

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1952 - 013

Enige methoden om random-numbers te maken. 2

H.J.A. Duparc en W. Peremans



1952

Enige methoden om random-numbers te maken. II.2

door

H.J.A. Duparc en W. Peremans.

§ 3. De algemene recursiebetrekking van de tweede orde.

Wij beschouwen thans de meer algemene recursiebetrekking $u_{n+2} = au_{n+1} + bu_n$, waarbij a en b willekeurige gehele getallen zijn.

Hierbij onderscheiden wij twee gevallen al naar de G.G.D. $(a,b) = 1$ is of niet. Wij beschouwen eerst het laatste geval, waarbij men heeft

$$g = (a,b) \text{ en } a = ga', \quad b = gb', \text{ dus } (a',b') = 1.$$

A. Onderstellen wij eens dat $g \nmid b'$ en stellen wij $b' = gb''$, dan is $g^n \nmid u_n$, want stellen wij $u_n = g^n u'_n$, dan volgt uit $u_{n+2} = au_{n+1} + bu_n$ de relatie $u'_{n+2} = a'u'_{n+1} + b''u'_n$, waarbij wegens $(a',b') = 1$ ook $(a',b'') = 1$ is, zodat de getallen u'_n voldoen aan een recursiebetrekking van het nader te beschouwen type, waarbij de G.G.D. (a',b'') der coëfficiënten wel 1 is.

B. Is echter $g \mid b'$, dan heeft men, indien wij $g_1 = (g,b')$ stellen en $b' = g_1 b''$ en $g = g_1 g''$ noemen en tenslotte $u_n = g^{\lfloor \frac{n}{2} \rfloor} u'_n$ noemen, de relaties

$$u'_{2n+2} = a'u'_{2n+1} + b''u'_{2n}; \quad u'_{2n+1} = au'_{2n} + b'u'_{2n-1},$$

waaruit volgt

$$u'_{n+4} = (aa' + 2b'')u'_{n+2} - b'^2 u'_n,$$

zodat de rij der getallen u'_n in twee rijen uiteenvalt. Nu is $(a',b'') = 1$, zodat de G.G.D. der coëfficiënten

$$aa' + 2b'' = g_1 g'' a'^2 + 2g_1 b'' \text{ en } b'^2 = g_1^2 b''^2,$$

of gelijk is aan g_1 en dan verkeren wij in het zoëven bekeken geval of deze is een veelvoud $g_2 g_1$ van g_1 . Omdat b''^2 en $g'' a'^2 + 2b''$ geen factor gemeen hebben (want $(b'',g'') = 1$ en $(b',a') = 1$), is $g_2 = (g_1, g'' a'^2 + 2b'')$. Indien $g_2^2 \mid g_1$, dan verkeren wij weer in geval A; is $g_2^2 \nmid g_1$, dan verkeren wij in geval B en onderscheiden wij weer twee mogelijkheden, waarbij men hetzij weer tot geval A wordt gevoerd of tot een deler g_3 van g_2 . Bij gegeven a en b breekt de rij $g_2, g_3, \dots$, die gevonden wordt indien steeds de tweede mogelijkheid in geval B optreedt, vanzelf af.

Thans gaan wij over tot de behandeling van het geval dat de G.G.D. $(a,b) = 1$ is.

Zij ω een wortel van de vergelijking $x^2 - ax - b = 0$, waarvan wij onderstellen, dat de wortels verschillend zijn. Zij $\bar{\omega}$ de andere wortel dezer vergelijking.

