Samenvatting

Wagstaff-getallen zijn getallen van de vorm $\frac{2^n+1}{3}$, waarbij n een natuurlijk getal is. We zullen in hoofdstuk 2 kijken naar eigenschappen van deze getalvorm die iets zeggen over n wanneer $\frac{2^n+1}{3}$ priem is. Deze eigenschappen leiden tot een algoritme dat voor $n < 61$ snel kan controleren of $\frac{2^n+1}{3}$ priem is. Voor grotere Wagstaff-getallen hebben we in hoofdstuk 3 stellingen bewezen die iets zeggen als:

$$\frac{2^n+1}{3} \text{ is priem} \quad \Rightarrow \quad \begin{array}{l}\text{Het } n\text{'de getal in allerlei rijtjes} \\ \text{voldoet aan een zekere voorwaarde.}\end{array}$$

We hebben een stelling geconstrueerd die een aantal stellingen van deze vorm overkoepelt. Voor deze nieuwe stelling zullen we, net als voor de reeds bestaande stellingen, de noodzaak ($\Rightarrow$) van de voorwaarde bewijzen. Echter kunnen we nog niet bewijzen dat deze voorwaarde voldoende is ($\Leftarrow$). Wel zullen we in dit onderzoek het reeds bekende bewijs herhalen van een vergelijkbare stelling van een primaliteitstest - de Lucas-Lehmer test - voor een vergelijkbaar soort getallen, namelijk Mersenne-getallen, gedefinieerd als $2^n - 1$, waarbij n wederom een natuurlijk getal is. Tenslotte zal in hoofdstuk 4 de primaliteit voor een aantal Wagstaff-getallen aangetoond worden met behulp van twee verschillende stellingen, waarvan een bekende en een nieuwe stelling.

Inhoudsopgave

Hoofdstuk 1

Introductie

In 1989 zijn door onder andere S.S.Wagstaff in het artikel 'The New Mersenne Conjecture' [1] Wagstaff-getallen $W_n = \frac{2^n+1}{3}$ geintroduceerd. Het grootste Wagstaff-getal waarvan tot nu toe de primaliteit is aangetoond is W_{42737}. Wagstaff-getallen lijken tamelijk veel op Mersenne-getallen, $M_n = 2^n - 1$. Om het Mersenne-getal op primaliteit te testen is de Lucas-Lehmer test bedacht. Deze werd al in 1930 in het artikel "An extended theory of Lucas' functions" [2] door Lehmer gepubliceerd. Met behulp van deze test zijn heel grote priemgetallen M_n gevonden, bijvoorbeeld voor $n = 43112609$. Dit is op dit moment het grootst bewezen priemgetal. Dit getal telt maar liefst 12978189 cijfers. Eigenlijk is het Wagstaff-getal een variant op het Mersenne-getal. Er werd waarschijnlijk eerst gekeken naar $2^n + 1$. Echter geldt $(2^n + 1) \bmod 3 = (2^n) \bmod 3 + (1) \bmod 3 = (-1)^n \bmod 3 + (1) \bmod 3$. Nemen we nu n oneven dan geldt:$(-1)^n \bmod 3 + (1) \bmod 3 = (-1 + 1) \bmod 3 = 0 \bmod 3$. Oftewel: $2^n + 1$ is deelbaar door 3 voor een oneven n. Merk op dat als n even is, dan geldt $(-1)^n = 1$, oftewel $\frac{2^n+1}{3} \bmod 3 = \frac{2}{3}$. Een even n levert dus nooit een geheel getal op. Vandaar dat Wagstaff besloot naar het getal $\frac{2^n+1}{3}$ te kijken voor oneven n. Er is inmiddels van 30 Wagstaff-getallen bekend dat ze priem zijn. Hieronder laten we in een tabel de eerste 22 n'en zien, waarvoor W_n priem is.

#	n zodat W_n priem is	#	n zodat W_n priem is
1	3	12	79
2	5	13	101
3	7	14	127
4	11	15	167
5	13	16	191
6	17	17	199
7	19	18	313
8	23	19	347
9	31	20	701
10	43	21	1709
11	61	22	2617

Merk op dat er geen even n in het rijtje voorkomt. Merk bovendien op dat de eerste 8 priemgetallen na 2 allemaal een Wagstaff-priem geven en dat voor de andere n'en tot het 22ste Wagstaff-getal ook geldt dat ze priem zijn. De vereiste van de primaliteit voor n blijkt te gelden voor alle Wagstaff-priemen. Deze eigenschap en andere zullen nu aan bod komen.

Hoofdstuk 2

Beginselen

Definitie. *Voor $n \geq 1$ een geheel getal noteren we $W_n = \frac{2^n+1}{3}$. Dit noemen we een Wagstaff-getal.*

2.1 Eigenschappen

Hier volgen 6 eigenschappen van Wagstaff-getallen:

1. Er geldt: $W_{n+2} = 4 \cdot W_n - 1$ voor n oneven.
2. Als n oneven is dan is W_n geheel.
3. Als n oneven is en W_n priem dan is n priem.
4. Als W_p niet priem is en $p > 2$ en priem dan geldt voor de priemdelers l van W_p dat ze 1 mod $2p$ zijn.
5. Als $p > 2$ en priem is en $l > 2$, priem en $l \mid W_p$ dan geldt: $l \equiv 1 \bmod 8$ of $l \equiv 3 \bmod 8$.
6. Als $n > 1$ en oneven is, dan is W_n geen kwadraat.

2.2 Bewijzen

In deze sectie zullen we de bewijzen van de in 2.1 genoemde eigenschappen geven.

1. Het bewijs van de eerste eigenschap volgt direct uit de definitie van Wagstaff-getallen:

$$W_{n+2} = \frac{2^{n+2}+1}{3} = \frac{4 \cdot 2^n + 1}{3} = 4 \cdot \frac{2^n+1}{3} - 1 = 4 \cdot W_n - 1.$$

2. Het bewijs van de tweede eigenschap wordt met behulp van inductie gegeven. Je ziet: $n = 1 \Rightarrow W_n = 1 \in \mathbb{N}$. Dan volgt de inductiehypothese: $W_n \in \mathbb{N}$. Nu moet er gecontroleerd worden dat $W_{n+2} \in \mathbb{N}$. Dit volgt direct uit eigenschap 1 en de inductiehypothese.

3. De derde eigenschap zal bewezen worden door te laten zien dat als n samengesteld is dan heeft W_n delers. Dus stel $n = a \cdot b$, waarbij $a > 1$ en $b > 1$ en beide oneven, dan is $W_n = (2^{ab} + 1)/3$. Dit herschrijven we nu door $(-2)^a = c$ te substitueren. Met behulp van de algebraische identiteit
$$(1 - c)(1 + c + c^2 + ... + c^{b-1}) = 1 - c^b$$
[9] kunnen we de breuk nu als volgt opschrijven:
$$\frac{(2^{ab} + 1)}{3} = \frac{(1 - c^b)}{3} = \frac{(1 - c)(1 + c + c^2 + ... + c^{b-1})}{3} = \tag{2.1}$$
$$= W_a \cdot (1 + c + c^2 + ... + c^{b-1}) \tag{2.2}$$
De twee factoren W_a en $(1 + c + c^2 + ... + c^{b-1})$ zijn geheel (want a is oneven, zie eigenschap 2). Verder geldt: $1 < W_a < W_n$ omdat $1 < a < n$. Beide factoren zijn dus 'echte' factoren. Hiermee is eigenschap 3 bewezen.

4. De vierde eigenschap wordt als volgt bewezen: je weet: $\frac{2^p+1}{3} \equiv 0 \bmod l$. Dus $2^p + 1 \equiv 0 \bmod l$. Oftewel $2^p \equiv -1 \bmod l$, waar $2^{2p} \equiv 1 \bmod l$ uit volgt. Nu gaan we kijken naar de orde van 2 in de groep $(\mathbb{Z}/l\mathbb{Z})^* = {\mathbb{F}_l}^*$. Je weet dat de orde een deler is van $2p$. De orde is dus $1, 2, p$ of $2p$. Stel de orde is 1, dan volgt hieruit dat $2 \equiv 1 \bmod l$. Maar $l \neq 1$, omdat l priem is, dus dit kan niet. Stel dat de orde 2 is, dan volgt hieruit $l \mid (4 - 1) = 3$. Dus $l = 3$. Dan heb je: $3 \mid \frac{2^p+1}{3}$, dus $9 \mid 2^p + 1$. Nu herschrijven we als volgt: $2^p + 1 = 1 + ((-1) \cdot (-2))^p = 1 - (-2)^p = 1 - (1 - 3)^p$. Vervolgens nemen we dit modulo 9. Dus, met behulp van het binomium van Newton, krijg je: $1 - (1 - 3)^p \bmod 9 = 1 - (1 + (-3))^p = [1^p + \binom{p}{1} 1^{p-1}(-3) + ... + \binom{p}{p-1}(-3)^{p-1} + (-3)^p] \bmod 9 = (1 - (1 + \binom{p}{1}(-3)))\bmod 9 = 3p \bmod 9 = 0 \bmod 9$. Hierbij wordt gebruikt dat: $3^i \bmod 9 = 0$ voor $i \geq 2$. Aangezien p priem is, volgt er dat $p = 3$, maar dan is W_p priem, wat tegen de aannames ingaat. Ten slotte kan de orde van 2 ook geen p zijn, aangezien $2^p \equiv -1 \bmod l$ en $l > 2$. Conclusie: de orde van $\bar{2}$ in ${\mathbb{F}_l}^*$ is $2p$. Omdat de orde een deler is van het aantal elementen van ${\mathbb{F}_l}^*$, volgt $2p \mid l - 1$, oftewel $l \equiv 1 \bmod 2p$.

