Enige methoden om random-numbers te maken. I

door

H.J.A. Duparc, C.G. Lekkerkerker, A. Nijenhuis en W. Peremans.

§ 1. Toepassing van de stelling van Fermat.

Door Lehmer is opgemerkt dat de stelling van Fermat die zegt dat $a^{p-1} \equiv 1 \pmod p$, een middel biedt om bij speciaal te kiezen p en a "random-numbers" op te leveren. Is nl. a een primitieve wortel mod p d.w.z. is $a^d \not\equiv 1 \pmod p$ voor $0 < d < p-1$, dan vormen de p-1 getallen ba^h $(h = 0,1,2,\ldots,p-2)$, waarbij $p \nmid b$, een compleet restsysteem mod p op het getal 0 na. Deze getallen nu leveren bij grote p een verzameling, die men "random-numbers" zou kunnen noemen.

Ook als a geen primitieve wortel is mod p, maar de periode van a mod p (dit is de kleinste natuurlijke exponent g, waarvoor $a^g \equiv 1 \pmod p$ is) groot genoeg is, levert deze methode een bruikbaar resultaat op en dat is ook het geval als a weliswaar niet priem is, maar de periode van a nog voldoende groot is.

In de practijk is de reductie mod m eenvoudig als $m = 10^n \pm 1$, waarbij n een nader te bepalen natuurlijk getal is. Werkt men met de ARRA, dan neme men bij voorkeur $m = 2^n \pm 1$.

Wij onderzoeken eerst even het geval dat $m = 10^n \pm 1$ is.

Is $m = 10^n - 1 = p_1^{r_1} \ldots p_s^{r_s}$, dan is de maximale periode van een getal mod $p_i^{r_i}$ volgens de stelling van Euler, die zegt dat voor $(a,t)=1$ geldt $a^{\varphi(t)} \equiv 1 \pmod t$, gelijk aan $(p_i-1)p_i^{r_i-1}$ $(i = 1 \ldots s)$, zodat de periode van ieder natuurlijk getal ten hoogste gelijk is aan het K.G.V. der getallen $(p_i-1)p_i^{r_i-1}$ $(i = 1,\ldots,s)$. Deze maximale periode geven wij aan met L. Hieronder volgt een tabel, dat bij $n = 1,2,3,\ldots$ de ontbinding van $m = 10^n-1$ geeft en tevens het K.G.V. dat dus periode L is.

n	m	$\varphi(p_i^{s_i})$	L
1	3^2	6	6
2	$3^2.11$	6;10	30
3	$3^3.37$	18;36	36
4	$3^2.101$	6;100	300
5	$3^2.41.271$	6;40;270	1080
6	$3^3.7.11.13.37$	18;6;10;12;36	180
7	$3^2.239.4649$	6;238;4648	711144
8	$3^2.73.101.137$	6;72;100;136	30600
9	$3^4.37.333667$	54;36;333666	667332
10	$3^2.11.41.271.9091$	6;10;40;270;9090	109080

Hierbij zij nog opgemerkt, dat uit $p_1 \mid 10^n-1$, dus $10^{n_1} \equiv 1 \pmod{p_1}$ volgt dat als het priemgetal p_1 geen factor is van 10^d-1 met $0 < d < n$ uit

$10^{p_1-1} \equiv 1 \pmod{p_1}$ volgt dat $n \mid p_1-1$, dus $p_1 \equiv 1 \pmod{n}$. Geldt dit ook voor $p_2, p_3, \ldots, p_h$, dan is het K.G.V. van de getallen $(p_1-1)p_1^{s_1}, \ldots, (p_h-1)p_h^{s_h}$ aanzienlijk kleiner dan hun product (nl. ten hoogste gelijk aan hun product gedeeld door n^{h-1}), dus $L < \frac{m}{n^{h-1}}$.

