgende patroon dringt zich op

$$\begin{aligned} (1 + 2) \cdot 2 &= 6 \\ (1 + 2 + 4) \cdot 4 &= 28 \\ (1 + 2 + 4 + 8 + 16) \cdot 16 &= 496 \\ (1 + 2 + 4 + 8 + 16 + 32 + 64) \cdot 64 &= 8128. \end{aligned}$$

Je kunt je afvragen waarom bijvoorbeeld $(1+2+4+8) \cdot 8 = 120$ geen perfect getal oplevert. Dit getal lijkt immers dezelfde structuur te hebben als de perfecte getallen hierboven. Toch is er een groot verschil tussen 120 en de getallen hierboven. Namelijk de som $1 + 2 + 4 + 8 = 15$ is geen priemgetal, terwijl de som tussen de haakjes bij de perfecte getallen wel een priemgetal is. Ga maar na

$$\begin{aligned} (1 + 2) &= 3 \\ (1 + 2 + 4) &= 7 \\ (1 + 2 + 4 + 8 + 16) &= 31 \\ (1 + 2 + 4 + 8 + 16 + 32 + 64) &= 127. \end{aligned}$$

Euclides bewees dat elk getal van de vorm

$$\underbrace{(1 + 2 + 4 + 8 + 16 + \dots + \text{laatste term})}_{\text{priemgetal}} \cdot \text{laatste term}$$

perfect is. Later bewees Leonhard Euler (1707–1783) dat alle even perfecte getallen van deze vorm zijn. Men vermoedt dat er geen oneven perfecte getallen bestaan.

Mersenne-priemgetallen

Met het resultaat van Euclides werd een zoektocht naar perfecte getallen een zoektocht naar priemgetallen van de vorm $1 + 2 + 4 + 8 + \dots + \text{laatste term}$. Getallen van deze vorm zullen we noteren met M_n waarbij n het aantal termen is in de som. Zo is $M_3 = 1 + 2 + 4$ en $M_8 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 128$. Priemgetallen van de vorm M_n noemen we Mersenne-priemgetallen, naar de Franse monnik Marin Mersenne (1588–1648).

In de volgende tabel zie je in chronologische volgorde tot het computertijdperk voor welke n het getal M_n een Mersenne-priemgetal is (zie [18, Hoofdstuk 8.5]). (Voor de volledige lijst van bekende Mersenne-priemgetallen zie de appendix.)

n	M_n	jaar van ontdekking	ontdekker
2	3	5e eeuw voor Christus	de Oude Grieken
3	7	5e eeuw voor Christus	de Oude Grieken
5	31	3e eeuw voor Christus	de Oude Grieken
7	127	3e eeuw voor Christus	de Oude Grieken
13	8191	1456	onbekend
17	131071	1588	Cataldi
19	524287	1588	Cataldi
31	2147483647	1772	Euler
127	17014118...884105727	1876	Lucas
61	2305843009213693951	1883	Pervushin
89	618970019...449562111	1911	Powers
107	162259276...010288127	1914	Powers

Opmerkelijk is het resultaat van Edouard Lucas (1842–1891). Hoe is hij in staat geweest om aan te tonen dat het getal M_{127} , dat uit 39 cijfers bestaat, een priemgetal is? Het antwoord op deze vraag is: veel geduld en een slimme door Lucas zelf ontwikkelde priemtest voor getallen van de vorm M_n . Deze test werd in 1930 aangepast door Derrick Lehmer (1905–1991). De aangepaste versie van de test noemen we nu de Lucas-Lehmer-test.

Pas in 1952 toonde de Amerikaanse wiskundige Raphael Robinson (1911–1995) m.b.v. de computer en de Lucas-Lehmer-test aan dat M_{521} een Mersenne-priemgetal is. Hiermee was Lucas’ record M_{127} van het grootste bekende priemgetal verbroken.

Vandaag de dag gebruikt men nog steeds de Lucas-Lehmer-test om grote priemgetallen te vinden. Het grootste bekende priemgetal op dit moment is $M_{43112609}$. Het is gevonden door een netwerk van computers die zich hebben aangesloten bij het GIMPS-project (Great Internet Mersenne Prime Search) opgericht door George Woltman (1957) in 1996.

De Lucas-Lehmer-test

Lucas wist dat M_n alleen een priemgetal kan zijn als n zelf een priemgetal is. Aangezien 127 een priemgetal is maakte Lucas een kans met het testen van M_{127} op primaliteit. Zijn test deed hij op twee grote damborden van 127 bij 127 hokjes. Op het ene dambord werd geschoven met steentjes en op het andere dambord werden de tussenresultaten bijgehouden.