5. Het bewijs van de vijfde eigenschap bestaat uit twee delen. Merk allereerst op dat als $l|W_p$ dan is l oneven. In het eerste deel zal worden bewezen dat als $l|W_p$ dan bestaat er een $x \in \mathbb{F}_l$ waarvoor geldt dat

$x^2 = -2 \bmod l$. In het tweede deel zal worden bewezen dat: als l een oneven priemgetal is en er een $x \in \mathbb{F}_l$ bestaat zodat $x^2 = -2 \bmod l$ dan geldt: $l = 1 \bmod 8$ of $l = 3 \bmod 8$. Met deze twee delen is het bewijs van eigenschap 4 gegeven.
Deel 1: je weet dat $l \mid W_p$, dus $(2^p + 1)/3 = 0 \bmod l$. Dus is $2^p + 1 \equiv 0 \bmod l$, waar $2^p \equiv -1 \bmod l$ uit volgt. Nu geldt het volgende uiteraard ook: $2^{p+1} = -2 \bmod l$. Dus met $x = 2^{(p+1)/2}$ is deel 1 bewezen.
Deel 2: we kijken hier naar een uitbreiding van $\mathbb{F}_l$ namelijk $\mathbb{F}_{l^2}$. Dit is een lichaam met precies $l^2 - 1$ elementen. De theorie over eindige lichamen zegt dat ${\mathbb{F}_{l^2}}^*$ een cyclische groep is [3]. Stel dat $y \in {\mathbb{F}_{l^2}}^*$ deze groep voortbrengt, dus $orde(y) = l^2 - 1$. Omdat l oneven is, geldt $l^2 - 1 = (l-1) \cdot (l+1)$ is deelbaar door 8. Dus bestaat $\zeta := y^{(p^2-1)/8} \in (\mathbb{F}_{l^2})^*$ zodat $orde(\zeta) = 8$. Er geldt dus $\zeta^8 = 1$. Dan volgt $(\zeta^4 + 1)(\zeta^4 - 1) = \zeta^8 - 1 = 0$. Omdat $\zeta^4 - 1 \neq 0$ (immers de orde van ζ is 8), moet wel gelden: $\zeta^4 + 1 = 0$. Er geldt dus $\zeta^4 = -1$. Als we nu kijken we naar het element $x = \zeta + \zeta^3 \in (\mathbb{F}_{l^2})^*$, zien we:

$$x^2 = (\zeta + \zeta^3)^2 = \zeta^2 + (\zeta^3)^2 - 2 = -2.$$

Er geldt namelijk $\zeta^6 = \zeta^4 \cdot \zeta^2 = -\zeta^2$. Stel nu dat $l = 8k+1$ of $l = 8k+3$ dan zien we:

$$x^l = (\zeta + \zeta^3)^l = \zeta^l + \zeta^{3l} = \zeta + \zeta^3 = x,$$

waar bij het tweede gelijkteken gebruikt wordt gemaakt van lemma 3.1.2. Er geldt dus dat $x^l = x$. Hieruit volgt dat $x \in \mathbb{F}_l$. Stel nu dat $l = 8k + 5$ of $l = 8k + 7$ dan volgt:

$$x^l = (\zeta + \zeta^3)^l = \zeta^l + \zeta^{3l} = -(\zeta + \zeta^3) = -x.$$

Dan volgt dat $x \notin \mathbb{F}_l$. Hiermee is deel 2 bewezen.

6. Voor het bewijs van de zesde eigenschap beredeneren we als volgt: uit eigenschap 1 volgt $W_n \equiv -1 \bmod 4$ als $n \geq 3$ oneven. Omdat $\mathbb{Z}/4\mathbb{Z}$ geen element bevat met kwadraat $-1 \bmod 4$, volgt dat W_n geen kwadraat is als $n \geq 3$ oneven.

Commentaar. *De vraag is nu hoe eigenschap* 4, 5 *en* 6 *helpen bij het nagaan of* W_p *een priemgetal is. Eigenschap* 6 *wil gewoon zeggen dat* $\sqrt{W_p}$ *geen deler is van* W_p*. Eigenschap* 4 *is als volgt te lezen: als geen enkel priemgetal* 1 *mod* $2p$ *een deler van* W_p *is, dan is* W_p *een priemgetal. Verder is eigenschap* 5 *als volgt te lezen: als er geen priemen* 1 *mod* 8 *of* 3 *mod* 8 *zijn die* W_p *delen, dan is* W_p *een priemgetal. Met deze interpretaties kun je al vrij makkelijk grote Wagstaff-getallen controleren op hun primaliteit.*

Voorbeeld. *Om* $W_{31} = 715827883$ *te controleren ben je dus alleen gebonden aan de oneven priemgetallen* $< \sqrt{W_{31}}$ *(eigenschap 2,3 en 6). Verder*

moeten ze ook 1 *mod* 62 *zijn (eigenschap* 4*). Tevens moeten ze* 1 *mod* 8 *of* 3 *mod* 8 *zijn (eigenschap 5). We weten dat er iets minder dan* 3000 *oneven priemgetallen kleiner zijn dan deze wortel. Deze priemgetallen verdelen zich (op eentje na, namelijk* 31*,) over de restklassen* 1 *mod* 2 *en a mod* 31*, met* $1 \leq a \leq 30$*. Dus* $\frac{1}{30}$ *van deze getallen zit in de restklasse* 1 *mod* 31*. Dus ongeveer* 100 *priemgetallen zijn* 1 *mod* 31 *en vanwege eigenschap* 5 *zijn er nog ongeveer* 50 *getallen, die een deler zouden kunnen zijn van* W_{31}*. Dit wordt hieronder geverifieerd met een simpel Maple13 programmaatje.*

2.3 Maple13 programma's

In het programma hieronder worden 3 dingen berekend: ten eerste wordt, als W_{31} geen priemgetal is, W_{31} geprint, ten tweede worden het aantal priemen dat zowel 1 mod 62 als $< \sqrt{W_{31}}$ is, geprint (97) en ten derde wordt het aantal priemen van de overgeblevene dat bovendien 1 mod 8 of 3 mod 8 is, geprint (53).

```
> W:=(2^31+1)*1/3;
wortel := evalf(sqrt(715827883));
s := (wortel-1)*1/62;
delers := 0; priemen := 0;
for n to s do h := 1+62*n;
if isprime(h) then
priemen_1_modulo_62 := priemen_1_modulo_62+1;
if (modp(h, 8) = 1 `or` modp(h, 8) = 3) then
delers := delers+1;
if modp(W, h) = 0 then print(W)
end if end if end if end do;
print(priemen_1_modulo_62);
print(delers);
                                    97
                                    53
```

De vraag is nu tot welke Wagstaff-getallen het mogelijk is om snel te controleren of ze priem zijn. Omdat Maple13 de priemgetallen $< 2 \cdot 10^7$ al opgeslagen heeft, kun je voor Wagstaff-getallen waarvan de wortel kleiner is dan $2 \cdot 10^7$ heel snel de primaliteit uitrekenen. Hieronder zie je dat het grootste Wagstaff-getal waarvan de priemgetallen onder de wortel ervan opgeslagen zijn in Maple13 W_{47} is.

```
> weetniet := true;
for n from 3 to 100 while
weetniet do
gr := evalf(sqrt((2^ithprime(n)+1)*(1/3)));
```

```
if gr > 2*10^7 then weetniet := false
else print(ithprime(n))
end if end do;
5, 7, 11,13,17,19,23,29,31, 37,41,43,47
```

Het volgende programma controleert W_p voor $p \leq 60$ op primaliteit door het te delen door de mogelijk delers. Mocht W_p geen priem zijn dan staat de kleinste bijbehorende deler in de output.

```
>for getal from 3 to 60 do
if isprime(getal) then print(getal);
p := getal;
Wagst := (2^q+1)*1/3;
Wp := subs(q = p, Wagst);
wortelWp := evalf(sqrt(Wp));
d := (wortelWp-1)/(2*p);
weetniet:=true:
for n to d while weetniet do
h := 1+2*p*n;
if `or`(modp(h, 8) = 1, modp(h, 8) = 3)
then x := modp(2^p, h)+1;
y := modp(x, h);
if y = 0 then print(helaas, het*is*geen*priemgetal);
print(,is*deler*h);
weetniet:=false:
end if end if end do end if end do;

3,5,7,11,13,17,19,23,
29 helaas, het is geen priemgetal, 59 is deler
31,
37 helaas, het is geen priemgetal, 1777 is deler
41 helaas, het is geen priemgetal, 83 is deler
43,
47 helaas, het is geen priemgetal, 283 is deler
53 helaas, het is geen priemgetal, 107 is deler
59 helaas, het is geen priemgetal, 2833 is deler
```

Merk op dat de for-loop van dit programma doorloopt tot 60. Dit is het geval omdat voor $47 < p \leq 60, W_p$ geen Wagstaff-priem is en de delers van deze W_p's relatief kleine getallen zijn. Verder kunnen we dus concluderen dat Wagstaff getallen $< W_{61}$ makkelijk te controleren zijn op primaliteit vanwege de opgeslagen priemgetallen in Maple13 tot $2 \cdot 10^7$. Dus als we grotere Wagstaff-getallen willen controleren, zullen we andere methodes moeten gebruiken.

Hoofdstuk 3

Primaliteitstesten

Voor grote Wagstaff-getallen zijn er tests ontwikkeld die stellen aan welke eigenschap zo'n getal voldoet als het priem is. Een van de tests is ontwikkeld door Anton Vrba [7]. Verder zijn er ook nog tests ontwikkeld door Henri en Renaud Lifschitz [6] en Robert Gerbicz [5]. Deze tests zeggen allemaal iets als: W_p is priem $\Rightarrow$ bepaalde voorwaarde. Er wordt bij ieder van de tests vermoed dat het ook de andere kant op geldt, echter is dit bij geen der tests bewezen. Voor deze tests hebben we een algemenere test bedacht, die deze bestaande tests overkoepelt. Voordat we naar deze tests zullen kijken zal er eerst een link worden gelegd met een ander soort grote getallen, namelijk Mersenne getallen. Voor deze getallen is een primaliteitstest ontwikkeld die wel beide kanten op bewezen kan worden.

3.1 Mersenne getallen en de Lucas-Lehmer test

Definitie. *Voor $n > 1$ en n geheel noteren we $M_n = 2^n - 1$. Dit getal noemen we een Mersenne-getal.*

Voor dit getal is een primaliteitstest ontwikkeld door de heren Lucas en Lehmer. Deze test is als volgt:

Stelling 1 (De Lucas-Lehmer test)**.** *M_n priem $\Leftrightarrow S_{n-2} \equiv 0$ mod M_n, waarbij n een oneven priemgetal is, $S_n = (S_{n-1})^2 - 2 \bmod M_n$ en $S_0 = 4$.*

Voordat het bewijs gegeven wordt, zal eerst een aantal noodzakelijke lemma's gegeven worden.

Lemma 3.1.1. *Voor de rij $S_n = (S_{n-1})^2 - 2$ met $S_0 = 4$ geldt: $S_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$.*

Bewijs. Dit bewijs zal met behulp van inductie gegeven worden. Allereerst moet er voor $n = 0$ gecontroleerd worden. De directe formule geeft $S_0 = 2 + \sqrt{3} + 2 - \sqrt{3} = 4$, wat overeenkomt met S_0 van de recursieformule. Vervolgens

wordt met de inductiehypothese gesteld dat de directe formule klopt voor n. Nu rest ons nog om de directe formule op basis van de inductiehypothese voor $n+1$ aan te tonen:

$$\begin{aligned} S_{n+1} &= S_n^2 - 2 = \\ &= ((2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n})^2 - 2 \\ &= (2+\sqrt{3})^{2^{n+1}} + (2-\sqrt{3})^{2^{n+1}}. \end{aligned} \tag{3.1}$$

Er geldt immers $(2+\sqrt{3}) \cdot (2-\sqrt{3}) = 1$. Hiermee is het bewijs gegeven. □

Beide richtingen van de Lucas-Lehmer test zullen apart bewezen worden.