Voor $m=10^n+1$ gelden analoge beschouwingen. De factoren van 10^n+1 zijn ook deelbaar op $10^{2n}-1$. Treedt een factor p op in 10^n+1, maar niet in 10^d+1 met $0 < d < n$, dan treedt p op in $10^{2n}-1$ maar niet in $10^{2d}-1$ met $0 < d < n$. Immers zij c de kleinste exponent waarvoor $10^c \equiv 1 \pmod{p}$, dan is wegens $10^n \equiv -1 \pmod{p}$ ook $10^{n-c} \equiv -1 \pmod{p}$. Nu is $10^{p-1} \equiv -1 \pmod{p}$, dus $2n \mid p-1$. Is $n-c > 0$, dan is $c \mid n-c$, dus $c \mid n$, maar dan is wegens $10^c \equiv 1 \pmod{p}$ ook $10^n \equiv 1 \pmod{p}$ in strijd met de onderstelling. Het is dus uitgesloten, dat $n > c$. Uit $n-c < 0$ volgt nu verder $10^{c-n} \equiv -1 \pmod{p}$, dus $n \mid c-n$, dus $c \geq 2n$. Wegens $c \leq 2n$ is dan $c = 2n$, waarmee de bewering bewezen is, Hieruit volgt $p \equiv 1 \pmod{2n}$. Ook voor dit geval geven wij een tabel analoog aan de bovenstaande.

n	m	$\varphi(p_i^{s_i})$	L
1	11	10	10
2	101	100	100
3	7.11.13	6;10;12	60
4	73.137	72;136	1224
5	11.9091	10;9090	9090
6	101.9901	100;9900	9900
7	11.909091	10;909090	909090

Is eenmaal een keuze voor m gedaan, dan dient achteraf nog een grondtal a te worden bepaald, waarvan de periode L is en niet kleiner. Hierbij is het niet noodzakelijk, dat a een primitieve wortel is van elk der getallen $p_i^{s_i}$, maar slechts is vereist, dat het K.G.V. der exponenten mod $p_i^{s_i}$ van a gelijk is aan L.

Bij $m = 10^5-1$ is $a = 7$ bruikbaar. Hier is nl. $L = 1080$. Dat factor 3 van L bij $a = 7$ nodig is blijkt uit $7^{20} \equiv -1 \pmod{41}$, dat factor 5 van L nodig is blijkt uit $7^8 \equiv -4 \pmod{41}$ en dat de factor 27 van L nodig is blijkt uit $7^{90} \equiv -29 \pmod{271}$. Het getal 7 is echter geen primitieve wortel mod 9 want $7^3 \equiv 1 \pmod{9}$. De factoren 2 van L bleken echter door de factor 41 van m te worden vereist. Bij dit getal m is echter $a = 2$ niet bruikbaar, want $2^{20} \equiv 1 \pmod{41}$, evenmin 3 wegens $3^{30} \equiv 1 \pmod{271}$ en evenmin 5 wegens $5^{20} \equiv 1 \pmod{41}$.

Geheel analoge beschouwingen treden op bij getallen $m = g^n \pm 1$, voor willekeurige g. Bij de ARRA is reductie mod m, zoals al wordt opgemerkt, eenvoudig als $m = 2^n \pm 1$, en ook als $m = 2^n$. Deze drie gevallen gaan wij nader beschouwen.

Voor $m = 2^n-1$ heeft men de volgende tabel

n	m	$\varphi(p_i^{s_i})$	L
2	3	2	2
3	7	6	6
4	3.5	2;4	4
5	31	30	30
6	3^2.7	6;6	6
7	127	126	126
8	3.5.17	2;4;16	16
9	7.73	6;72	72
10	3.11.31	2;10;30	30
11	23.89	22;88	88
12	3^2.5.7.13	6;4;6;12	12
13	8191	8190	8190
14	3.43.127	2;42;126	126
15	7.31.151	6;30;150	150
16	3.5.17.257	2;4;16;256	256
. . . . .			
29	233.1103.2089	232;1102;2088	39672
30	3^2.7.11.31.151.331	6;6;10;30;150;330	1650