Voorlopig zullen wij $u_0 = 0$ en $u_1 = 1$ nemen. Dan heeft men $\omega^n = u_n \omega + bu_{n-1}$. Immers voor $n = 1$ is deze bewering juist en als zij reeds voor n bewezen is, volgt daaruit

$$\omega^{n+1} = u_n \omega^2 + bu_{n-1} \omega = (au_n + bu_{n-1}) \omega + bu_n = u_{n+1} \omega + bu_n.$$

Verder heeft men nog $\omega^n = u_n \omega - au_n + u_{n+1}$. Evenals bij de rij van Fibonacci vinden wij uit

$$\begin{aligned} u_{2n} \omega + u_{2n-1} b &= \omega^{2n} = (u_n \omega + bu_{n-1})^2 = u_n^2 \omega^2 + 2bu_n u_{n-1} \omega + b^2 u_{n-1}^2 = \\ &= u_n (au_n + 2bu_{n-1}) \omega + b(u_n^2 + bu_{n-1}^2) = u_n (u_{n+1} + bu_{n-1}) \omega + b(u_n^2 + bu_{n-1}^2) \end{aligned}$$

de verdubbelingsformules

$$u_{2n} = u_n (u_{n+1} + bu_{n-1}); \quad u_{2n-1} = u_n^2 + bu_{n-1}^2.$$

Zij m een willekeurig natuurlijk getal, waarvan wij onderstellen, dat het relatief priem is met b . Evenals vroeger definiëren wij dan het getal $c(m)$ als het kleinste natuurlijke getal c , waarvoor ω^c rationaal is mod m , d.w.z. waarvoor $u_c \equiv 0 \pmod{m}$ is.

Dan is ook ω^{tc} rationaal mod m voor elke natuurlijke t en men heeft

$$u_{tc+1} \equiv \omega^{tc} \equiv u_{c+1}^t \pmod{m}.$$

Verder is dan $(u_{c+1}, m) = 1$, want hadden u_{c+1} en m een priemfactor gemeen dan zat die ook in $bu_{c-1} = u_{c+1} - au_{c-1}$ dus in u_{c-1} enz., zodat die priemfactor ook in $u_1 = 1$ zat, wat onmogelijk is. Bijgevolg is dan ook $(u_{tc+1}, m) = 1$ voor alle natuurlijke t . Zij nu omgekeerd gegeven, dat ω^d rationaal is mod m . Stel dan $d = qc + r$ met $0 \leq r < c$. Dan is

$$\begin{aligned} \omega^d &= \omega^{qc+r} = (u_{qc} \omega + u_{qc+1} - au_{qc}) (u_r \omega + bu_{r-1}) = \\ &= u_{qc+1} (u_r \omega + bu_{r-1}) \pmod{m}, \end{aligned}$$

dus $u_{qc+1} u_r \equiv 0 \pmod{m}$, waaruit volgt $u_r \equiv 0 \pmod{m}$, dus $r = 0$. Bijgevolg is $c \mid d$.

Vervolgens definiëren wij evenals vroeger het getal $C(m)$ als het kleinste natuurlijke getal C waarvoor $\omega^C \equiv 1 \pmod{m}$ is, dus waarvoor geldt $u_C \equiv 0 \pmod{m}$ en $u_{C+1} \equiv 1 \pmod{m}$. Omdat $u_C \equiv 0 \pmod{m}$ is, is C een veelvoud van c . Wij stellen $C = cv$ en hebben dan $1 \equiv u_{C+1} = u_{vc+1} \equiv u_{c+1}^v \pmod{m}$ en voor ieder natuurlijk getal $w < v$ geldt dan $u_{c+1}^w \not\equiv 1 \pmod{m}$. Het getal v is dus het kleinste natuurlijke getal, waarvoor $u_{c+1}^v \equiv 1 \pmod{m}$. Omgekeerd geldt deze relatie voor zekere natuurlijke v en voor geen kleiner natuurlijk getal, dan is

$$\omega^{vc} = u_{vc} \omega + u_{vc+1} - au_{vc} \equiv u_{vc+1} \equiv u_{c+1}^v \equiv 1 \pmod{m},$$

en voor iedere natuurlijke $w < v$ geldt dan

$$\omega^{wc} = u_{wc} \omega + u_{wc+1} - au_{wc} \equiv u_{wc+1} \equiv u_{c+1}^w \not\equiv 1 \pmod{m}.$$

Uit $\omega^c \equiv u_{c+1} \pmod{m}$ en de hieruit volgende formule

$\bar{\omega}^c \equiv u_{c+1} \pmod{m}$, volgt na vermenigvuldiging $(-b)^c \equiv u_{c+1}^2 \pmod{m}$.
Uiteraard heeft men wegens Fermat de relatie $v \mid p-1$.