($\Rightarrow$). Eerst nemen we aan dat M_n priem is. We definieren $\omega = 2+\sqrt{3}$ en $\bar{\omega} = 2-\sqrt{3}$. Het volgende moet dus bewezen worden:

$$((\omega)^{2^{n-2}} + (\bar{\omega})^{2^{n-2}}) \pmod{M_n} \equiv 0. \tag{3.2}$$

We gaan nu kijken naar de vermenigvuldigingsgroep van het uitbreidinglichaam, namelijk $\mathbb{F}^*_{M_n^2}$. De volgende lemma's zijn nu van toepassing:

Lemma 3.1.2. *Stel q is een priemgetal en R is een ring met $\mathbb{F}_q \subset R$, dan geldt voor $a, b \in R$ dat*

$$(a+b)^q = a^q + b^q.$$

Bewijs. Bij het bewijs van dit lemma wordt gebruik gemaakt van onder andere het binomium van Newton. Dat zegt namelijk het volgende:

$$(a+b)^q = a^q + \binom{q}{1} a^{q-1}b + ... + \binom{q}{q-1} a \cdot b^{q-1} + b^q. \tag{3.3}$$

Aangezien $\binom{q}{i} = \frac{q!}{(q-i)!i!}$ en voor $i = 1, ..., q-1$ de factor q in de teller niet weggedeeld zal worden, zullen alle termen $\binom{q}{i}$ weg vallen (voor $i = 1, ..., q-1$ dus). Hiermee is het lemma bewezen.

□

Lemma 3.1.3 (De kleine stelling van Fermat)**.** *Voor q priem en $a \in \mathbb{Z}$ geldt: $a^q \equiv a \ mod \ q$.*

Bewijs. [4] □

Lemma 3.1.4 (criterium van Euler)**.** *Er geldt: $r^{(q-1)/2} = 1 \Leftrightarrow \sqrt{r} \in \mathbb{F}_q$ voor een oneven priem q en een geheel getal r dat geen veelvoud is van q.*

($\Rightarrow$). Aannemende dat $r^{(q-1)/2} = 1$ en wetende dat er een primitieve wortel g modulo q is, zodat $\bar{g^a} = \bar{r}$ voor een bepaalde waarde van a, dan weten we: $g^{a\cdot(q-1)/2} = 1 \bmod q$ betekent precies dat $a \cdot \frac{q-1}{2}$ een veelvoud is van de orde van g. Die orde is $q-1$, dus je hebt $g^{a(q-1)/2} = 1 \Leftrightarrow q-1 \mid a \cdot \frac{q-1}{2} \Leftrightarrow \exists m : a \cdot \frac{q-1}{2} = m \cdot (q-1) \Leftrightarrow \exists m : \frac{a}{2} = m \Leftrightarrow a$ is even.
($\Leftarrow$). Aannemende dat $\sqrt{r} \in \mathbb{F}_q$, kiezen we k zodat $k^2 = r \bmod q$. Er volgt nu dat: $r^{q-1)/2} = k^{q-1} = 1 \bmod q$ (, waarbij de kleine stelling van Fermat wordt gebruikt). □

Gevolg 1. *Omdat vanwege de kleine stelling van Fermat $r^{q-1} = 1$, geldt dus dat $r^{(q-1)/2} = \pm 1$. Dus als $\sqrt{r} \in \mathbb{F}_q$, dan $r^{(q-1)/2} = 1$ en als $\sqrt{r} \notin \mathbb{F}_q$, dan $r^{(q-1)/2} = -1$, tenzij r deelbaar is door q, dan $r^{(q-1)/2} = 0$.*

Lemma 3.1.5. *$\sqrt{3} \in \mathbb{F}_q \Leftrightarrow q = 1$ mod 12 of $q = 11$ mod 12, voor een priem q.*

Bewijs. Er wordt gekeken naar een eindige uitbreiding K van $\mathbb{F}_q$ waar een element α in zit zodat $\alpha^4 - \alpha^2 + 1 = 0$. Hieruit kunnen we afleiden dat $orde(\alpha) = 12$. Namelijk als volgt: $\alpha^{12} - 1 = (\alpha^6 - 1)(\alpha^6 + 1) = (\alpha^2 + 1)(\alpha^4 - \alpha^2 + 1) = 0$. Dus $\alpha^{12} = 1$. Als we nu aan kunnen tonen dat $\alpha^4 \neq 1$ en $\alpha^6 \neq 1$, dan hebben we aangetoond dat $orde(\alpha) = 12$. Merk op dat $orde(\alpha) \neq 1$ anders geldt $1 = 0$. Als $\alpha^4 = 1$ dan hebben we vanwege de aanname dat $\alpha^2 = 2$ maar daar volgt weer uit dat $\alpha^4 = 4$, wat een tegenspraak oplevert. Als $\alpha^6 = 1$, dan heeft $\alpha^{12} - 1$ een dubbel nulpunt. Dan geldt volgens stelling 3.6.4 uit [3] dat dit ook een nulpunt is van de afgeleide van $\alpha^{12} - 1$, namelijk $12\alpha^{11}$. Oftewel: $12 \equiv 0$, of $\alpha = 0$. Dit levert weer tegenspraak. Hiermee is dus bewezen dat $orde(\alpha) = 12$.
We definieren nu het element $\beta := \alpha + \alpha^{11} \in K$. Er geldt nu:

$$\beta^2 = (\alpha + \alpha^{11})^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2 = \alpha^2 - \alpha^4 + 2 = 3. \quad (3.4)$$

Hier wordt bij de tweede gelijkheid de orde van α gebruikt, bij de vierde gelijkheid wordt gebruik gemaakt van het feit dat $\alpha^6 = -1$ en $\alpha^6 \cdot \alpha^4 = \alpha^{-2}$ en bij de laatste gelijkheid dat $\alpha^4 - \alpha^2 = -1$. Als $q = 1 \bmod 12$ of als $q = 11 \bmod 12$ dan geldt het volgende:

$$\beta^q = (\alpha + \alpha^{11})^q = \alpha + \alpha^{11} = \beta \quad (3.5)$$

Hier wordt bij de tweede gelijkheid gebruik gemaakt van lemma 3.1.2 en wederom van de orde van α en van het feit dat $\alpha^{11\cdot 11} = \alpha$ (voor het geval dat $q = 11 \bmod 12$). Vervolgens geldt, omdat $\beta^q = \beta$, dat $\beta \in \mathbb{F}_q$.
Omgekeerd kun je ook aantonen dat $\beta^q = -\beta$ als $q = 5 \bmod 12$ of als $q = 7 \bmod 12$, namelijk als volgt:

$$\beta^q = (\alpha + \alpha^{11})^q = \alpha^5 + \alpha^{-5} = \alpha^{-1} + \alpha^1 = -\beta. \quad (3.6)$$

Hierbij wordt wederom gebruik gemaakt van het feit dat $\alpha^6 = -1$ en $\alpha^{12} = 1$ en van lemma 3.1.2. Dus $\beta^q = -\beta$, wat impliceert dat $\beta \notin \mathbb{F}_q$. □

Lemma 3.1.6. $2^{(M_n-1)/2} = 1 \Leftrightarrow \sqrt{2} \in \mathbb{F}_{M_n} \Leftrightarrow M_n = 1 \ mod\ 8$ *of* $M_n = 7$ *mod* 8.

Bewijs. De eerste d.e.s.d.a. volgt direct uit het criterium van Euler. Voor de tweede d.e.s.d.a. verwijzen we naar [3]. □

Lemma 3.1.7. *Er geldt:* $M_n \equiv 7 \bmod 12$ *voor een oneven* $n > 1$.

Bewijs. $M_n = 1 \bmod 3$ en $M_n = 3 \bmod 4$. Dus $M_n = 7 \bmod 3$ en $M_n = 7 \bmod 4$, oftewel $M_n = 7 \bmod 12$. □

Gevolg 2. *Er geldt:* $3^{(M_n-1)/2} \bmod M_n = -1$ *als* M_n *priem en* > 3 *is.*

Bewijs. Met lemma 3.1.5 en lemma 3.1.7 kun je gemakkelijk alsvolgt redeneren: $\beta^2 = 3 \Rightarrow 3^{(M_n-1)/2} = \beta^{M_n-1} = -\frac{\beta}{\beta} = -1$. □

Met al deze kennis kunnen we nu een richting van de Lucas-Lehmer test bewijzen. We schrijven ω eerst om tot $((6 + 2\sqrt{3})^2)/24$. Nu kunnen we alsvolgt herleiden:

$$\begin{aligned}(6+2\sqrt{3})^{M_n} &= 6^{M_n} + 2^{M_n}\sqrt{3}^{M_n} && \text{(lemma 3.1.2)}\\ &= 6 + 2 \cdot 3^{(M_n-1)/2}\sqrt{3} && \text{(lemma 3.1.3)}\\ &= 6 + 2(-1)\sqrt{3} && \text{(lemma 3.1.4)}\\ &= 6 - 2\sqrt{3}\end{aligned} \tag{3.7}$$

Als we nu $\omega = ((6 + 2\sqrt{3})^2)/24$ substitueren, komen we tot de volgende vergelijkingen:

$$\begin{aligned}(\omega)^{(M_n+1)/2} &= \frac{(6+2\sqrt{3})^{M_n+1}}{24^{(M_n+1)/2}}\\ &= \frac{(6+2\sqrt{3})^{M_n}(6+2\sqrt{3})}{24 \cdot 24^{(M_n-1)/2}}\\ &= \frac{(6-2\sqrt{3})(6+2\sqrt{3})}{-24} \qquad \text{(vanwege 3.7) en (3.9))}\\ &= -1,\end{aligned} \tag{3.8}$$

waarbij gebruik wordt gemaakt van het volgende:

$$\begin{aligned}24^{(M_n-1)/2} &= (2^{(M_n-1)/2})^3 \cdot (3^{(M_n-1)/2})\\ &= 1^3 \cdot -1\\ &= -1\end{aligned} \tag{3.9}$$

Hier wordt bij de tweede gelijkheid gebruik gemaakt van het feit dat $M_n \equiv 7 \bmod 8$ (voor $n > 2$) en lemma 3.1.6 en gevolg 2.
Door nu bij (3.8) de eerste en de laatste term te vermenigvuldigen met