en voor $m = 2^n+1$ heeft men

1	3	2	2
2	5	4	4
3	3^2	6	6
4	17	16	16
5	3.11	2;10	10
6	5.13	4;12	12
7	3.43	2;42	42
8	257	256	256
9	3^3.19	18;18	18
10	5^2.41	20;40	40
11	3.683	2;682	682
12	17.241	16;240	240
13	3.2731	2;2730	2730
14	5.29.113	4;28;112	112
15	3^2.11.331	6;10;330	330
16	65537	65536	65536
. . . . .			
29	3.59.3033169	2;58;3033168	3033168
30	5^2.13.41.61.1321	20;12;40;60;1320	1320

De ARRA reduceert verreweg het eenvoudigste mod $2^{30}\pm1$ of mod 2^{30}. Nu is bij $2^{30}\pm1$ de periode L echter vrij klein. Iets ingewikkelder, maar toch nog goed uitvoerbaar verloopt reductie mod $2^{29}\pm1$. Bij $m=2^{29}-1$ kan men a=3 nemen, want

de factor 8 in L is noodzakelijk wegens $3^{116} \equiv -1 \pmod{233}$
" " 9 " " " " " $3^{696} \equiv 826 \pmod{2089}$;
" " 19 " " " " " $3^{58} \equiv 620 \pmod{1103}$;
" " 29 " " " " " $3^{8} \equiv 37 \pmod{233}$.

In het geval dat $m = 2^{29}+1$ moet men $a \neq 2$ nemen, want 2 heeft uiteraard de periode 58; ook is a=3 uitgesloten. Echter is a=5 evenmin bruikbaar, want de factor 16 van L treedt in de periode van 5 niet op wegens $5^{\frac{1}{2}L} \equiv 1 \pmod{3033169}$. Het getal a=7 is echter wel bruikbaar, want de factor 16 van $L = 3033168 = 2^4.3.29.2179$ is noodzakelijk wegens $7^{\frac{1}{2}L} \equiv -1 \pmod{3033169}$;

de factor 3 is noodzakelijk wegens $7^{\frac{1}{3}L} \equiv 1554651 \pmod{3033169}$;
" " 29 " " " $7^{2} \equiv 49 \pmod{59}$ en
" " 2179 " " " $7^{1292} \equiv 1511637 \pmod{3033169}$.

Wij beschouwen thans nog het geval dat $m=2^{2n}$ wordt gekozen.

Eerst bewijzen wij de volgende hulpstelling.

Zij p een oneven priemgetal. Is c de kleinste exponent met $a^{c} \equiv 1 \pmod{p^{k}}$ en is $a^{c} \not\equiv 1 \pmod{p^{k+1}}$, dan is pc de kleinste exponent met $a^{pc} \equiv 1 \pmod{p^{k+1}}$ en $a^{pc} \not\equiv 1 \pmod{p^{k+2}}$.

Bewijs: Zij d de kleinste exponent met $a^{d} \equiv 1 \pmod{p^{k+1}}$, dan is $d \neq c$ en verder is dan $a^{d} \equiv 1 \pmod{p^{k}}$, dus $c \mid d$. Zij $d = ec$. Wegens $a^{c} = 1+p^{k}v$, waarin $p \nmid v$, is dan $a^{d} = (1+p^{k}v)^{e} \equiv 1+p^{k}ve \pmod{p^{k+1}}$, dus $p \mid ve$, dus $p \mid e$. Wegens $e = 1$ is dan $e = p$. Inderdaad is $a^{pc} = (1+p^{k}v)^{p} \equiv 1 \pmod{p^{k+1}}$ en verder is $a^{pc} = (1+p^{k}v)^{p} \equiv 1+p^{k+1}v \not\equiv 1 \pmod{p^{k+2}}$ wegens $p \nmid v$.

Gevolg: Is c de kleinste exponent met $a^{c} \equiv 1 \pmod{p}$ en is n de grootste exponent met $a^{c} \equiv 1 \pmod{p^{n}}$, dan is de exponent van a mod p^{k} (voor $k > n$) gelijk aan $p^{k-n}c$.

