MATH. SCAND. 44 (1979), 225–230

ON A CONJECTURE OF BRUCKMAN

TORLEIV KLØVE

In connection with problem 6044 in the Amer. Math. Monthly [1] P. Bruckman made some conjectures. Let $g(x)=x^4+x+1$ and define P_n by

$$3P_n = \prod_{k=1}^{n} g(\exp(2\pi ik/n)) .$$

Bruckman's conjectures were:

(A) $2^4 \mid P_n$ iff $n \equiv 0 \pmod{15}$; (B) $2^8 \mid P_n$ iff $n \equiv 0 \pmod{30}$;
(C) $3^3 \mid P_n$ iff $n \equiv 0 \pmod{13}$; (D) $3^7 \mid P_n$ iff $n \equiv 0 \pmod{39}$;
(E) $5 \mid P_n$ iff $n \equiv 0 \pmod{4}$; (F) $5^2 \mid P_n$ iff $n \equiv 0 \pmod{20}$;
(G) $7 \nmid P_n$ for all n; (H) $11 \mid P_n$ iff $n \equiv 0 \pmod{10}$.

In this paper we prove these conjectures as far as they are true. We will study a more general situatiion. Let

$$f(x) = x^r + a_1 x^{r-1} + \ldots + a_r$$

where $a_1, a_2, \ldots, a_r$ are integers, $a_r \neq 0$. Let

$$Q_n = Q_n(f) = \prod_{k=1}^{n} f(\exp(2\pi ik/n)), \qquad n \geqq 1 ,$$

$$Q_0 = 0 .$$

We will show that Q_n is always an integer and we characterize the set

$$\mathscr{X}_m(f) = \{n \mid Q_n(f) \equiv 0 \pmod{m}\} .$$

Let

$$\varphi_d(x) = \prod_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} (x - \exp(2\pi ik/n)) .$$

Then φ_d, which is a cyclotomic polynomial, has integral coefficients. Let $x_1, x_2, \ldots, x_r$ be zeros of f and let

---

Received April 19, 1978.

$$F_d = \prod_{k=1}^{r} \varphi_d(x_k) .$$

LEMMA 1. (i) *F_d is an integer for $d \geqq 1$.*
(ii) $Q_n = (-1)^{rn} \prod_{d \mid n} F_d$ *for* $n \geqq 1$.

PROOF. F_d is a symmetric polynomial in $x_1, x_2, \ldots, x_r$ with integral coefficients. Hence it is possible to express F_d as a polynomial in $a_1, a_2, \ldots, a_r$ with integral coefficients. Since $a_1, a_2, \ldots, a_r$ are integers, (i) follows. In (ii) we have

$$\begin{aligned} Q_n &= \prod_{k=1}^{n} \prod_{j=1}^{r} (\exp(2\pi ik/n) - x_j) \\ &= (-1)^{rn} \prod_{cd=n} \prod_{\substack{\gcd(k,n)=c \\ 1 \leqq k \leqq n}} \prod_{j=1}^{r} (x_j - \exp(2\pi ik/n)) \\ &= (-1)^{rn} \prod_{cd=n} \prod_{j=1}^{r} \prod_{\substack{\gcd(l,d)=1 \\ 1 \leqq l \leqq d}} (x_j - \exp(2\pi il/d)) \\ &= (-1)^{rn} \prod_{d \mid n} F_d . \end{aligned}$$

THEOREM 1. Q_n is an integer for all $n \geqq 0$.

PROOF. Follows immediately from lemma 1. Let

$$\mathscr{G}_m(f) = \{ n \in \mathscr{Z}_m(f) \mid \text{ if } d < n \text{ and } d \mid n, \text{ then } d \notin \mathscr{Z}_m(f) \} .$$

THEOREM 2. *$n \in \mathscr{Z}_m(f)$ iff $q \mid n$ for some $q \in \mathscr{G}_m(f)$.*

PROOF. By lemma 1 (ii), if $n \mid n_1$ then $Q_n \mid Q_{n_1}$. Hence, if $Q_n \equiv 0 \pmod{m}$, then $Q_{n_1} \equiv 0 \pmod{m}$ for all n_1 which are multiples of n, and so $\mathscr{Z}_m$ consists of the multiples of the set of generators $\mathscr{G}_m$.