Wij beschouwen thans het getal m nader. Zij de ontbinding van m gegeven door $m = p_1^{s_1} \dots p_j^{s_j}$, dan hangen de grootheden $C(m)$ en $c(m)$ weer samen met $C(p_i)$ en $c(p_i)$ ($i = 1, \dots, j$). Het is direct duidelijk, dat $C(m)$ het K.G.V. is der getallen $C(p_i^{s_i})$ ($i = 1, \dots, j$) en dat $c(m)$ het K.G.V. is der getallen $c(p_i^{s_i})$ ($i = 1, \dots, j$) en dat $C(p^s) = p^{s-n}C(p)$ als n de grootste exponent is waarvoor $p^n \mid \omega^{C(p)} - 1$. Wij kunnen dus volstaan met verder de grootheden $C(p)$ en $c(p)$ voor een willekeurig priemgetal p te beschouwen, waarvan wij wegens $(b, m) = 1$ eisen, dat het niet deelbaar is op b . Wij voeren nog in de exponent e van het getal $-b \pmod{p}$. Uiteraard is dan $e \mid p-1$.

Voor de wortels der vierkantsvergelijking $x^2 - ax - b = 0$ vinden wij

$$\omega, \bar{\omega} = \frac{a}{2} \pm \sqrt{\frac{a^2}{4} + b} = \frac{a}{2} \pm \sqrt{D}.$$

1). Beschouw nu een priemgetal p , dat niet deelbaar is op D , dat qua-
draatrest $\pmod{p}$ is. Men heeft dan $D^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

dus $(2\omega - a)^{p-1} \equiv 1 \pmod{p}$, dus $2^p \omega^p - a^p \equiv 2\omega - a \pmod{p}$, dus $\omega^{p-1} \equiv 1 \pmod{p}$. In dit geval is dus $C \mid p-1$.

2). Zij thans het getal D nietrest $\pmod{p}$, waarbij weer ondersteld is

$p \nmid D$. Dan is $D^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, dus analoog aan hierboven dus $2^p \omega^p - a^p \equiv a - 2\omega \pmod{p}$, dus $\omega^p \equiv a - \omega \pmod{p}$, dus $\omega^{p+1} \equiv a\omega - \omega^2 = -b \pmod{p}$. Dus $\omega^{(p+1)e} \equiv 1 \pmod{p}$, dus $C \mid (p+1)e$.

3). Zij $p \mid D$. Dan is $(2\omega - a)^2 \equiv 0 \pmod{p}$, dus $(2\omega - a)^p \equiv 0 \pmod{p}$, dus $2^p \omega^p - a^p \equiv 0 \pmod{p}$, dus $2\omega^p \equiv a \pmod{p}$ derhalve $C \mid p$, waaruit volgt $C = p$. Verder is dan $4\omega^{2p} \equiv a^2 \equiv -4b \pmod{p}$, dus $\omega^{2pe} \equiv (-b)^e \equiv 1 \pmod{p}$, dus $C \mid 2pe$.

4). Voor $p = 2$ heeft men als $2 \nmid a$ de relatie (waarbij weer $p \nmid b$ onder-
steld is) $\omega^2 \equiv 1 \pmod{2}$, dus $C(2) = 2$.

Is a oneven, dan volgt uit $\omega^2 = a\omega + b$ de relatie $\omega^3 = a\omega^2 + b\omega = a^2\omega + ab + b\omega \equiv 1 \pmod{2}$, want $a^2 + b$ is dan even en ab oneven. In dit geval is dus $C(2) = 3$.