Voor p=2 luidt de stelling iets anders. Is c de kleinste exponent met $a^{c} \equiv 1 \pmod{2^{k}}$ en is $a^{c} \not\equiv 1 \pmod{2^{k+1}}$, dan is 2c de kleinste exponent met $a^{2c} \equiv 1 \pmod{2^{k+1}}$ en $a^{2c} \not\equiv 1 \pmod{2^{k+2}}$, mits $k \geq 2$.

Het bewijs van de eerste bewering loopt geheel als boven en wat de tweede bewering betreft, merke men op dat uit $a^{c} = 1+2^{k}v$ met $2 \nmid v$ volgt $a^{2c} = 1+2^{k+1}v+2^{2k}v^{2} \not\equiv 1 \pmod{2^{k+2}}$ mits $2k > k+1$, dus $k > 1$.

Gevolg: Is c de kleinste exponent met $a^{c} \equiv 1 \pmod{4}$ en is n de grootste exponent met $a^{c} \equiv 1 \pmod{2^{n}}$, dan is voor $k > n$ de kleinste exponent $d(2^{k})$ met $a^{d} \equiv 1 \pmod{2^{k}}$ gelijk aan $d(2^{k}) = 2^{k-n}c$.

Voor p=2 geven wij ook hiervan een tabel.

a	c	n	d(k)
3	2	3	2^{k-2}
5	1	2	2^{k-2}
7	2	4	2^{k-3}
9	1	3	2^{k-3}
11	1	3	2^{k-3}
13	1	2	2^{k-2}
15	2	5	2^{k-4}
17	1	4	2^{k-4}
19	2	3	2^{k-2}
21	1	2	2^{k-2}

De periode mod 2^{30} van het getal 3 is dus gelijk aan $2^{28}=268435456$.

Ten slotte zij nog opgemerkt dat de periode mod m van een getal a in het geval dat m de priemontbinding $p_1^{r_1}\ldots p_s^{r_s}$ bezit, het K.G.V. is der perioden mod $p_i^{r_i}$ van a, die op de bovengenoemde wijze samenhangen met de perioden van a mod p_i zelf (i=1,...,s).

§2. Toepassing van de rij van Fibonacci.

Een andere methode om "random-numbers" te maken, bestaat daaruit dat men de recurrente betrekking $u_{n+1} \equiv au_n \pmod p$ vervangt door een iets ingewikkelder recurrente betrekking, waarbij u_n afhangt van $u_{n-1}, u_{n-2}, \ldots$. Wij beschouwen het eenvoudige geval, dat $u_n = u_{n-1} + u_{n-2}$ en $u_o = 0$; $u_1=1$. Men krijgt dan de reeks van Fibonacci. Om deze nader te bestuderen voeren wij het getal $\omega > 1$ in, dat voldoet aan $\omega^2 - \omega - 1 = 0$. De andere wortel dezer vergelijking noemen wij $\bar\omega$. Zoals men - zo nodig door volledige inductie - inziet, gelden dan de volgende bekende eigenschappen

$$\sqrt{5} = 2\omega - 1; \quad \omega^2 = \omega + 1; \quad \frac{1}{\omega} = \omega - 1; \quad \omega + \bar\omega = 1; \quad \omega\bar\omega = -1.$$

$$\omega^n = u_n\omega + u_{n-1}$$

$$u_n = \frac{\omega^n - \bar\omega^n}{\omega - \bar\omega};$$

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

$u_n \mid u_m$, als $n \mid m$.

Wij beschouwen de getallen u_n gereduceerd mod p. Zij c het kleinste natuurlijke getal waarvoor $u_c \equiv 0 \pmod p$. Dus $\omega^c = u_c\omega + u_{c+1} \equiv u_{c+1} \pmod p$. Zij d willekeurig met $\omega^d \equiv a \pmod p$, waarbij a geheel rationaal. Zij $d = ce+r$ met $0 \leq r < d$. Dan is $\omega^r = \omega^d : \omega^{ce} \equiv a^d u_{c+1}^{-e} \pmod p$, dus ook ω^r is mod p congruent met een rationaal getal. Wegens de minimaaleigenschap van c is dan r=0, dus d=ce.