$\bar{\omega}^{(M_n+1)/4}$ en te bedenken dat $\bar{\omega} \cdot \omega = 1$, komen we tot de volgende vergelijkingen:

$$\begin{aligned}
&\omega^{(M_n+1)/2} \cdot \bar{\omega}^{(M_n+1)/4} = -\bar{\omega}^{(M_n+1)/4}, \text{ beide kanten } + \bar{\omega}^{(M_n+1)/4} \\
&\omega^{(M_n+1)/4} \cdot \omega^{(M_n+1)/4} \bar{\omega}^{(M_n+1)/4} + \bar{\omega}^{(M_n+1)/4} = 0, \text{ oftewel:} \\
&\omega^{(2^n-1+1)/4} + \bar{\omega}^{(2^n-1+1)/4} = 0, \text{ oftewel:} \\
&\omega^{2^{n-2}} + \bar{\omega}^{2^{n-2}} = 0
\end{aligned} \tag{3.10}$$

waarmee een richting van de stelling is bewezen.
($\Leftarrow$) Deze kant op zal worden bewezen door aan te nemen dat M_n geen priem is, wat tot tegenspraak zal leiden. We nemen aan dat $\omega^{2^{n-2}} + \bar{\omega}^{2^{n-2}}$ mod $M_n = 0$. Er geldt dus dat:

$$\omega^{2^{n-2}} + \bar{\omega}^{2^{n-2}} = R \cdot M_n \tag{3.11}$$

met $R \in \mathbb{Z}$. Deze vergelijking vermenigvuldigen met $\omega^{2^{n-2}}$ geeft:

$$\omega^{2^{n-1}} = \omega^{2^{n-2}} \cdot R \cdot M_n - 1. \tag{3.12}$$

Stel nu dat M_n geen priem is. We kijken dan naar de groep ${\mathbb{F}_{q^2}}^*$, waarbij q de kleinste factor van de priemfactorisatie is van M_n. Als we nu naar (3.12) kijken, zien we dat deze als $\omega^{2^{n-1}} = -1$ geschreven kan worden. Kwadrateren geeft: $\omega^{2^n} = 1$. Nu zien we dat de orde van ω in ${\mathbb{F}_{q^2}}^*$ een deler is van 2^n, maar niet van 2^{n-1}. De orde van ω is dus 2^n. Maar nu geldt er: $2^n \leq q^2 - 1 < q^2 < M_n = 2^n - 1$. Oftewel: stellen dat M_n geen priemgetal is levert een tegenspraak, ergo M_n is een priemgetal. □

3.2 Algemene test voor Wagstaff getallen

Stelling 2. *Als gegeven is dat W_n priem is en dat $S_n = S_{n-1}^2 - 2$ en S_0 mod $W_n \in \mathbb{Z}/W_n\mathbb{Z}$, dan geldt: $S_n = S_1$ mod W_n of $S_n = S_2$ mod W_n.*

Bewijs. Als $S_0^2 - 4 \equiv 0$ mod W_n of als $S_0 \in \{1, 0, -1\}$ ontstaat er een rij S_n die bij elk van deze waarden dezelfde term aanneemt vanaf maximaal de tweede term. De stelling is dan triviaal. Voor het bewijs van de andere gevallen wordt het volgende lemma gegeven:

Lemma 3.2.1. *De directe formule voor S_n is gegeven door: $S_n = \tau^{2^n} + \bar{\tau}^{2^n}$, waarbij τ en $\bar{\tau}$ oplossingen zijn van de vergelijking $x^2 - S_0 x + 1 = 0$, oftewel: $\tau = \frac{S_0 + \sqrt{S_0^2 - 4}}{2}$ en $\bar{\tau} = \frac{S_0 - \sqrt{S_0^2 - 4}}{2}$.*

Bewijs. Het bewijs gaat met volledige inductie. Eerst laten we het zien voor $n = 0$. Er geldt $S_0 = \tau + \bar{\tau} = S_0$. Dit klopt dus. Vervolgens stellen we de

inductiehypothese dat het klopt voor n. Nu zullen we bewijzen dat het dan ook voor $n+1$ ook klopt.

$$S_{n+1} = S_n^2 - 2 = (\tau^{2^n} + \bar{\tau}^{2^n})^2 - 2 = \tau^{2^n \cdot 2} + \bar{\tau}^{2^n \cdot 2} = \tau^{2^{n+1}} + \bar{\tau}^{2^{n+1}} \quad (3.13)$$

Merk op dat $\tau \cdot \bar{\tau} = 1$. □

Bovenstaand lemma zal in het vervolg veelvuldig gebruikt worden. Merk nu op dat er vanwege lemma 3.1.2 het volgende geldt:

$$\tau^{W_n} = (\frac{S_0 + \sqrt{S_0^2 - 4}}{2})^{W_n} = \frac{S_0^{W_n} + (S_0^2 - 4)^{\frac{W_n - 1}{2}} \sqrt{S_0^2 - 4}}{2^{W_n}} \quad (3.14)$$

Voordat we verder gaan met bovenstaande vergelijking, zullen we eerst het Legendre symbool introduceren.

Definitie. *[3] Laat p een oneven priemgetal zijn en $a \in \mathbb{Z}$. Dan is het Legendre symbool $(\frac{a}{p}) \in \{-1, 0, 1\}$ gedefinieerd door:*

$$\begin{array}{lll} (\frac{a}{p}) = 0 & \Leftrightarrow & a \text{ is deelbaar door } p \\ (\frac{a}{p}) = 1 & \Leftrightarrow & \exists x \in \mathbb{Z} : x \not\equiv 0 \bmod p \text{ en } x^2 = a \bmod p \\ (\frac{a}{p}) = -1 & \Leftrightarrow & \nexists x \in \mathbb{Z} : x^2 = a \bmod p \end{array}$$

We kunnen met behulp van deze definitie de laatste term van vergelijkingen van (3.14) opschrijven als: $\frac{S_0 + (\frac{S_0^2-4}{W_n})\sqrt{S_0^2-4}}{2}$, waarbij gebruik wordt gemaakt van gevolg 1 en lemma 3.1.4. We kunnen nu twee gevallen onderscheiden:
Geval 1: $(\frac{S_0^2-4}{W_n}) = 1$. Dan geldt: $\tau^{W_n} = \tau$, dus

$$\begin{aligned} \tau^{W_n - 1} &= 1 \bmod W_n, \text{ oftewel:} \\ \tau^{(2^n-2)/3} &= 1 \bmod W_n, \text{ daaruit volgt:} \\ \tau^{2^n-2} &= 1 \bmod W_n, \text{ dus} \\ \tau^{2^n} &= \tau^2 \bmod W_n. \end{aligned} \quad (3.15)$$

Dan is ook $\bar{\tau}^{2^n} = \bar{\tau}^2$, want $\bar{\tau}^m = (\frac{1}{\tau})^m = \frac{1}{t^m}$ voor elke m. Met lemma 3.2.1 volgt nu: $S_n = S_1 \bmod W_n$.
Geval 2: $(\frac{S_0^2-4}{W_n}) = -1$. Dan geldt $\tau^{W_n} = \bar{\tau}$. Dus, na beide kanten met τ te hebben vermenigvuldigd:

$$\begin{aligned} \tau^{W_n + 1} &= 1 \bmod W_n 1, \text{ oftewel:} \\ \tau^{(2^n+4)/3} &= 1 \bmod W_n \text{ en daaruit volgt:} \\ \tau^{2^n+4} &= 1 \bmod W_n, \text{ dus:} \\ \tau^{2^n} &= \tau^{-2^2} = \bar{\tau}^{2^2} \bmod W_n \end{aligned} \quad (3.16)$$

Dus na links en rechts de inverse te nemen en op te tellen, krijg je: $S_n = S_2 \bmod W_n$. Hiermee is het bewijs voor stelling 2 gegeven.

3.2.1 Maple13 programma voor de Algemene test

In deze subsectie zullen we met behulp van een Maple13 programma illustreren dat het niet uitmaakt wat je voor S_0 kiest. We kijken naar $3 \leq S_0 \leq 20$ voor $S_0 \in \mathbb{N}$. Wagstaff getallen W_n zullen worden getest op de algemene eigenschap voor $n \leq 2000$. We berekenen dus voor iedere W_n de bijbehorende S_n. Als S_n modulo W_n gelijk is aan S_2 of S_1, dan wordt als output de desbetreffende n gegeven. Zo onstaat het rijtje $3, 5, 7, ...$ Overigens wordt ook elke keer de benodigde tijd in seconden gemeten. Deze staat na $\#S = x$ voor $3 \leq x \leq 15$ weergegeven. Bij $S = 3$ is bijvoorbeeld 4.742 seconden nodig. S In het programma hieronder wordt S_0 met S aangeduid..

```
> for S from 3 to 15 do
S0 := h; S1 := S0^2-2; S2 := S1^2-2;
tijd := time();
W := (2^q+1)*(1/3);
for n from 3 to 2000 do
if isprime(n) then Wp := subs(q = n, W);
sn := S2;
for p to n-2 do sn := `mod`(sn^2-2, Wp)
end do;
if sn = `mod`(S2, Wp) then
print(n) end if;
if sn = `mod`(S1, Wp)
then print(n) end if end if end do;
eindtijd := time()-tijd;
print(eindtijd) end do;
```

```
3,5,7,11,13,17,19,23, 31, 43, 61,79, 101,127,167, 191,199, 313,347,701,1709
#S=3 4.742,
3, 3,5,7, 11,13,17, 19,23, 31, 43, 61,79, 101,127,167, 191,199, 313,347,701,1709
#S=4 4.930
3, 3,5 ,7, 11,13,17, 19,23, 31,43, 61,79, 101,127,167, 191,199, 313,347,701,1709
#S=5 4.742
3, 5 ,7, 11,13,17, 19,23, 31,43, 61,79, 101,127,167, 191,199, 313,347,701,1709
#S=6 4.914
3, 3,5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
#S=7 4.758
3, 3,5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
#S=8 4.821
3, 5,5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
#S=9 4.789
3, 3,5,5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
#S=10 4.805
3, 3,5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
```

```
#S=11 4.929
3, 5,5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
#S=12 4.789
3, 3,5,5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
#S=13 4.696
3, 3,5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
#S=14 4.727
3, 5 ,7, 11,13,17, 19,23, 31,43, 61,79,101,127,167, 191,199, 313,347,701,1709
#S=15 4.727
```

Commentaar. *Bij sommige rijtjes zie je dat er twee keer een* 3 *of* 5 *voorkomt. Dit betekent dat* $S_1 \equiv S_2 \equiv S_n$*. Overigens is* $\#S = x$ *geen output van het programma, maar dit is er later bijgezet. Voor de rest hebben we nog de gemiddelde tijd berekend over alle gebruikte* S_0*. Deze bedraagt* 4.798*.*

□

3.3 Wagstaff waarschijnlijke priem test door Robert Gerbicz

Gevolg 3. *:* W_n *is priem* $\Rightarrow S_n \equiv S_1 \ mod\ W_n$*, waarbij* $S_n = S_{n-1}^2 - 2$*, met* $S_0 = \frac{3}{2}$*.*

Voor het bewijs zal wederom allereerst eenzelfde soort lemma gegeven worden als lemma 3.1.1.