Since $Q_n \equiv 0 \pmod{\prod_{i=1}^{s} p_i^{\alpha_i}}$ iff $Q_n \equiv 0 \pmod{p_i^{\alpha_i}}$ for $i = 1, 2, \ldots, s$, we will from now on only consider $m = p^\alpha$, where p is a prime.

LEMMA 2. (i) *If $p \nmid n$, then $F_{pn} \equiv F_n^{p-1} \pmod{p}$.*
(ii) *If $p \mid n$, then $F_{pn} \equiv F_n^p \pmod{p}$.*

PROOF. If $p \nmid n$, then it is well known that

$$\varphi_{pn}(x) = \frac{\varphi_n(x^p)}{\varphi_n(x)} .$$

If $h(x)$ is any polynomial with integral coefficients, then $h(x^p) = h(x)^p + ph_1(x)$ for some polynomial h_1 with integral coefficients. In particular

$$\varphi_n(x)\varphi_{pn}(x) = \varphi_n(x)^p + p\psi(x) .$$

For this to be possible $\psi(x) = \varphi_n(x).\ \psi_1(x)$ and so

$$\varphi_{pn}(x) = \varphi_n(x)^{p-1} + p\psi_1(x) .$$

Hence

$$F_{pn} = \prod_{k=1}^{r} \varphi_{pn}(x_k) = \prod_{k=1}^{r} \varphi_n(x_k)^{p-1} + p\Psi(x_1, x_2, \ldots, x_r) .$$

Here Ψ is a symmetric polynomial in $x_1, x_2, \ldots, x_r$ with integral coefficients and so $\Psi(x_1, x_2, \ldots, x_r)$ is an integer. Hence $F_{pn} \equiv F_n^{p-1} \pmod{p}$. If $p \mid n$, then $\varphi_{pn}(x) = \varphi_n(x^p)$. From this we prove (ii) similarly.

Before we go on with the study of $\mathscr{G}_{p^\alpha}$ we give a congruence for Q_n of another kind than those conjectured by Bruckman.

THEOREM 3. *We have* $Q_{pn} \equiv Q_n \pmod{p}$ *for all* n.

PROOF. If $Q_n \equiv 0 \pmod{p}$, then $Q_{pn} \equiv 0 \pmod{p}$ since $Q_n \mid Q_{pn}$. Suppose $Q_n \not\equiv 0 \pmod{p}$. Let $n = p^b n_1$ where $p \nmid n_1$. We show that

$$(-1)^{rp^\alpha n_1} Q_{p^\alpha n_1} \equiv (-1)^{rn_1} Q_{n_1} \pmod{p} \qquad \text{for all } \alpha \geqq 0 .$$

Let $d \mid n_1$. Then $Q_d \not\equiv 0 \pmod{p}$. Hence by lemma 2 (i) and Fermat's theorem, $F_{pd} \equiv 1 \pmod{p}$. By lemma 2 (ii), $F_{p^\beta d} \equiv 1 \pmod{p}$ for all $\beta \geqq 1$. By lemma 1 (i)

$$(-1)^{rp^\alpha n_1} Q_{p^\alpha n_1} = \prod_{d \mid p^\alpha n_1} F_d = \prod_{d \mid n_1} \prod_{\beta=0}^{\alpha} F_{p^\beta d} \equiv \prod_{d \mid n_1} F_d = (-1)^{rn_1} Q_{n_1} \pmod{p} .$$

Hence

$$(-1)^{rpn} Q_{pn} \equiv (-1)^{rn_1} Q_{n_1} \equiv (-1)^{rn} Q_n \pmod{p} .$$

If p is odd, then $(-1)^{rpn} = (-1)^{rn}$, and if $p = 2$, then $(-1)^{2rn} = 1 \equiv (-1)^{rn} \pmod{2}$.