Om dit te illustreren zullen we gaan testen of M_5 een priemgetal is. Daartoe tekenen we een dambord van 5 bij 5 hokjes en leggen op de eerste rij derde kolom één steen neer. Dit is de beginpositie. Vanaf de beginpositie gaan we $5 - 2$ keer de volgende stappen uitvoeren (voor M_n voer je de stappen $n - 2$ keer uit).

STAP 1: Leg voor elke steen in de i -de kolom van de eerste rij een kopie van de eerste rij neer en schuif deze kopie $i - 1$ hokjes naar rechts. Als je een steen in de laatste kolom één hokje naar rechts moet verschuiven, dan leg je de steen in de eerste kolom neer.

STAP 2: Verwijder zo mogelijk één steen uit de tweede kolom. Als er geen steen in de tweede kolom ligt, dan leg je in alle kolommen behalve de tweede kolom een steen neer.

STAP 3: Pak zo lang dat mogelijk is twee stenen uit kolom i en leg daarvoor in de plaats één steen in kolom $i + 1$. Twee stenen uit de laatste kolom worden vervangen door één steen in de eerste kolom. Daarna schuif je elke steen naar de eerste rij zonder de steen van kolom te veranderen.

De borden 1 t/m 4 zien we hieronder. Op bord 1 zie je de beginpositie. De eerste rij van deze beginpositie neem je over op het resultatendambord. Door STAP 1 uit te voeren krijg je de positie op bord 2. Door STAP 2 uit te voeren krijg je de positie op bord 3, en door STAP 3 uit te voeren krijg je de positie op bord 4.

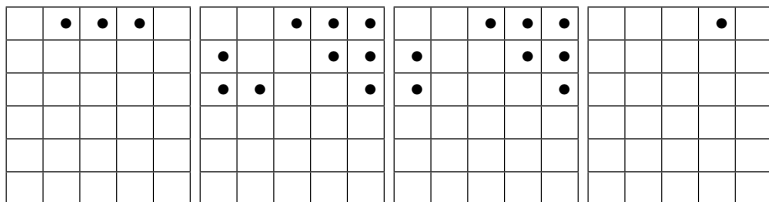
Nu hebben we de stappen 1 t/m 3 één keer uitgevoerd. De eerste rij van bord 4 zou Lucas op zijn resultatendambord overnemen. Door vanaf bord 4 nogmaals de stappen 1 t/m 3 uit te voeren komen we bij bord 7. De eerste rij van bord 7 wordt wederom op het resultatendambord overgenomen.

De laatste drie stappen staan hieronder op de borden 7 t/m 10. We zien dat bij het eindresultaat (bord 10) de eerste rij leeg is. Het resultatendambord krijgen we door de eerste rij van bord 1, bord 4, bord 7 en bord 10 onder elkaar te zetten in een dambord van 5 bij 5. Hieronder zie je de resultatendamborden voor M_3 t/m M_8 .

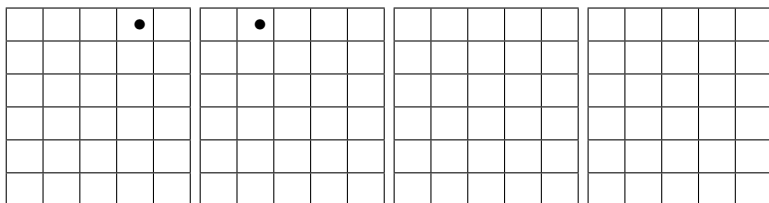
De Lucas-Lehmer-test zegt dat M_n een priemgetal is alleen als de voorlaatste rij van het resultatendambord dat bij M_n behoort leeg is of helemaal vol ligt met stenen. Door bij de resultatendamborden hieronder de voorlaatste rij af te lezen zien we dat M_3 , M_5 en M_7 priemgetallen zijn en M_4 , M_6 en M_8 geen priemgetallen zijn.