Voor de bepaling van $C(2^k)$ is het nodig om $C(4)$ te kennen. Wij be-
schouwen weer diverse gevallen.

Is $a \equiv 2 \pmod{4}$, dan is $\omega^2 = a\omega + b \not\equiv 1 \pmod{4}$, maar wel geldt $\omega^4 \equiv a^2\omega^2 + 2ab\omega + b^2 \equiv 1 \pmod{4}$, dus $C(4) = 4$. In dit geval is echter $8 \nmid \omega^4 - 1$, dus de maximale exponent n met $2^n \mid \omega^{C(4)} - 1$ is $n=2$. Is echter $4 \mid a$, dan is $\omega^2 = a\omega + b \equiv b \pmod{4}$. Is $b \equiv 1 \pmod{4}$ dan is $C(4) = 2$. Indien $b \equiv -1 \pmod{4}$, dan is $\omega^2 \equiv -1 \pmod{4}$, dus $C(4) = 4$. In dit geval is $n \geq 3$.

Is a oneven, dan is bij $b \equiv 1 \pmod{4}$ wegens $\omega^3 = (a^2 + b)\omega + ab \equiv 2\omega + 1 \pmod{4}$ het getal $C(4) \neq 3$, maar $\omega^6 \equiv 1 \pmod{4}$, dus $C(4) = 6$. Is a oneven en $b \equiv -1 \pmod{4}$, dan is $\omega^3 \equiv -a \pmod{4}$, dus $C(4) = 3$ als $a \equiv -1 \pmod{4}$ en $C(4) = 6$ als $a \equiv +1 \pmod{4}$.

Wij krijgen dus het volgende overzicht van de 8 gevallen aangaande het karakter mod 4 van a en b en de daarbij behorende waarde van $C(4)$.

$\begin{array}{c c} & a \\ \hline b & \end{array}$	0	1	2	3
1	2	6	4	6
3	4	6	4	3

5). Indien $p \mid b$, dan is $\omega^2 \equiv a\omega \pmod{p}$. Geen exponent $c(p)$ bestaat waarvoor ω^c rationaal is mod p . Is echter d de exponent van a mod p , dan is $\omega^{d+t} \equiv \omega^t \pmod{p}$ en $u_{d+t} \equiv u_t \pmod{p}$ voor alle natuurlijke t .

6). Indien $p \mid a$, dan is $\omega^2 \equiv b \pmod{p}$, dus $c(p) = 2$. Dus $u_{2n} \equiv 0 \pmod{p}$ voor natuurlijke n . Is e_1 de exponent van b mod p , dan is $C(p) = 2e_1$. Uiteraard is $e_1 \mid p-1$, dus $C(p) \mid 2(p-1)$.

Voor willekeurige p met $p \nmid b$ heeft men, zoals wij reeds zagen, $\omega^c \equiv u_{c+1} \pmod{p}$, dus $\overline{\omega}^c \equiv u_{c+1} \pmod{p}$, dus na vermenigvuldiging dezer relaties

$$(-b)^c \equiv u_{c+1}^2 \pmod{p}.$$

Om hieruit verdere conclusies over het getal v af te leiden, beschouwen wij weer de exponent e van $-b \pmod{p}$. Dan is $u_{c+1}^{\frac{2e}{(c,e)}} \equiv (-b)^{\frac{ce}{(c,e)}} \pmod{p}$, dus $v \mid \frac{2e}{(c,e)}$. Verder is $u_{c+1}^{2v} \equiv (-b)^{cv} \equiv 1 \pmod{p}$, dus cv is een veelvoud van e en uiteraard van c , dus van het K.G.V. van e en c .

Dus $\frac{ce}{(c,e)} \mid cv$, dus $\frac{e}{(c,e)} \mid v$. Bijgevolg heeft men $v = \frac{e}{(c,e)}$ of $v = \frac{2e}{(c,e)}$.