Lemma 3.3.1. S_n *wordt gegeven door de volgende directe formule:* $S_n = \psi^{2^k} + \bar{\psi}^{2^k}$*, waarbij* $\psi = \frac{3+\sqrt{-7}}{4}$ *en* $\bar{\psi} = \frac{3-\sqrt{-7}}{4}$*.*

Bewijs. Als je bij lemma 3.1.1 $S_0 = \frac{3}{2}$ invult bij de functie van τ, dan krijg je het bewijs voor dit lemma. □

We zullen nu een stelling en een lemma geven om het bewijs van Gevolg 3 voor te zetten:

Lemma 3.3.2. *Er geldt* $(\frac{nm}{p}) = (\frac{n}{q}) \cdot (\frac{m}{q})$

Bewijs. Voor het bewijs zie dictaat algebra. □

Stelling 3 (kwadratische reciprociteitswet (Gauss, 1801))**.** *Als* p *en* q *verschillende oneven priemgetallen zijn, dan geldt:*

$$(\tfrac{q}{p}) = \quad (\tfrac{p}{q}) \quad als\ p \equiv 1\ mod\ 4\ of\ q \equiv 1\ mod\ 4$$

$$(\tfrac{q}{p}) = \quad -(\tfrac{p}{q}) \quad als\ p \equiv q \equiv 3\ mod\ 4$$

Bewijs. Zie dictaat algebra. □

Nu vervolgen we als volgt:

Lemma 3.3.3. *Er geldt:* $(-7)^{(W_p-1)/2} = 1 \ mod \ W_p$

Bewijs. Met behulp van de definitie van het Legendre symbool kunnen we lemma 3.3.3 als volgt noteren: $(\frac{-7}{W_p}) \equiv 1$. Dit kunnen we met behulp van bovenstaande eigenschap van het legendre symbool en de reciprociteitsstelling als volgt bewijzen: $(\frac{-7}{W_p}) = (\frac{7}{W_p})(\frac{-1}{W_p}) = (\frac{W_p}{7})(\frac{-1}{W_p}) = (\frac{-1}{7})^2 \cdot 1 = 1$. □

Het bewijs van Gevolg 3 gaat nu als volgt: vanwege lemma 3.3.3 geldt: $\psi^{W_n} = \psi \bmod W_p$. Passen we nu Geval 1 van de algemene stlling toe, dan is daarmee het bewijs van dit gevolg gegeven.

3.3.1 Maple13 Programma voor de Gerbics test

In het programma hieronder wordt wederom S_n berekend. Dan wordt S_n modulo W_n vergeleken met S_1. Mochten deze waardes gelijk zijn, dan wordt de betreffende n weergegeven als output. (Dit geeft het rijtje: $3, 5, 7, 11, ...$). Als laatste output staat nog de tijd die de computer nodig had de berekeningen te maken (3.848 seconden).

```
> tijd := time();
W := (2^q+1)*1/3;
S0 := 3/2; S1 := S0^2-2; for n from 3 to 2000
do if isprime(n) then Wp := subs(q = n, W);
sn := 1/4; b := n-1;
for p to b do
sn := `mod`(sn^2-2, Wp)
end do;
if sn = `mod`(S1, Wp)
then print(n)
end if end if end do;
eindtijd := time()-tijd;
print(eindtijd);
3,5,7,11,13, 17,19,23,31,43,61,79,101,127,167,191, 199, 313, 347, 701,1709
3.848
```

3.4 Wagstaff waarschijnlijke priemtest door Anton Vrba

Gevolg 4 (Anton Vrba test)**.** *W_n is priem $\Rightarrow S_n \equiv S_2 \ mod \ W_n$, waarbij $S_0 = 6$ en $S_n = S_{n-1}^2 - 2$.*

Bewijs. Het bewijs van de test van Anton Vrba is een voorbeeld van geval 2 van de algemene stelling. We nemen wederom aan dat W_n priem is en

we definieren nu $\mu := 3 + 2\sqrt{2}$ en $\bar{\mu} := 3 - 2\sqrt{2}$. (Dit zijn dus eigenlijk τ en $\bar{\tau}$, respectievelijk, met $S_0 = 6$ ingevuld.) Voor de stelling moet worden aangetoond dat $S_n \equiv S_2 \bmod W_n$. Als we dus kunnen laten zien dat $\mu^{W_n} = \bar{\mu}$, dan kunnen we geval 2 van de algemene stelling toepassen, waarmee direct het bewijs gegeven is. Nu wil het zo zijn dat we dit kunnen laten zien, namelijk als volgt:

$$\begin{aligned} \mu_n^W &= (3 + 2\sqrt{2})^{W_n} \\ &= 3^{W_n} + 2^{W_n} \cdot 2^{(W_n-1)/2} \cdot \sqrt{2} && \text{(lemma 3.1.2)} \\ &= 3 + 2 \cdot -1 \cdot \sqrt{2} && \text{(lemma 3.1.3 en 3.1.6)} \\ &= \bar{\mu}, \end{aligned} \tag{3.17}$$

N.B.: bij de toepassing van lemma 3.1.6 wordt gebruik gemaakt van het feit dat $W_n \equiv 3 \bmod 8$ als $n > 2$. Dit geldt omdat $W_n \bmod 8 = (3^{-1}) \bmod 8 \cdot 1 \bmod 8 = 3 \bmod 8$. □

3.4.1 Maple13 programma voor Anton Vrba's test

In het programma wordt weer S_n berekend. Deze wordt ditmaal vergeleken met S_2. Mochten deze waardes, modulo W_n, gelijk zijn, dan wordt de betreffende n weergegeven als output. (Dit geeft het rijtje: $3, 5, 7, 11, ...$). Als laatste output staat nog de tijd die de computer nodig had de berekeningen te maken (3.888 seconden).

```
> tijd := time();
W := (2^q+1)*1/3;
for n from 3 to 2000
do if isprime(n) then Wp := subs(q = n, W);
sn := 1154; r := n-2;
for p to r do
sn := `mod`(sn^2-2, Wp)
end do;
a := sn;
if sn = `mod`(1154, Wp) then print(n)
end if end if end do;
eindtijd := time()-tijd;
print(eindtijd);
3, 5, 7, 11,13,17,19,23,31,43,61,79,101,127,167,191,199,313,347,701,1709
3.888
```

3.5 Wagstaff waarschijnlijke priem test door Renaud en Henri Lifschitz

Stelling 4. *Gegeven dat W_n priem is, $c \in (\mathbb{Z}/W_n\mathbb{Z})^*$, $3 \leq c \leq W_n - 1$ en c^2 mod $W_n = b$, dan geldt: $b^{2^n} \equiv b^2$ mod W_n*

Bewijs. Er geldt: $b^{2^{n-1}} = \bar{c}^{2^n} = \bar{c}^{3W_n-1} = \bar{c}^3 \cdot \bar{c}^{-1} = b$. Hierbij wordt de Kleine stelling van Fermat (lemma 3.1.3) gebruikt bij het derde gelijkteken. □

Commentaar. *Stelling 4 geldt overigens ook voor $c = 1$ en $c = 2$, maar hierbij wordt niet gebruikt dat W_n priem is. Stel $c = 1$. Nu geldt de stelling gewoonweg omdat alle machten van 1 gelijk zijn aan 1. Stel $c = 2$. De orde van 2 in $(\mathbb{Z}/W_n\mathbb{Z})^*$ is $2p$ (zie eigenschap 4). Verder geldt ook vanwege lemma 3.1.3 dat $2^n = 2 + n \cdot k$, voor een even k. Dus geldt: $b^{2^{n-1}} = 2^{2^n} = 2^2 \cdot 2^{nk} = 4 \cdot 1 = 4$ Hierbij wordt dus ook niet gebruik gemaakt van het feit dat W_n priem is. Overigens geldt dit dus ook voor $c = 4$.*

3.5.1 Maple13 programma voor Lifschitz test

We zullen in deze paragraaf met een Maple programma illustreren hoe je de Lifschitz-test kunt gebruiken. In dit programma wordt $25^{2^{n-1}}$ berekend, oftewel: we nemen $b = 5$. Er wordt gekeken of deze gelijk is (modulo $\frac{2^n+1}{3}$) aan 25. Zo ja, dan wordt deze n weergegeven als output. Zie wederom het rijtje $3, 5, 7, ...$ Als laatste is wederom de tijd gegeven die de computer nodig had om de berekening uit te voeren (4.020 seconden).

```
> tijd := time();
W := (2^q+1)*1/3;
b := 5; for n from 3 to 2000 do
if isprime(n) then
Wq := subs(q = n, W);
a := 25;
for p to n-1 do
a := `mod`(a^2, (2^n+1)*1/3)
end do;
if modp(25, Wq) = modp(a, Wq)
then print(n) end if
end if end do;
eindtijd := time()-tijd;
print(eindtijd);
3,5,7,11,13,17,19,23,31,43,61,79,101,127,167,191,199,313,347,701,1709
4.020
```

3.6 Conclusie

Concluderend kunnen we stellen, dat er bij de 4 testen allemaal dezelfde waarden voor n als output gegeven worden. Voor alle getallen n die in de output in dit rijtje staan, is al bewezen dat de bijbehorende W_n priem zijn. We achten het daarom erg waarschijnlijk dat het doorstaan van een der testen door W_n voldoende is om de primaliteit ervan aan te tonen. Verder zien we dat de hoeveelheid tijd die nodig is voor Anton Vrba's, Robert Gerbicz' en Renaud en Henri Lifschitz' test respectievelijk $3.888, 3.848$ en 4.020 bedraagt. Oftewel: deze tests hebben vrijwel dezelfde snelheid. De gemiddelde tijd voor de waarden voor $3 \leq S_0 \leq 15$ die nodig is voor de algemene test is 4.798 seconden. Het tijdsverschil is te wijten aan het feit dat S_n bij de algemene test wordt vergeleken met S_0 en S_1, terwijl S_n bij de Vrba en Gerbicz slechts met 1 waarde wordt vergeleken, net zoals er bij de test van Lifschitz ook slechts twee waarden worden vergeleken.

Hoofdstuk 4

Primaliteitsbewijzen

In dit hoofdstuk zullen we de primaliteit van een aantal Wagstaff-getallen aantonen.