Zij verder C de kleinste exponent met $\omega^C \equiv 1 \pmod p$. Dan is dus $c \mid C$. Zij $C = vc$. Dan is v het kleinste getal met $u_{c+1}^v \equiv 1 \pmod p$. Immers $\omega^c = u_c\omega + u_{c-1} = u_c\omega + u_{c+1} - u_c \equiv u_{c+1} \pmod p$. Dus $u_{c+1}^v \equiv \omega^{vc} =$

$= \omega^c \equiv 1 \pmod p$ en als $w < v$ is $u_{c+1} \equiv \omega^{wc} \not\equiv 1 \pmod p$ wegens de minimaal eigenschap van $C = vc > wc$. Is omgekeerd v de kleinste exponent met $u_{c+1}^v \equiv 1 \pmod p$, dan is cv de kleinste exponent met $\omega^{cv} \equiv 1 \pmod p$. Immers $u_{c+1}^v \equiv \omega^{cv} \equiv 1 \pmod p$ en als $\omega^C \equiv 1 \pmod p$ met $C < cv$ en C minimaal, dan gold wegens $\omega^{cv} \equiv 1 \pmod p$ de betrekking $c \mid C \mid cv$ dus $C = wc$ met $w < v$. Dus $\omega^C = \omega^{wc} \equiv u_{c+1}^w \equiv 1 \pmod p$ in strijd met de minimaal eigenschap van v.

Wij onderstellen vervolgens dat $p \equiv +1 \pmod{10}$. Dan is $\left(\frac{5}{p}\right) = +1$ dus $5^{\frac{p-1}{2}} \equiv 1 \pmod p$, dus $(2\omega - 1)^{p-1} \equiv 1 \pmod p$ dus $(2\omega-1)^p \equiv 2\omega - 1 \pmod p$, dus $2^p \omega^p - 1 \equiv 2\omega - 1 \pmod p$, zodat men wegens $2^{p-1} \equiv 1 \pmod p$ krijgt $\omega^{p-1} \equiv 1 \pmod p$. Men heeft dus $c \mid C \mid p-1$. Omgekeerd: is $C \mid p-1$, dan is $\omega^C \equiv 1 \pmod p$, dus $\omega^{p-1} \equiv 1 \pmod p$, dus $(2\omega-1)^{p-1} \equiv 1 \pmod p$ dus $5^{\frac{p-1}{2}} \equiv 1 \pmod p$, dus $p \equiv \pm 1 \pmod{10}$.

Is echter $p \equiv \pm 3 \pmod{10}$, dan is $\left(\frac{5}{p}\right) = -1$, dus $5^{\frac{p-1}{2}} \equiv -1 \pmod p$, dus $(2\omega-1)^{p-1} \equiv -1 \pmod p$, dus $(2\omega-1)^p \equiv 1 - 2\omega \pmod p$, dus wegens $2^{p-1} \equiv 1 \pmod p$ krijgt men in dit geval $\omega^p \equiv 1 - \omega \pmod p$, dus $\omega^{p+1} \equiv \omega - \omega^2 = -1 \pmod p$, waaruit volgt dat $C \mid 2p+2$, $C \nmid p+1$. Omgekeerd is $C \mid 2p+2$, maar $C \nmid p+1$, dan is $\omega^{2p+2} \equiv 1 \pmod p$, maar $\omega^{p+1} \not\equiv 1 \pmod p$, dus $\omega^{p+1} \equiv -1 \pmod p$ (omdat p priem is in de ring $k(\omega)$ en omdat deze ring een hoofdideaalring is), dus $\omega^p \equiv -\frac{1}{\omega} = 1 - \omega \pmod p$, dus $(2\omega-1)^p \equiv -1 \pmod p$, dus $\left(\frac{5}{p}\right) = -1$, dus $p \equiv \pm 3 \pmod{10}$. In dit geval is wegens $C \nmid p+1$ zeker $c \neq C$, dus $v \neq 1$.