--	--	--	--

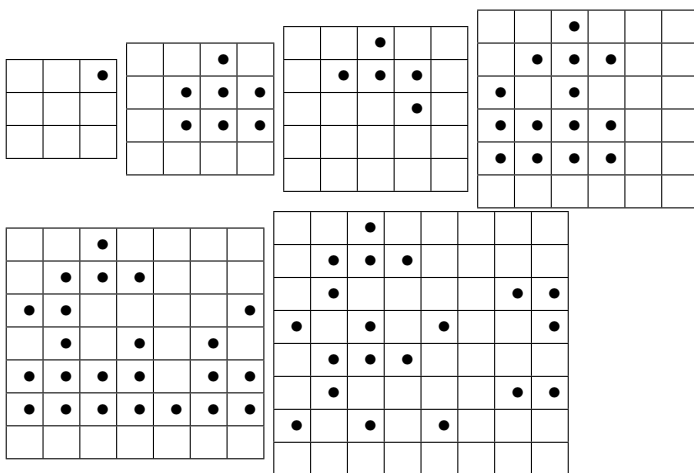
Bord 1 t/m 4



Bord 4 t/m 7



Bord 7 t/m 10

Resultatendamborden behorend bij M_3 t/m M_8

Lehmer's vraag

Als M_n een Mersenne-priemgetal is, dan weet je dat de voorlaatste rij van het resultatendambord van M_n óf helemaal leeg is óf helemaal vol ligt met stenen. Lehmer vroeg zich af of het mogelijk is om snel te bepalen welke van de twee mogelijkheden zich zal voordoen. Dit proefschrift gaat over deze vraag.

Vele beginposities

Tot nu toe was de beginpositie telkens één steen in de derde kolom (beginpositie I). Er zijn ook andere beginposities waarmee je de Lucas-Lehmer-test kunt uitvoeren. Zowel in de tweede als vierde kolom één steen is zo'n andere beginpositie (beginpositie II). Voor borden met meer dan vier hokjes is een steen in de eerste én tweede kolom en daarna alternerend geen en wel een steen in overige kolommen ook beginpositie waarmee je de Lucas-Lehmer-test kunt uitvoeren (beginpositie III). Voor elke beginpositie kunnen we Lehmer's vraag stellen.

In dit proefschrift geven we meerdere formules waarmee je oneindig veel beginposities kunt maken en we geven aan hoe je andere van dit soort formules kunt maken. Deze formules komen in twee typen, A en B. De formules van type A zijn de formules waarvoor we voor alle beginposities die uit de formule komen Lehmer's vraag kunnen beantwoorden met ja, en de formules van type B zijn de formules waarvoor we voor geen van de beginposities die uit de formule komen Lehmer's vraag kunnen beantwoorden.

Beginpositie I en II komen uit formules van type B. Beginpositie III komt uit een formule van type A. Voor beginpositie III geldt dat de voorlaatste rij van het resultaatendambord van M_n leeg is dan en slechts dan als $n - 1$ deelbaar is door 4 (en $n \neq 5$). Voor andere beginposities die uit formules van type A komen gelden soortgelijke uitspraken.

Woltman's vermoeden

Hoewel we geen antwoord hebben op Lehmer's vraag voor beginpositie I en beginpositie II is er wel een verband tussen deze twee beginposities. De voorlaatste rij van het resultaatbord van M_n met beginpositie I is gelijk aan de voorlaatste rij van het resultaatbord van M_n met beginpositie II dan en slechts dan als $n - 5$ of $n - 7$ deelbaar is door 8 en $n \neq 5$. Dit verband werd als eerste gezien door Woltman in 1996. In dit proefschrift bewijzen we dit vermoeden en geven we andere voorbeelden van relaties tussen verschillende beginposities die komen van formules van type B.

Terug naar Lehmer's vraag voor beginpositie I

Lehmer's vraag voor beginpositie I blijft onbeantwoord. Wel laten we in dit proefschrift zien: als iemand voor beginpositie I (of elke andere beginpositie die komt van een formule van type B) een soortgelijke stelling kan vinden als voor beginpositie III, dan is het gedrag van de Mersenne-priemgetallen heel anders dan je zou mogen verwachten.

Klassenlichamentheorie en priemgetallen van de vorm $x^2 - 2 \cdot y^2$

Diophantische problemen vormen een belangrijke motor voor het ontwikkelen van nieuwe getaltheorie. Een voorbeeld van een Diophantisch probleem is de vraag: welke priemgetallen kun je schrijven als het verschil van een kwadraat

en tweemaal een ander kwadraat? Voor de priemgetallen kleiner dan of gelijk aan 53 geeft dit het volgende resultaat.

p	wel of geen oplossing?	bijvoorbeeld
2	wel	$2^2 - 2 \cdot 1^2$
3	geen	
5	geen	
7	wel	$5^2 - 2 \cdot 3^2$
11	geen	
13	geen	
17	wel	$7^2 - 2 \cdot 4^2$
19	geen	
23	wel	$5^2 - 2 \cdot 1^2$
29	geen	
31	wel	$9^2 - 2 \cdot 5^2$
37	geen	
41	wel	$7^2 - 2 \cdot 2^2$
43	geen	
47	wel	$7^2 - 2 \cdot 1^2$
53	geen	

Het is niet lastig om aan te tonen dat voor priemgetallen 3, 5, 11, 13, 19, 29, 37, 43, 47 en 53 er inderdaad geen oplossing bestaat voor het hierboven beschreven probleem.