4.1 Bewijs van primaliteit van W_{101}

Stelling 5. *$W_{101} = \frac{2^{101}+1}{3}$ is priem.*

Bewijs. We zullen de primaliteit aan tonen met behulp van het volgende lemma:

Lemma 4.1.1. *$\#(\mathbb{Z}/W\mathbb{Z})^* = W - 1 \Leftrightarrow W$ is priem, voor $W \in \mathbb{Z}_{\geq 2}$.*

($\Rightarrow$). Als voor $W-1$ getallen $x \in (\mathbb{Z}/W\mathbb{Z})^*$ geldt dat: $ggd(x, W) = 1$, dan betekent dit dat W geen delers heeft en dus priem is.
($\Leftarrow$). Als W priem is betekent dit dat $ggd(x, W) = 1$ voor alle $x \in (\mathbb{Z}/W\mathbb{Z})$, behalve voor $x = 0$, oftewel: er zitten $W - 1$ elementen in $(\mathbb{Z}/W\mathbb{Z})^*$. □

We weten dus nu dat als we een element $y \in (\mathbb{Z}/W_{101}\mathbb{Z})^*$ met $orde(y) = W_{101} - 1$ kunnen vinden dan geldt, omdat $orde(y) \leq \#(\mathbb{Z}/W_{101}\mathbb{Z})^*$ en $max(\#(\mathbb{Z}/W_{101}\mathbb{Z})^*) = W_{101} - 1$, dat W_{101} priem is. We zullen nu kijken naar de orde van 3 in $(\mathbb{Z}/W_{101}\mathbb{Z})^*$. Vanwege stelling 4 geldt $3^{2^{101}} \equiv 9 \mod W_{101}$. Nu hebben we met maple berekend dat $3^{2^{100}} \mod W_{101} = 3$. Hier volgt uit dat $3^{2^{100}-1} = 1 \mod W_{101}$. Nu geldt uiteraard het volgende lemma:

Lemma 4.1.2. *Gegeven een groep G, met een element $x \in G$. Als $x^n = 1$ dan $orde(x) \mid n$*

Bewijs. [4] □

Oftewel: de orde van 3 is een deler van $2^{100} - 1$. Om te vinden welke deler dit is, zullen we met behulp van Maple kijken naar de priemfactorisatie van $2^{100} - 1$.

```
> p := 101; orde := 2^(p-1)-1; lengte := 12; basis := 3;
if ‘mod‘(‘&^‘(basis, 2^(p-1)), (2^p+1)*(1/3)) = basis then
z := basis else z := -basis end if;
for n to lengte do
a := ifactors(2^(p-1)-1)[2][n][1];
b := ‘mod‘(‘&^‘(z, (2^(p-1)-1)/a), (2^p+1)*(1/3));
if b = 1 then orde := ifactor(orde/a)
end if end do;
print(orde); print(ifactor(2^(p-1)-1));

(5)^3  (11) (31) (41) (101) (251) (601) (268501) (8101) (4051) (1801)
(3) (5)^3  (11) (31) (41) (101) (251) (601) (268501) (8101) (4051) (1801)
```

Het programma bekijkt dus voor alle 12 priemfactoren p_i of ze weggelaten kunnen worden, terwijl 3 tot de macht de factorisatie zonder p_i toch 1 blijft. Je ziet in de output dat voor W_{101} geldt dat 3 het enige getal is dat je uit de factorisatie kan halen, mits 3 tot de macht de factorisatie 1 blijft. Oftewel: de orde van 3 in $(\mathbb{Z}/W_{101}\mathbb{Z})^*$ is $\frac{2^{100}-1}{3}$. Aangezien dit precies gelijk is aan $\frac{W-1}{2}$, hebben we een element nodig met een twee maal zo grote orde om lemma 4.1.1 te te gebruiken. We maken nu gebruik van het volgende lemma:

Lemma 4.1.3. *Als G een abelse groep is en $g, h \in G$ en $ggd(orde(g), orde(h)) = 1$ dan volgt $orde(gh) = orde(g) \cdot orde(h)$.*

Bewijs. [4] □

Aangezien $ggd(orde(-1), orde(3)) = 1$ en $orde(-1) = 2$, geldt: $orde(-3) = 2 \cdot orde(3) = W_n - 1$. Er zit dus een element met orde $W_n - 1$ in $(\mathbb{Z}/W_n\mathbb{Z})^*$. Hieruit volgt dus vanwege (4.1.1) dat W_{101} priem is. □

4.2 Bewijs van primaliteit van W_{1709}

Stelling 6. *$W_{1709} = \frac{2^{1709}+1}{3}$ is priem.*

Bewijs. We gaan hier hetzelfde te werk als bij W_{101}. We weten vanwege het bewijs van stelling 4 dat er een c in $(\mathbb{Z}/W_{1709}\mathbb{Z})^*$ bestaat zodat $c^{2^{1708}-1}$ mod $W_{1709} \equiv 1$. Met behulp van Maple13 hebben we gevonden dat $3^{2^{1708}} = 3$, oftewel: $3^{2^{1708}-1} = 1$. Om de orde van 3 te vinden moeten we dus op zoek naar de factorisatie van $2^{1708} - 1$. Hierover kunnen we het volgende stellen: $2^{1708} - 1 = (2^{854} + 1)(2^{854} - 1)$. Verder weten we dat $2^{854} - 1 = (2^{427} + 1)(2^{427} - 1)$. Deze twee termen kunnen we allebei vinden in de Cunningham Tables. De term $(2^{854} + 1)$ kunnen we ook nog in de Cunningham Tables vinden. Bij deze term wordt overigens nog gebruik gemaakt van het feit 854 een getal is van de vorm $4 \cdot k + 2$ voor $k \in \mathbb{N}$. Er kan dan namelijk

gebruik gemaakt worden van de volgende factorisatie [10]: $(2y^2)^2 + 1 = (2y^2 - 2y + 1)(2y^2 + 2y + 1)$. Hier bij is y dus 2^{213}. De volledige factorisatie van $2^{1708} - 1$ ziet er nu als volgt uit:

```
5124001*117955793453*581734233397519028692308134729144162832 29*
700853105860613436635135420807573041760568706 1*
370393844845927760114962950169816222976285440258519929 41*
755329623338365767690003976874558819319370593128035091773*
733*368140581013*667055378149*3456749*1709*29*113*5*3*43*
768614336404564651*2305843009213693951*33282089*127*
453889188212439220765312640491855058688001924855077127131818185 63*
57461778571*13402353088548115060442057393947 87*
(355601934129723190620617682616397275174784999141
675484960316882805849770775621916710592232824694659 59)
```

Met behulp van Maple13 hebben we $3^{(2^{1708}-1)/p_i} \bmod W_{1709}$ berekend, waarbij p_i, met $1 \leq i \leq 24$, de priemfactoren van $2^{1708} - 1$ zijn. Alleen voor $p_{14} = 3$ is de uitkomst 1. Voor alle andere p_i kwam er een andere uitkomst uit. Dit betekent dus dat $orde(3) = (2^{1708} - 1)/3 = \frac{W_{1709}-1}{2}$. Dus als we nu kijken naar het element -3 en lemma 4.1.3 gebruiken, kunnen we concluderen dat $orde(-3) = W_{1709} - 1$ en dus dat W_{1709} priem is.

□

4.3 Twee manieren om te bewijzen dat W_{701} priem is

Stelling 7. *$W_{709} = \frac{2^{709}+1}{3}$ is priem.*

Bewijs. Deze keer gaan we twee methodes toepassen:
Methode 1. We zullen voor de eerste methode wederom gebruik maken van vergelijking 4.1.1. Vanwege het bewijs van stelling 4 geldt: $5^{2^{701}} = 25$. Hieruit volgt, analoog aan wat bij de stelling 5 gebeurt, waarbij wederom gebruik wordt gemaakt van Maple13, dat $5^{2^{700}-1} = 1$, oftewel: de orde van 5 is een deler is van $2^{700} - 1$. Het gaat dus om het factoriseren van $2^{700}-1$. Dit hebben we met Maple kunnen doen met behulp van onderstaand programma:

```
> p := 701;
orde := 2^(p-1)-1; lengte := 32; basis := 5;
 if `mod`(`&^`(basis, 2^(p-1)), (2^p+1)*1/3) = basis then
z := basis else z := -basis end if;
for n to lengte do
a := ifactors(2^(p-1)-1)[2][n][1];
b := `mod`(`&^`(z, (2^(p-1)-1)/a), (2^p+1)*1/3);
if b = 1 then
```

```
orde := ifactor(orde/a)
end if
end do;
print(orde);
print(ifactor(2^(p-1)-1));

(5)^3  (11) (29) (31) (41) (43) (71) (101) (113) (127) (251) (281)
(601) (701) (1051) (2430065924693517198550322751963101)
(10382137934478419409082933558714614 01) (347833278451)
(34010032331525251) (535347624791488552837151) (60816001)
(39551) (110251) (268501) (8101) (4051) (1801) (47392381) (7416361)
(86171) (122921)

(3) (5)^3  (11) (29) (31) (41) (43) (71) (101) (113) (127) (251) (281)
(601) (701) (1051) (2430065924693517198550322751963101)
(10382137934478419409082933558 71461401) (347833278451)
(34010032331525251) (535347624791488552837151) (60816001)
(39551) (110251) (268501) (8101) (4051) (1801) (47392381) (7416361)
(86171) (122921)
```

Je ziet dat de orde van 5 gelijk is aan $\frac{2^{700}-1}{3}$. (Merk op dat 3 ook precies het getal is dat in de bovenste van de twee factorisaties niet voorkomt.) Dit is weer gelijk aan $\frac{W_n-1}{2}$. Wederom gebruik makende van lemma 4.1.3, kunnen we concluderen dat $orde(-5) = W_n - 1$. Nu volgt vanwege dezelfde argumenten als bij stelling 5 dat W_{701} priem is. □

De vraag is nu hoe groot de n van de W_n kan worden, mits de factorisatie van $2^{n-1} - 1$ te vinden is. Voor de factorisatie van grote getallen van de vorm $2^q \pm 1$, met $q \in \mathbb{N}$ kan je goed gebruik maken van de 'Cunningham Tables' [8]. Deze tabellen bevatten alle factorisaties van $2^q \pm 1$ voor $q \leq 1199$ en oneven. Merk op dat $2^q - 1$ voor een even q direct te factoriseren is als $(2^{q/2} + 1)(2^{q/2} - 1)$. Dus als q even is, is de grootste factorisatie die je nodig hebt $(2^{q/2} + 1)$. Aangezien je met methode 1 op zoek bent naar de factorisatie van $2^{n-1} - 1$ voor een priem n, kun je dus concluderen dat je met behulp van de Cunningham Tables factorisaties van $2^{n-1} - 1$ kan krijgen voor $n \leq 2399$. Dit betekent dus dat je voor Wagstaff-getallen W_n met $n \leq 2399$ de primaliteit kan bewijzen met behulp van deze tabellen. De grootste Wagstaff-priem kleiner dan $\frac{2^{2399}+1}{3}$ is $\frac{2^{1709}+1}{3}$. Dus alle Wagstaff-priemen die je met de Cunningham tabellen kan vinden, staan in de tabel op pagina 2.

Methode 2. Voor de tweede methode zullen we eerst een aantal dingen introduceren. Vervolgens zullen we een stelling poneren die helpt de primaliteit van W_{701} aan te tonen.