De factorisatie van de getallen u_n wordt vergemakkelijkt allereerst door de eigenschap $u_n \mid u_N$ voor $n \mid N$. Verder treedt een priemfactor p op in u_n waarbij $n = c(p)$, maar niet in u_m met $m < n$.
Zij $p \equiv +1 \pmod{10}$. Dan is dus $n \mid p-1$, dus $p-1 = nw \equiv 0 \pmod{10}$;
bij $p \equiv -1 \pmod{10}$ heeft men $n \mid p-1$, dus $p-1 = nw \equiv 8 \pmod{10}$;
" $p \equiv +3 \pmod{10}$ " " $n \mid p+1$, " $p+1 = nw \equiv 4 \pmod{10}$;
" $p \equiv -3 \pmod{10}$ " " $n \mid p+1$, " $p+1 = nw \equiv 8 \pmod{10}$.
Het getal $p-1$ of $p+1$ is dus een deler van die veelvouden van n, die $\equiv 0, 4$ of $8 \pmod{10}$ zijn. B.v.: $n=23$; $u_n = 28657$. Men kan het onderzoek als steeds beperken tot priemgetallen p, die $< \sqrt{28657}$ zijn. Men zoeke veelvouden van 23, die eindigen op 0,4 of 8. Bij het eerste geval is het kleinste veelvoud 230, maar 231 is niet priem. Bij het tweede geval is het kleinste veelvoud 184, maar ook 183 is niet priem. In het derde geval is het kleinste veelvoud 138. Dan is $p=137$ of 139, maar geen dezer getallen blijkt deelbaar te zijn op 28657. Het getal u_{23} is dus ondeelbaar.

Bij $n=37$, $u_n = 24157817$ zoeke men dus veelvouden van 37, die eindigen op 0,4 of 8. Reeds 74 levert ons $p = 73$ en inderdaad is $73 \mid u_{37}$. Ook het veelvoud 148 van 37 levert ons een priemfactor, nl. 149, van u_{37}. Dat $u_{37} : 73.149 = 9349$ priem is, volgt nu reeds uit het feit, dat $73 \nmid 9349$.

Wij onderzoeken thans het gedrag der getallen c, C en v nader. Wij weten $\omega^c \equiv u_{c+1} \pmod p$, dus $\bar{\omega}^c \equiv u_{c+1} \pmod p$, dus $u_{c+1}^2 \equiv (\omega\bar{\omega})^c \equiv$

$\equiv (-)^c \pmod p$, derhalve $u_{c+1}^4 \equiv 1 \pmod p$ dus $v \mid 4$.

Thans onderscheiden wij drie gevallen:

1. c oneven. Dan is $u_{c+1}^2 \equiv -1 \pmod p$, dus $v = 4$.
2. $c = 2d$, d oneven. Dan is $u_{c+1}^2 \equiv 1 \pmod p$, dus $u_{c+1} \equiv \pm 1 \pmod p$. Was $u_{c+1} \equiv -1 \pmod p$, dan was $\omega^{2d} = \omega^c \equiv u_{c+1} \equiv -1 = (-)^d \pmod p$, dus na vermenigvuldiging met $(-\bar{\omega})^d$ kreeg men $\omega^d \equiv \bar{\omega}^d \pmod p$, dus ω^d was rationaal (mod p) in strijd met de minimaliteit van c. Bijgevolg is $u_{c+1} \equiv 1 \pmod p$, dus $v = 1$.
3. $c = 2d$, d even. Dan is $u_{c+1}^2 \equiv 1 \pmod p$, dus $u_{c+1} \equiv \pm 1 \pmod p$. Was $u_{c+1} \equiv +1 \pmod p$, dan was $\omega^{2d} = \omega^c \equiv u_{c+1} \equiv 1 \pmod p$, dus na vermenigvuldiging met $\bar{\omega}^d$ kreeg men $\omega^d \equiv \bar{\omega}^d \pmod p$, dus ω^d was rationaal (mod p) in strijd met de minimaliteit van c. Bijgevolg is $u_{c+1} \equiv -1 \pmod p$, dus $v = 2$.