Veel interessante Diophantische problemen kunnen worden aangepakt door in een handige uitbreiding van de natuurlijke getallen te gaan redeneren. Voor het bovenstaande probleem is de verzameling $\mathbb{Z}[\sqrt{2}]$ van alle elementen van de vorm $a + \sqrt{2} \cdot b$ met a en b gehele getallen een handige uitbreiding. De term $x^2 - 2 \cdot y^2$ kan met coëfficiënt $\sqrt{2}$ uit de verzameling $\mathbb{Z}[\sqrt{2}]$ worden geschreven als een product, namelijk $(x - \sqrt{2} \cdot y) \cdot (x + \sqrt{2} \cdot y)$. Dit betekent: als een priemgetal p te schrijven is als $x^2 - 2 \cdot y^2$, dan is p geen priemgetal meer in $\mathbb{Z}[\sqrt{2}]$. Bijvoorbeeld:

$$\begin{aligned} 2 &= \sqrt{2} \cdot \sqrt{2} \\ 7 &= (5 - \sqrt{2} \cdot 3) \cdot (5 + \sqrt{2} \cdot 3) \\ 17 &= (7 - \sqrt{2} \cdot 4) \cdot (7 + \sqrt{2} \cdot 4). \end{aligned}$$

De getallen $\sqrt{2}$, $(5 - \sqrt{2} \cdot 3)$, $(5 + \sqrt{2} \cdot 3)$, $(7 - \sqrt{2} \cdot 4)$ en $(7 + \sqrt{2} \cdot 4)$ zijn voorbeelden van priemgetallen in $\mathbb{Z}[\sqrt{2}]$. Tevens geldt: als een priemgetal p ook in $\mathbb{Z}[\sqrt{2}]$ een priemgetal blijft, dan is p niet te schrijven als $x^2 - 2 \cdot y^2$. Bijvoorbeeld: 3, 5 en 11 zijn priemgetallen in $\mathbb{Z}[\sqrt{2}]$.

Klassenlichamentheorie vertelt direct of een priemgetal p in de verzameling $\mathbb{Z}[\sqrt{2}]$ een priemgetal blijft. De theorie impliceert namelijk: een priemgetal p blijft alleen een priemgetal in $\mathbb{Z}[\sqrt{2}]$ als $p - 3$ of $p - 5$ deelbaar is door 8. Hiermee is het bovenstaande Diophantische probleem in essentie opgelost (we gebruiken namelijk ook dat in de verzameling $\mathbb{Z}[\sqrt{2}]$ elk getal op een unieke

manier te schrijven is als product van priemgetallen). De volgende tabel geeft een overzicht.

p	wel of geen oplossing?	p priemgetal in $\mathbb{Z}[\sqrt{2}]$?	8 deelt $p - 3$ of $p - 5$?
2	wel	nee	nee
3	geen	ja	ja
5	geen	ja	ja
7	wel	nee	nee
11	geen	ja	ja
13	geen	ja	ja
17	wel	nee	nee
19	geen	ja	ja
23	wel	nee	nee
29	geen	ja	ja
31	wel	nee	nee
37	geen	ja	ja
41	wel	nee	nee
43	geen	ja	ja
47	wel	nee	nee
53	geen	ja	ja

De uitbreiding van de natuurlijke getallen naar $\mathbb{Z}[\sqrt{2}]$ komt van een zogenaamde abelse uitbreiding van getallenlichamen. Klassenlichamentheorie geeft voor elke abelse uitbreiding van getallenlichamen op soortgelijke wijze als in ons voorbeeld aan hoe de priemgetallen zich in de uitbreiding gedragen.

Bewijsmethode

In dit proefschrift wordt Lehmer's vraag vertaald naar een probleem dat met behulp van de klassenlichamentheorie kan worden aangepakt. Op deze manier zijn de resultaten in dit proefschrift komend van Lehmer's vraag bewezen.

Aangezien klassenlichamentheorie een diepgaande moderne theorie is waar vele grote wiskundigen aan hebben gewerkt, zal het hoogstwaarschijnlijk ondoenlijk zijn om met elementaire wiskunde deze resultaten te bewijzen.