

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1953-2022

Deelbaarheidseigenschappen bij homogeen
lineair recurrente rijen van de derde orde

H.J.A. Duparc



Deelbaarheidseigenschappen bij homogeen lineair recurrente rijen van de derde orde

door H. J. A. DUPARC (Amsterdam)

Wij beschouwen de rij elementen $u_0, u_1, \dots$ gedefinieerd door

$$u_{n+3} = a_0 u_{n+2} + a_1 u_{n+1} + a_2 u_n \quad (n = 0, 1, \dots),$$

$u_0 = u_1 = 0, u_2 = 1$, waarbij a_0, a_1 en a_2 gehele getallen zijn en vragen ons af of bij gegeven natuurlijke m met $(a_2, m) = 1$ een natuurlijk getal H te vinden is zodanig dat

$$u_{n+H} \equiv u_n \pmod{m} \quad (n = 0, 1, \dots).$$

Elke dergelijke H blijkt een veelvoud te zijn van het kleinste natuurlijke dergelijke getal, dat wij C noemen. Het blijkt dat het getal C het kleinste natuurlijke getal is waarvoor de rest bij deling van x^C door $f(x) = x^3 - a_0 x^2 - a_1 x - a_2$ een veelterm $r_0 x^2 + r_1 x + r_2$ is met $r_0 \equiv r_1 \equiv 0 \pmod{m}, r_2 \equiv 1 \pmod{m}$.

Voor dit getal $C = C(f, m)$ gelden de volgende eigenschappen. $C(f, m)$ is het KGV der getallen $C(f, p_i^{r_i})$ ($i = 1, \dots, s$) als $m = p_1^{r_1} \dots p_s^{r_s}$ de kanonieke ontbinding van m in priemgetallen is; $C(f, p^r) = p^h C(f, p)$, waarbij h een geschikt gekozen geheel getal ≥ 0 en $\leq r-1$ is (hier en in het vervolg stelt p een priemgetal voor).

$C(f, p)$ is het KGV der getallen $C(f_j^{t_j}, p)$ ($j = 1, \dots, u$), waarbij mod p de kanonieke ontbinding van $f(x)$ luidt

$$(f_1(x))^{t_1} \dots (f_u(x))^{t_u}.$$

Het bewijs dezer bewering maakt gebruik van het feit dat de mod p gereduceerde veeltermen met gehele coëfficiënten een ontbindingsring vormen.

$C(f^t, p) = p C(f, p)$ voor $t = 2, 3$ en een willekeurig priemgetal p , behalve voor $t = 3, p = 2$. Dan geldt $C(f^3, 2) = 4C(f, 2)$.

$C(f, p) \mid p^N - 1$ als N de graad is van $f(x)$ en $f(x)$ irreducibel is mod p .

Voor bovengenoemde rij krijgt men hieruit de volgende resultaten.

Is $p \nmid D$, dan is $C(f, p) \mid p^3 - 1, p^2 - 1, p - 1$ al naar gelang $f(x)$ mod p uiteenvalt in 1, 2 resp. 3 irreducibele onderling verschillende factoren.

Is $p \mid D$, dan is $C(f, p) \mid p(p-1)$, behalve bij $p = 2$ en $f(x) \equiv (x-1)^3 \pmod{2}$. Dan is $C(f, p) = 4$.

Het kleinste getal $c = c(f, m)$ waarbij een geheel getal r te bepalen is met $u_{n+c} \equiv ru_n \pmod{m}$ ($n = 0, 1, \dots$) blijkt het kleinste getal c te zijn met $x^c \equiv r \pmod{m}$. Voor $c(f, m)$ gelden analoge eigenschappen als voor $C(f, m)$.

Het getal $v(f, m) = \frac{C(f, m)}{c(f, m)}$ blijkt geheel te zijn en slechts de waarden $\frac{e}{(e, c)}$ of $\frac{3e}{(e, c)}$ aan te nemen, waarbij e de exponent mod p van a_2 is.

Overeenkomstige eigenschappen gelden voor hogere orde rijen mod m , waarbij echter een verdere gevalsonderscheiding nodig blijkt.