THEOREM 4. *If* $Q_n \equiv 0 \pmod{p^\alpha}$ *for some* $\alpha \geqq 1$, *then* $Q_{pn} \equiv 0 \pmod{p^{\alpha+1}}$.

PROOF. Let $n = p^b n_1$ where $p \nmid n_1$. If $Q_n \equiv 0 \pmod{p^\alpha}$, then $Q_n \equiv 0 \pmod{p}$, and by lemma 1 (ii) $F_d \equiv 0 \pmod{p}$ for some $d \mid n$. By lemma 2 (i), $F_{d_1} \equiv 0 \pmod{p}$ for some $d_1 \mid n_1$ and so $F_{p^{b+1} d_1} \equiv 0 \pmod{p}$. Since $Q_n \cdot F_{p^{b+1} d_1} \mid Q_{pn}$ and $p^{\alpha+1} \mid Q_n F_{p^{b+1} d_1}$, the theorem follows.

Let

$$S_k = \sum_{i=1}^{r} x_i^k, \qquad k=0,1,2,\dots,$$

and

$$f_n(x) = \prod_{i=1}^{r} (x-x_i^n) = x^r + a_1^{(n)}x^{r-1} + \dots + a_r^{(n)} .$$

LEMMA 3. (i) *For* $n \geqq 0$ *we have* $Q_n = (-1)^{r(n+1)} f_n(1)$,
(ii) $S_k = -ka_k - \sum_{j=1}^{k-1} a_j S_{k-j}$ for $1 \leqq k < r$,
(iii) $S_k = -\sum_{j=1}^{r} a_j S_{k-j}$ *for* $k \geqq r$.
(iv) *For* $j=1,2,\dots,r$ *there exist polynomials* A_j *with integral coefficients such that*

$$j!\, a_j^{(n)} = A_j(S_n, S_{2n}, \dots, S_{jn}) .$$

PROOF. (i)

$$\begin{aligned} Q_n &= \prod_{k=1}^{n} \prod_{j=1}^{r} (\exp(2\pi ik/n) - x_j) \\ &= (-1)^{rn} \prod_{j=1}^{r} \prod_{k=1}^{n} (x_j - \exp(2\pi ik/n)) \\ &= (-1)^{rn} \prod_{j=1}^{r} (x_j^n - 1) \\ &= (-1)^{r(n+1)} \prod_{j=1}^{r} (1 - x_j^n) = (-1)^{r(n+1)} f_n(1) . \end{aligned}$$

(ii) and (iii) are Newton's equations and (iv) we get by solving for $a_j^{(n)}$ in Newton's equations for $f_n(x)$.

By lemma 3 (iii), S_k satisfies a linear recurrence, and so it is periodic modulo any integer m. More precisely, for each m there exist integers $K_m \geqq 0$ and $\varrho_m > 0$ such that if $k \geqq K_m$, then $S_{k+\varrho_m} \equiv S_k \pmod m$. If $\gcd(m, a_r) = 1$, then $K_m = 0$.

LEMMA 4. *If* p^γ *is the exact power of* p *which divides* $r!$ *and* $m = p^{\alpha+\gamma}$ *then*

$$f_{n+\varrho_m}(1) \equiv f_n(1) \pmod{p^\alpha}$$

for $n \geqq K_m$.

PROOF. By lemma 3, if $\varrho = \varrho_m$, then

$$r!\, f_{n+\varrho}(1) = r! + \sum_{j=1}^{r} \frac{r!}{j!} A_j(S_{n+\varrho}, S_{2n+2\varrho}, \dots, S_{jn+j\varrho})$$

$$\equiv r!+\sum_{j=1}^{r}\frac{r!}{j!}A_j(S_n, S_{2n}, \ldots, S_{jn})$$
$$= r!f_n(1) \pmod{p^{\alpha+\gamma}}\,.$$