Het eerste geval treedt dan en slechts dan op als $u_{c+1}^{\frac{e}{(c,e)}} \equiv +1 \pmod{p}$, het tweede dan en slechts dan als $u_{c+1}^{\frac{e}{(c,e)}} \equiv -1 \pmod{p}$.

Thans onderscheiden wij drie gevallen.

I. Het getal e bevat meer factoren 2 dan het getal c . Dit is aequivalent daarmee, dat $\frac{e}{(c,e)}$ even is. In dit geval is

$$u_{c+1}^{\frac{e}{(c,e)}} \equiv (u^2)^{\frac{e}{2(c,e)}} \equiv (-b)^{\frac{ce}{2(c,e)}} \pmod{p}.$$

Gesteld, dat $v = \frac{e}{(c,e)}$, dan was $(-b)^{\frac{2e}{(c,e)}} \equiv 1 \pmod{p}$, dus $e \mid \frac{ce}{2(c,e)}$,

dus $\frac{c}{(c,e)}$ is even, wat niet kan, omdat e meer factoren 2 bevat dan c . Dus in dit geval is $v = \frac{2e}{(c,e)}$. Wegens $v \mid p-1$ is in dit geval $p \equiv 1 \pmod{4}$.

II. Het getal c bevat meer factoren 2 dan het getal e . Dit is aequivalent daarmee, dat $\frac{c}{(c,e)}$ even is. In dit geval is c even, $c = 2d$. Uit

$u_{c+1}^2 \equiv (-b)^c \pmod{p}$ volgt dan $u_{c+1} \equiv \pm (-b)^{\frac{c}{2}} \pmod{p}$. Dus $\omega^c \equiv \pm (-b)^{\frac{c}{2}} \pmod{p}$. Dus na vermenigvuldigen met $\bar{\omega}^d$ heeft men

$$(-b)^d \omega^d \equiv \pm (-b)^d \bar{\omega}^d \pmod{p},$$

dus

$$\omega^d \equiv \pm \bar{\omega}^d \pmod{p}.$$

Was nu $u_{c+1} \equiv (-b)^{\frac{c}{2}} \pmod{p}$, dan was $\omega^d \equiv \bar{\omega}^d \pmod{p}$,

dus ω^d was rationaal mod p in strijd met de minimaaleigenschap van c . Men heeft dus $u_{c+1} \equiv -(-b)^{\frac{c}{2}} \pmod{p}$. Verder is dan

$$u_{c+1}^{\frac{e}{(c,e)}} \equiv (-1)^{\frac{e}{(c,e)}} (-b)^{\frac{d}{(c,e)}} \equiv -1 \cdot ((-b)^e)^{\frac{d}{(c,e)}} \equiv -1, \text{ omdat } \frac{d}{(c,e)}$$

geheel is, want $\frac{c}{(c,e)}$ is even. Bijgevolg is ook in dit geval $v = \frac{2e}{(c,e)}$.

III. Wij onderstellen nu, dat de even getallen c en e eventueel factoren 2 bezitten, wat daarmee equivalent is, dat $\frac{c}{(c,e)}$ en $\frac{e}{(c,e)}$ beide oneven en c en e beide even zijn. Omdat c even is, heeft men weer evenals in geval II dat $u_{c+1} \equiv -(-b)^{\frac{c}{2}} \pmod{p}$. Verder is dan $c = 2f$ en $(-b)^{\frac{c}{2}} \equiv \pm 1 \pmod{p}$, dus wegens de minimaaleigenschap van e is dan $(-b)^{\frac{c}{2}} \equiv -1 \pmod{p}$. Wij vinden dan

$$u_{c+1}^{\frac{e}{(c,e)}} \equiv (-1)^{\frac{e}{(c,e)}} (-b)^{\frac{de}{(c,e)}} \equiv -(-b)^{\frac{fc}{(c,e)}} \equiv 1 \pmod{p},$$

omdat $\frac{c}{(c,e)}$ oneven is. In dit geval is dus $v = \frac{e}{(c,e)}$.