Wij krijgen dus, lettende op $C = cv$, het volgende overzicht:

c(mod 4)	v	C(mod 8)
± 1	4	4
0	2	0
2	1	± 2

Wij onderscheiden nu verder de volgende gevallen:

Is $p \equiv 11$ of $19 \pmod{20}$, dan is zoals wij zagen $C \mid p-1$, dus omdat $4 \nmid p-1$, is dan $v = 1$. Is $p \equiv 3$ of $7 \pmod{20}$, dan is zoals wij zagen $C \mid 2(p+1)$, maar $C \nmid p+1$. Dus C bevat meer factoren 2 dan het getal p+1, dat er tenminste 2 bevat. Bijgevolg is dan $8 \mid C$, dus $v = 2$. Is $p \equiv 13$ of $17 \pmod{20}$, dan is eveneens $C \mid 2(p+1)$ en $C \nmid p+1$, dus C bevat 1 factor 2 meer dan het getal p+1, dat er juist 1 bevat. Dus $4 \mid C$, $8 \nmid C$. Bijgevolg is dan $v = 4$.

Is $p \equiv 1$ of $9 \pmod{20}$, dan kan $v = 1$, 2 of 4 zijn. Het geval $v = 2$ leidt tot $8 \mid C \mid p-1$, dus $p \equiv 1$ of $9 \pmod{40}$. Wij krijgen dus het volgende overzicht

p(mod 20)	v	c(mod 4)	C(mod 8)	Opmerkingen
1	1,2,4	0,$\pm$1,2	0,$\pm$2,4	v = 2 slechts bij $p \equiv 1 \pmod{40}$
3	2	0	0	
7	2	0	0	
9	1,2,4	0,$\pm$1,2	0,$\pm$2,4	v = 2 slechts bij $p \equiv 9 \pmod{40}$
11	1	2	± 2	
13	4	± 1	4	
17	4	± 1	4	
19	1	2	± 2	

Voor p=2 heeft men voorts c=3; C=3 en voor p=5 tenslotte c=5; C=20. Is de periode $C=C(p)$ voor $p \neq 2$ bekend, dan volgt hieruit op precies dezelfde wijze als boven geschied is dat $C(p^k) = p^{k-n}C(p)$, als n de grootste exponent is met $p^n \mid \omega^C - 1$. Voor p=2 heeft men weer het iets afwijkende resultaat $C(2^k) = 2^{k-2}C(4)$, want $C(4) = 6$ en $\omega^6 - 1$ is deelbaar door 4, maar niet door 8. Dus $C(2^k) = 2^{k-2}.6 = 3.2^{k-1}$. Of er priemgetallen p zijn, waarvoor $p^2 \mid \omega^{C(p)} - 1$ onderzoeken wij hier niet nader.

Wij geven hieronder een staatje van de getallen c en C voor de priemgetallen p, waarbij alle getallen de bovenbeschouwde exponent n=1 is.

p	c	C	v
3	4	8	2
7	8	16	2
13	7	28	4
17	9	36	4
23	24	48	2
37	19	76	4
43	44	48	2
47	16	32	2
53	27	108	4
67	68	136	2
73	37	148	4
83	84	168	2
97	49	196	4
103	104	208	2
107	36	72	2
113	19	76	4
127	64	128	2

p	c	C	v
11	10	10	1
19	18	18	1
29	14	14	1
31	30	30	1
41	20	40	2
59	58	58	1
61	15	60	4
71	70	70	1
79	78	78	1
89	11	44	4
101	50	50	1
109	27	108	4
409	204	408	2