Hence

$$f_{n+\varrho}(1) \equiv f_n(1) \pmod{p^\alpha}\,.$$

LEMMA 5. *Let m have the same meaning as in lemma 4. If $n \in \mathscr{G}_{p^\alpha}(f)$, $d=\gcd(n, \varrho_m)$, and $c \geqq K_m/d$, then $cd \in \mathscr{Z}_{p^\alpha}(f)$.*

PROOF. There exist integers a and b such that $cd=an+b\varrho_m$. We may assume that $an \geqq K_m$ since otherwise we replace a and b by $a+bl\varrho_m$ and $b-bln$ for some l. Then by lemmata 3 and 4

$$Q_{cd} = (-1)^{r(cd+1)}f_{cd}(1) \equiv (-1)^{r(cd+1)}f_{an}(1)$$
$$= (-1)^{r(cd+an)}Q_{an} \equiv 0 \pmod{p^\alpha}\,.$$

THEOREM 5. *If $p \nmid a_r$, then*

(i) $\mathscr{G}_{p^\alpha}(f) \neq \varnothing$ *for all* $\alpha \geqq 1$,
(ii) *if $n \in \mathscr{G}_{p^\alpha}(f)$, then $n \mid \varrho_m$ where $m=p^{\alpha+\gamma}$.*

PROOF. If $p \nmid a_r$, then $K_m=0$ and so

$$Q_{\varrho_m} = (-1)^{r(\varrho_m+1)}f_{\varrho_m}(1) \equiv (-1)^{r(\varrho_m+1)}f_0(1) = 0 \pmod{p^\alpha}\,.$$

This proves (i). Let $n \in \mathscr{G}_{p^\alpha}$ and $d=\gcd(n, \varrho_m)$. Then, by lemma 5, $d \in \mathscr{Z}_{p^\alpha}$. Since $d \mid n$, $d=n$ by the definition of $\mathscr{G}_{p^\alpha}$. Hence $n=d \mid \varrho_m$.

THEOREM 6. *If $p \mid a_r$ and $n \in \mathscr{G}_p(f)$, then $n \mid \varrho_m$ where $m=p^{1+\gamma}$.*

PROOF. Let $d=\gcd(n, \varrho_m)$ and choose β such that $p^\beta d \geqq K_m$. Then, by lemma 5, $Q_{p^\beta d} \equiv 0 \pmod p$ and so, by theorem 3, $Q_d \equiv 0 \pmod p$. Hence $n=d \mid \varrho_m$.

For $g(x)=x^4+x+1$, $r=4$ and $a_r=1$, I have made a computer program to compute Q_n using lemma 3. The program also computed $\mathscr{G}_{p^\alpha}(g)$ for a number of p^α's by first computing ϱ_m and then testing Q_n for $n \mid \varrho_m$ to find if it is congruent to 0 modulo p^α. Some of the results are given in the following table which in particular proves that conjectures A, B, E, and H are true, whereas C, D, and F have to be modified and G is false.

Table

p^α	$\mathscr{G}_{p^\alpha}(g)$
$2^\alpha,\ 1 \leqq \alpha \leqq 9$	$\{15 \cdot 2^{[(\alpha-1)/4]}\}$
3	$\{1\}$
$3^\alpha,\ 2 \leqq \alpha \leqq 5$	$\{3^{\alpha-1}, 13 \cdot 3^{[(\alpha-2)/3]}\}$
5	$\{4\}$
5^2	$\{20, 124\}$
5^3	$\{100, 124\}$
7	$\{400\}$
7^2	$\{400\}$
11	$\{10\}$
13	$\{2380\}$
17	$\{16\}$
19	$\{18\}$
23	$\{11\}$
29	$\{14\}$

In the entries for 2^α and 3^α, $[x]$ denotes the greatest integer $\leqq x$.

I thank Helge Tverberg who pointed out Bruckman's conjectures to me. Also, lemma 3 is due to him.

REFERENCE

1. *Solution to problem* 6044, Amer. Math. Monthly 84 (1977), 392–394.

DEPARTMENT OF MATHEMATICS
ALLÉGT. 53–55
N-5014 BERGEN-UNIVERSITETET
NORWAY