Gegeven is dat $W > 1$ en oneven. Verder $s \in \mathbb{Z}$ met $ggd(s^2 - 4, W) = 1$ en $\bar{s} = s \bmod W \in \mathbb{Z}/W\mathbb{Z}$. Nu definieren we: $R = (\mathbb{Z}/W\mathbb{Z}[x])/(x^2 - sx + 1)$. Dit is een ring. Elk element van R is op een unieke manier te schrijven als: $a + bx \bmod (x^2 - sx + 1)$, voor $a, b \in \mathbb{Z}/W\mathbb{Z}$. Nu geven we de volgende definitie:

Definitie. *$N : R \longrightarrow \mathbb{Z}/W\mathbb{Z}$ door $a + bx$ mod $(x^2 - sx + 1) \mapsto a^2 + abs + b^2$ mod $(x^2 - sx + 1)$.*

Lemma 4.3.1. *$N(\alpha\beta) = N(\alpha) \cdot N(\beta)$, met $N(1) = 1$.*

Bewijs. We nemen de elementen $\alpha = a + bx$ en $\beta = c + dx$. Dus er geldt: $\alpha \cdot \beta = ac + bdx^2 + (ad + bc)x = ac + bd(sx - 1) + (ad + bc)x = ac - bd + (ad + bc + bds)x$. Nu vullen we deze term in, in de norm. We krijgen:

$$N(\alpha, \beta) = (ac - bd)^2(ac - bd)(ad + bc + bds)s + (ad + bc + bds)^2.$$

Haakjes wegwerken geeft:

$$a^2c^2 + b^2d^2 + acbds^2 + ac^2bs + a^2cds + a^2d^2 + ad^2bs + b^2c^2 + b^2cds.$$

We moeten dus uitkomen op $N(\alpha) \cdot N(\beta) =$

$$\begin{aligned} &= (a^2 + abs + b^2)(c^2 + cds + d2) \\ &= a^2c^2 + b^2d^2 + acbds^2 + ac^2bs + a^2cds + a^2d^2 + ad^2bs + b^2c^2 + b^2cds. \end{aligned} \tag{4.1}$$

We zien dat $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ en het bewijs is gegeven. □

Gevolg 5. *Als $\alpha \in R^*$, dan $N(\alpha) \in (\mathbb{Z}/W\mathbb{Z})^*$.*

Gevolg 6. *$N : R^* \longrightarrow (\mathbb{Z}/W\mathbb{Z})^*$ is een homomorfisme van groepen.*

Gevolg 7. *$G := \{\alpha \in R^* \mid N(\alpha) = 1\}$ is een ondergroep van R^*.*

Stelling 8. *Als G een element α bevat met $orde(\alpha) = W + 1$ dan is W priem.*

Bewijs. Stel $p^e \mid W$, maar $p^{e+1} \not| W$. Nu gaan we kijken naar hetvolgende homomorfisme:

$$R^* \longrightarrow ((\mathbb{Z}/p^e\mathbb{Z}[x])/(x^2 - sx + 1))^* \tag{4.2}$$

Dit homomorfisme stuurt de kern van de Norm naar de kern van de Norm. Het beeld van α noemen we α_p. Vanwege de chinese reststelling geldt er nu:

$$W + 1 = orde(\alpha) = kgv(orde(\alpha_p)). \tag{4.3}$$

Met $kgv(orde(\alpha_p))$ wordt de kleinste gemene veelvoud bedoeld van alle α_p's over de priemen p die W delen.
We kunnen vervolgens tellen hoeveel elementen er in $((\mathbb{Z}/p^e\mathbb{Z}[x])/(x^2 - sx + 1))^*$ zitten.

Lemma 4.3.2. *Het aantal elementen Q in de kern van de norm van $((\mathbb{Z}/p^e\mathbb{Z}[x])/(x^2 - sx + 1))^*$ naar $(\mathbb{Z}/p^e\mathbb{Z})^*$ is gegeven door:*

$$Q = p^{e-1}(p - (\frac{s_0^2 - 4}{p})) \tag{4.4}$$

Bewijs. We zullen voor het bewijs eerst kijken naar het aantal elementen van Q als $e = 1$, genoteerd als Q_1. Dus: $Q_1 = \#\{(a, b) \in \mathbb{Z}/p\mathbb{Z} \mid a^2 + abs + b^2 = 1\}$. Allereerst weten we dat $(1, 0) \in Q_1$, want $1^2 + 0 + 0^2 = 1$. Vervolgens kunnen we $a^2 + abs + b^2 = 1$ als figuur beschouwen, bijvoorbeeld als ellips. Kijken we nu naar de lijn door $(1, 0)$ met richtingscoefficient ∞ dan $a = 1$ en dus $bs + b^2 = 0$, oftewel: $b(b - s) = 0$. Maar $b = 0$ hebben we al en dus vinden we als ander punt op de ellips $(1, -s)$. Nu gaan we kijken naar alle mogelijke lijnen door het punt $(1, 0)$. We stellen daarvoor $y = r(x - 1)$. De punten waar we naar op zoek zijn voldoen dus aan $a^2 + abs + b^2 = 1$ en aan $y = r(x-1)$. Dus we vervangen nu a voor x en b voor y en we substitueren. Dit geeft:

$$\begin{aligned} 0 &= x^2 + xr(x - 1)s + r^2 \cdot (x - 1)^2 - 1 = \\ &= (x - 1)(x + 1 + xrs + r^2(x - 1)) = \\ &= (x - 1)(1 - r^2 + x(r^2 + rs + 1)) \end{aligned} \tag{4.5}$$

Nu zijn er drie mogelijkheden:

1. Het polynoom $x^2 - sx + 1$ is irreducibel. Gevolg: kijkend naar de laatste term van 4.5 en wetende dat we niet op zoek zijn naar het nulpunt $x = 1$, zien we dat we voor de andere oplossingen hebben: $x = \frac{r^2-1}{r^2+rs+1}$. Aangezien dit alles in $\mathbb{Z}/p\mathbb{Z}$ plaatsvindt, kan r, als richtingscoefficient, maar p waardes aannemen. Omdat er ook een lijn aan de ellips raakt en dus de ellips niet nog ergens anders snijdt, zijn dit nog $p - 1$ punten. Uiteindelijk hebben we dus $p - 1 + 2 = p + 1$ punten die aan $a^2 + abs + b^2 = 1$ voldoen.

2. Het polynoom $x^2 - sx + 1$ is een kwadraat. Gevolg: $s^2 - 4 = 0$, dus $s = 2$ of $s = -2$, maar we nemen aan dat $ggd(W, s) = ggd(W, s + 2) = ggd(W, s - 2) = 1$ en dus $s = 2$ of $s = -2$ geeft tegenspraak.

3. Het polynoom $x^2 - sx + 1$ heeft 2 nulpunten in $\mathbb{F}_p$, maar ± 1 is niet een van deze nulpunten. Gevolg: net als in het irreducibele geval geldt de vergelijking $x = \frac{r^2-1}{r^2+rs+1}$. Wederom hebben we de twee punten $(1, 0)$ en $(1, -s)$. Nu missen we echter nog twee punten omdat $r^2 + rs + 1$ twee keer de waarde nul aanneemt. Bovendien kan r geen $\frac{-2}{s}$ zijn, dus hebben we nog een oplossing minder. Er zijn dus $2 + p - 1 - 2 = p - 1$ oplossingen.

Nu zullen we kijken naar het geval $e = 2$. Dus stel $(a, b) \in \mathbb{Z}^2$ is een oplossing mod p. We willen nu c, d zodat $(a + pc, b + pd)$ een oplossing mod p^2 is. We weten:

$$a^2 + abs + b^2 = 1 + k \cdot p.$$

Substitutie geeft:

$$(a + pc)^2 + (a + pc)(b + pd)s + (b + pd)^2 \equiv 1 \bmod p^2,$$

oftewel:

$$p(2ac + k + ads + bcs + 2bp) \equiv 0 \bmod p^2.$$

We willen dus eigenlijk (c, d) zodat:

$$c(2a + bs) + d(as + 2b) \equiv -k \bmod p. \tag{4.6}$$

Hier zijn oplossingen voor, behalve als $2a + bs = 0$ en $as + 2b = 0$, want: $\left(\begin{smallmatrix} 2 & s \\ s & 2 \end{smallmatrix}\right)\binom{a}{b} = \binom{0}{0} \Leftrightarrow (a, b) = (0, 0)$, maar $a^2 + abs + b^2 \neq 0$, dus dit gebeurt niet. We zien nu dat het aantal oplossingen p maal zo veel is geworden en dus:

$$Q_2 = p(p - 1).$$

Nu kunnen we met inductie de rest van het bewijs geven, namelijk als volgt: stel je neemt aan dat $Q_e = p^{e-1} \cdot Q_1$. Nu willen we Q_{e+1} bepalen. Dus stel $(a, b) \in \mathbb{Z}^2$ is een oplossing mod p^e. Dan geldt:

$$a^2 + abs + b^2 = 1 + k \cdot p^e.$$

Hiervan proberen we een oplossing mod p^{e+1} te maken. We willen (c, d) zodat: $(a + p^e c, b + p^e d)$ oplossingen oplevert. Substitutie geeft:

$$(a + p^{e-1}c)^2 + (a + p^{e-1}c)(b + p^{e-1}d)s + (b + p^{e-1}d)^2 \equiv 1 \bmod p^e,$$

oftewel:

$$(2ac + k + ads + bcs + 2bp) \equiv 0 \bmod p.$$

Deze vergelijking heeft net als (4.6) wederom p oplossingen. Dus het aantal oplossingen wordt wederom vermenigvuldigd met p. Hiermee is aangetoond dat $Q_{e+1} = p \cdot Q_e = p^e \cdot Q_1$. Zoals eerder aangegeven zijn er dus 3 mogelijkheden voor het polynoom $x^2 - sx + 1$. Als $x^2 - sx + 1$ irreducibel is, volgt hieruit dat $(\frac{s^2-4}{3}) = -1$, als $x^2 - sx + 1$ reducibel is volgt hieruit dat $(\frac{s^2-4}{3}) = 1$ en als $x^2 - sx + 1$ een kwadraat is dan volgt dat $(\frac{s^2-4}{3}) = 0$. Zo komen we dus tot de conclusie dat $Q = p^{e-1}(p - (\frac{s_0^2-4}{p}))$. □

Er geldt dus vanwege lemma 4.1.2 dat $orde(\alpha_p)$ zowel een deler is van $W + 1$ als van $p^{e-1}(p - (\frac{s^2-4}{p}))$ en dus omdat $p \not| W + 1$ is $orde(\alpha_p)$ een deler van $ggd(p^{e-1}(p - (\frac{s^2-4}{p})), W + 1) = ggd((p - (\frac{s^2-4}{p})), W + 1)$. Deze laatste

gelijkheid geldt vanwege het feit p^{e-1} geen deler van $W+1$ is. In het bijzonder is dus $orde(\alpha_p)$ een deler van $(\frac{s^2-4}{p})$. Hieruit voglt dat $W+1 = kgv(orde(\alpha_p))$ een deler is van $kgv(p-(\frac{s^2-4}{p}))$. We schrijven nu:

$$W = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_t^{e_t} \tag{4.7}$$

met alle p_j priemgetallen en alle $e_j > 0$ en $p_1 < p_2 < ... < p_t$. Nu kunnen we als volgt te werk gaan:

$$\begin{aligned} 1 + (p_1 \cdot ... \cdot p_t) \leq W+1 &= kgv(orde(\alpha_{p_1}), orde(\alpha_{p_2}), ..., orde(\alpha_{p_t})) \\ &\leq kgv(p_1 - (\frac{s^2-4}{p_1}), p_2 - (\frac{s^2-4}{p_2}), ..., p_t - (\frac{s^2-4}{p_t})) \\ &= 2 \cdot kgv(\frac{p_1 - (\frac{s^2-4}{p_1})}{2}, \frac{p_2 - (\frac{s^2-4}{p_2})}{2}, ..., \frac{p_t - (\frac{s^2-4}{p_t})}{2}) \\ &\leq (p_1+1) \cdot \frac{p_2+1}{2} \cdot \frac{p_3+1}{2} \cdot \frac{p_4+1}{2} \cdot ... \cdot \frac{p_t+1}{2} \\ &\leq \frac{p_1 \cdot p_2 \cdot ... \cdot p_t}{2^{t-1}} + \frac{1}{2^{t-1}} + 2^t \cdot \frac{p_2 \cdot ... \cdot p_t}{2^{t-1}} \end{aligned} \tag{4.8}$$