IV. In het geval dat c en e beide oneven zijn kan v zowel gelijk zijn aan $\frac{e}{(c,e)}$ als aan $\frac{2e}{(c,e)}$.

Wij combineren nu de gevallen 1, 2 en 3 met de gevallen I t/m IV. Hierbij zij opgemerkt dat in de gevallen 2 uit $c \nmid p+1$ en $e \nmid p-1$ volgt dat $(e, c) = 1$ of 2 is, dus $v = \frac{1}{2}e$, e of $2e$ is. In de gevallen 3 heeft men wegens $c = p$ en $e \nmid p-1$ dat $(e, c) = 1$, dus $v = e$ of $2e$.

De combinatie 2 III ~~tenslotte~~ treedt niet op. Immers men heeft voor priemgetallen van het type 2 de relatie $\omega^{p+1} \equiv -b \pmod{p}$, dus

$\omega^{(p+1)\frac{e}{2}} \equiv (-b)^{\frac{e}{2}} \equiv -1 \pmod{p}$. Wegens $v = \frac{e}{2}$, $C = vc$ is $C \nmid (p+1)\frac{e}{2}$, dus had men $\omega^{(p+1)\frac{e}{2}} \equiv 1 \pmod{p}$, hetgeen tot een contradictie voert.

Wij krijgen zo het volgende staatje:

		$e(\text{mod } 4)$	$c(\text{mod } 4)$	(e, c)	τ	$p(\text{mod } 4)$
1	I	0 of 2			$\frac{2e}{(e, c)}$	1
1	II		0 of 2		$\frac{2e}{(e, c)}$	1
1	III	0 of 2	0 of 2	even	$\frac{e}{(e, c)}$	± 1
1	IV 1	± 1	± 1	± 1	$\frac{e}{(e, c)}$	± 1
1	IV 2	± 1	± 1	± 1	$\frac{2e}{(e, c)}$	± 1
2	I 1	0	2	2	e	1
2	I 2	0 of 2	± 1	1	2e	1
2	II 1	2	0	2	e	-1
2	II 2	± 1	0 of 2	1	2e	-1
2	IV 1	± 1	± 1	1	e	± 1
2	IV 2	± 1	± 1	1	2e	± 1
3	I 1	0 of 2	± 1	1	e	1
3	I 2	0 of 2	± 1	1	2e	1
3	IV 1	± 1	± 1	1	e	± 1
3	IV 2	± 1	± 1	1	2e	± 1

Wij geven als voorbeeld de rij $u_{n+2} = u_{n+1} + 3u_n$ met $u_0 = 0$, $u_1 = 1$.

n	u_n	ontbinding van u_n
0	0	0
1	1	1
2	1	1
3	4	2^2
4	7	7
5	19	19
6	40	$2^3 \cdot 5$
7	97	97
8	217	$7 \cdot 31$
9	508	$2^2 \cdot 127$
10	1159	$19 \cdot 61$
11	2683	2683
12	6160	$2^4 \cdot 5 \cdot 7 \cdot 11$
13	14209	$13 \cdot 1093$
14	32689	$97 \cdot 337$
15	75316	$4 \cdot 19 \cdot 991$
16	173383	$7 \cdot 17 \cdot 31 \cdot 47$
17	399331	$103 \cdot 3877$
18	919480	$2^3 \cdot 5 \cdot 127 \cdot 181$

n	u_n	ontbinding van u_n
19	2117473	37.151.379
20	4875913	7.19.61.601
21	11228332	$2^2 \cdot 43.97.673$
22	25856071	23.419.2683
23	59541067	139.428353
24	137109280	$2^5 \cdot 5.7.11.31.259$
25	315732481	19.16617499
26	727060321	13.1093.51169
27	1674257764	$2^2 \cdot 127.3295783$
28	3855438727	7.29.97.337.581