Merk bij de afschatting naar $(p_1+1) \cdot \frac{p_2+1}{2} \cdot \frac{p_3+1}{2} \cdot \frac{p_4+1}{2} \cdot ... \cdot \frac{p_t+1}{2}$ op dat $(\frac{s_0^2-4}{p_i})$ de waarde $-1, 0$ of 1 kan aannemen. Verder worden bij de laatste ongelijkheid in $(p_1+1) \cdot \frac{p_2+1}{2} \cdot \frac{p_3+1}{2} \cdot \frac{p_4+1}{2} \cdot ... \cdot \frac{p_t+1}{2}$ de haakjes weggewerkt. Dit levert het product $p_1 \cdot ... \cdot p_t$ op, evenals het product 1 en dan nog $2^t - 2$ producten $p_{i_1} \cdot ... \cdot p_{i_s}$, waarbij $1 \leq s < t$ en $i_1 < i_2 < ... < i_s$.
Als we nu de meest linker en rechter term van 4.8 gebruiken, komen we tot:

$$\frac{(2^{t-1}-1)(((p_1) \cdot ... \cdot p_t)+1)}{2^{t-1}} \leq 2 \cdot p_2 \cdot ... \cdot p_t. \tag{4.9}$$

en dus geldt:

$$\frac{2^{t-1}-1}{2^{t-1}}(p_1 + \frac{1}{p_2 \cdot ... \cdot p_t}) \leq 2. \tag{4.10}$$

Nu gaan we als volgt te werk om tot de conclusie te komen dat $t = 1$. Stel $t \geq 3$: er geldt nu dat $\frac{3}{4} \leq \frac{2^{t-1}-1}{2^{t-1}}$ en dus $\frac{3}{4}(p_1 + \frac{1}{p_1 \cdot ... \cdot t}) \leq \frac{2^{t-1}-1}{2^{t-1}}(p_1 + \frac{1}{p_1 \cdot ... \cdot t}) \leq 2$ dus $p_1 + \frac{1}{p_2 \cdot ... \cdot p_t} \leq \frac{8}{3}$. Oftewel: $p \leq 2$, maar aangezien W oneven is vanwege Eigenschap 1 is geeft $p = 2$ een tegenspraak. Stel $t = 2$: dan hebben we $p_1 \cdot p_2 + 1 \leq (p+1)\frac{p+1}{2} = \frac{1}{2}(p_1 \cdot p_2 + 1 + p_1 + p_2)$ en dus $p_1 \cdot p_2 + 1 \leq p_1 + p_2$, oftewel $(p_1 - 1)(p_2 - 1) \leq 0$. Maar aangezien $p_j > 1$ per definitie, geeft dit wederom tegenspraak. Kortom: $t = 1$. Dit geeft vervolgens: $W = p^e$ met p priem en $e \geq 1$. In dit geval weten we: $W + 1 = orde(\alpha) = orde(\alpha_p)$ is een deler van $p - (\frac{s^2-4}{p})$, dus $p^e + 1 \leq p + 1$. Dus $e = 1$ en $W = p$ is priem. □

Gebruik makende van stelling 8, kunnen we nu op een andere manier aantonen dat W_{701} priem is. Eerst maken we ook gebruik van de algemene

stelling. Deze stelling stelt namelijk dat er voor een $x \in \mathbb{Z}/W_{701}\mathbb{Z}$ geldt dat $x^{2^n} \equiv x^2$ of $x^{2^n} \equiv x^{-4}$. Wetende dat er voor een $x \in \mathbb{Z}/W_{701}\mathbb{Z}$ het laatste geldt, volgt er dat $x^{2^n+4} = 1$. Nu gaat het er dus om 2^n+4, oftewel $2^{n-2}+1$ te factoriseren. We kunnen hier zelf al twee factoren van maken, wetende dat de priemfactorisatie van 699 gelijk is aan $3 \cdot 233$. Er geldt namelijk: $2^{699}+1 = (2^{233})^3+1 = (2^{233}+1)(2^{2\cdot 233}-2^{233}+1)$. Nu kunnen we dus kijken naar de factorisatie van $2^{233}+1$ en naar de factorisatie van $2^{2\cdot 233}-2^{233}+1$. Voor $n = 701$ is dit nog mogelijk om door Maple13 te laten doen, wat bij methode 1 wel gedaan is, maar het duurt vrij lang. Daarom is het voor een grote n efficienter om de Cunningham Tables te gebruiken.(Zeker als n nog groter wordt.) Deze tabellen bevatten de factorisaties van $2^n \pm 1$ voor $n \leq 1200$. De tabel geeft de volgende waardes:

```
233 467      27961. P63
699 9551137      373746913      53590752072775417 P108
```

Hierbij zijn 233 en 699 de n in $2^n + 1$. Verder zijn het allen priemfactoren, waarbij $P63$ en $P108$ priemgetallen zijn die, respectievelijk, uit 63 en 108 cijfers bestaan. Merk op dat niet een getal uit de factorisaite van $2^{233} + 1$ in de factorisaite van $2^{699} + 1$ voorkomt! Dit komt omdat de Cunningham Tables ervan uitgaan dat deze ontbingsstap al gemaakt is. Ze willen namelijk niet nog een keer de factorisatie van $2^{233} + 1$ opschrijven. De methode om de volledige factorisatie te verkrijgen, komt neer op het delen van $2^{699} + 1$ door de gegeven priemfactoren om vervolgens met het commando 'ifactor' van Maple de volledige factorisatie te vinden. Het ziet er dus als volgt uit (waarbij de procenttekens staan voor de laatst gegeven output):

```
> b:=2^{233}+1
b := 13803492693581127574869511724554 05
     0904902217944340773110325048447598593
>b/467;
29557800200387853479377969431593256755679267546768250771573979545179
>%/27961;
10571081220409804184177235947066720344651216890228622285173627 39
>ifactor(%)
(3)(352369374013660139472574531568890678155040563007620742839120913)

>a:=2^466-2^233+1;
a := (19053641054174757271616194029499306065360096085
60163055944309667740094917397058916312934519287971 11
57630962556173509660743538428428311278387 3)
> a/53590752072775417;
(35553972126198575822767730944359409118133849140881059532465579
37576780673238093554254481318584876537981504450928674632215369)
```

```
> %/373746913;
(951284703352147174062885997518845302626856723787336259081
438336208219243067860082701066033576811519505849256587351 3)

> %/9551137;
995991056721463815316318881740305162230273446802549538
428187488262621762275905039055628700098021334534149449

> ifactor(995991056721463815316318881740305162230273446802
549538428187488262621762275905039055628700098021334534149449);

(3) (331997018907154605105439627246768387410091148934183179476
606249608754058742530167968520956669934044844716483)
```

De volledige factoristatie $p_1 \cdot ... \cdot p_s$ hebben we dus. We moeten nu nog kijken voor $1 < i < s$ of we een factor p_i uit de factorisatie kunnen halen, terwijl $x^{p_1 \cdot ... \cdot p_{i-1} p_{i+1} \cdot ... \cdot p_s} = 1$. Dit kunnen we doen met behulp van het commando powmod van Maple13. Dit ziet er als volgt uit:

```
> p := 701;
w := (2^p+1)*(1/3);
‘mod‘(Powmod(x, (4*(2^699+1))/p[i], x^2-6*x+1, x), w);
```

We hebben dus alle priemfactoren ingevuld voor $p[i]$(, hiermee wordt uiteraard p_i bedoeld). Het blijkt dus dat alleen voor $p_i = 3$ de uitkomst 1 blijft. Oftewel de orde van x is $4 \cdot \frac{2^{699}+1}{3} = \frac{2^{701}+4}{3} = W_{701} + 1$. Nu gebruik makende van stelling 8 kunnen we concluderen dan W_{701} een priemgetal is.

Hoofdstuk 5

Conclusie

We kunnen concluderen dat we met behulp van de elementaire eigenschappen uit hoofdstuk 2, Wagstaff-getallen tot W_{61} makkelijk kunnen controleren op primaliteit. Vervolgens door gebruik te maken van de Algemene test, Vrba's test, Lifschitz test en Gerbicz test, kunnen we Wagstaff waarschijnlijke priemen berekenen. In deze scriptie hebben we alle Wagstaff waarschijnlijke priemen tot W_{2398} berekend met behulp van Maple13, waarvan de grootste W_{1709} is. Voor de Wagstaff waarschijnlijke priemen tot deze grootte konden we namelijk daadwerkelijk het primaliteitsbewijs geven. Dat hebben we dan ook in hoofdstuk 4 voor een aantal Wagstaff-priemen gedaan.

Bibliografie

[1] P. T. Bateman, J. L. Selfridge and Wagstaff, Jr., S. S., "The new Mersenne conjecture,"Amer. Math. Monthly, 96 (1989), 125-128.

[2] D.H. Lehmer, 'an axtended theory of Lucas' functions', Second Series, Vol. 31, No. 3 (Jul., 1930), pp. 419-448

[3] Prof. dr.F. Oort, Prof. dr. H.W. Lenstra, Jr. en Prof. B. van Geemen, Algebra: ringen, lichamen, 2001.

[4] Prof. dr. Jaap Top, Algebra: groepen, 2003.

[5] Robert Gerbicz, A proof of first part of Conjectures 2 and 3 (Wagstaff and Fermat) of previous paper, 2008, http://trex58.files.wordpress.com/2009/01/wagstaffandfermat.pdf.

[6] Renaud Lifschitz en Henri Lifschitz, An efficient probable prime test for numbers of the form $\frac{2^n+1}{3}$, 2nd release, 2002.

[7] Anton Vrba, A really trivial proof for proving Wagstaff numbers prime, 2008, http://trex58.files.wordpress.com/2009/01/waggstaff_ver20.pdf.

[8] Jeroen Demeyer, The Cunningham Tables, http://cage.ugent.be/ jdemeyer/cunningham.

[9] Stephen Abbott, Understanding analysis, Springer, 2001, p.64.

[10] Aurifeuillian Factorization, Andrew Granville and Peter Pleasants, 2006, http://www.dms.umontreal.ca/ andrew/PDF/AureFinal.pdf.