Hierbij is $D = 3$. De getallen van groep 1 zijn congruent met 1,3,4, 9,10 of 12 mod 13, die van groep 2 zijn congruent met 2,5,6,7,8 of 11 mod 13, terwijl tot de groep 3 slechts het getal 13 behoort. Uit 4 blijkt, dat $C(4) = 6$ is. Nu is $\omega^6 - 1 = 40\omega + 56$ deelbaar door 8, maar niet door 16. Derhalve is $C(2^k) = 2^{k-3} \cdot 6 = 3 \cdot 2^{k-2}$ voor $k \geq 3$. Geval 5 treedt slechts op voor $p = 3$. De exponent van $a = 1 \pmod{3}$ is uiteraard 1, dus voor alle natuurlijke getallen is $\omega^{t+1} \equiv \omega^t \equiv 1 \pmod{3}$.

Wij geven een staatje van een aantal priemgetallen en de bijbehorende waarden van e , v , c .

p	e	c	v	type
5	4	6	4	2 I 1
7	3	4	6	2 II 2
11	10	12	10	2 II 1
13	6	13	12	3 I 2
17	16	16	1	1 III
19	9	5	18	2 IV 2
23	22	22	1	1 III
29	28	28	1	1 III
31	15	8	30	2 II 2
37	18	19	9	2 I 2
41	8	42	8	2 I 1
43	21	21	2	1 IV 2
47	46	16	46	2 II 1
53	52	52	1	1 III
59	58	60	58	2 II 1
61	5	10	2	1 II
67	11	34	22	2 II 2
71	70	72	70	2 II 1
73	12	37	24	2 I 2
79	39	39	1	1 IV 1
151	25	19	25	2 IV 1
337	168	14	24	1 I

Wij beschouwen tenslotte de rij $w_0, w_1, w_2, \dots$, gedefinieerd door

$$w_{n+2} = aw_{n+1} + bw_n,$$

waarbij w_0 en w_1 willekeurige gehele waarden bezitten, die niet behoeven samen te vallen met de getallen 0 resp. 1. Is dat wel het geval, dan geven wij, evenals vroeger, de rij weer aan met $u_0, u_1, u_2, \dots$.

Zijn ω en $\bar{\omega}$ de wortels der karakteristieke vergelijking

$$\omega^2 - a\omega - b = 0, \text{ dan geldt}$$

$$\omega w_{n+1} + bw_n = \omega^n (w_1 \omega + bw_0).$$

Voor $n = 0$ is de bewering duidelijk en geldt zij voor zekere n , dan heeft men

$$\begin{aligned} \omega w_{n+2} + bw_{n+1} &= \omega aw_{n+1} + \omega bw_n + bw_{n+1} = \omega^2 w_{n+1} + \omega bw_n = \\ &= \omega^{n+1} (w_1 \omega + bw_0). \end{aligned}$$

Evenzo heeft men

$$\bar{\omega} w_{n+1} + bw_n = \bar{\omega}^n (w_1 \bar{\omega} + bw_0),$$

dus na eliminatie van w_{n+1} uit de gevonden betrekkingen

$$w_n = w_1 \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} + bw_0 \frac{\omega^{n-1} - \bar{\omega}^{n-1}}{\omega - \bar{\omega}}.$$

Hieruit volgt nog

$$w_n = u_n w_1 + bw_0 u_{n-1}.$$

Men heeft dus als $n \equiv N \pmod{C(p)}$ de relatie $w_n \equiv w_N \pmod{p}$, dus in het bijzonder $w_n \equiv w_{n+C(p)} \pmod{p}$. De periode van het getal p is kleiner, als de getallen w_1 en bw_0 beide deelbaar zijn door p . Sluiten wij dit uit, dan volgt dat $w_n \equiv w_N \pmod{p}$ voor alle n , dan en slechts dan als $n \equiv N \pmod{C(p)}$ wegens $\omega w_{n+1} + bw_n = \omega^n (w_1 \omega + bw_0)$ en de geconjugeerde formule.