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

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

\[
Q_n = Q_n(f) = \prod_{k=1}^{n} f(\exp(2\pi ik/n)), \quad n \geq 1 ,
\]

\[
Q_0 = 0 .
\]

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

\[
\mathcal{I}_m(f) = \{ n \mid Q_n(f) \equiv 0 \) (mod \( m \)) \} .
\]

Let

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

Then \( \varphi_d \), 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 \( d \geq 1 \).
(ii) \( Q_n = (-1)^n \prod_{d|n} F_d \) for \( n \geq 1 \).

**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

\[
Q_n = \prod_{k=1}^{n} \prod_{j=1}^{r} (\exp(2\pi ik/n) - x_j)
\]

\[
= (-1)^n \prod_{cd=n} \prod_{\gcd(k, n) = c} \prod_{1 \leq k \leq n} (x_j - \exp(2\pi ik/n))
\]

\[
= (-1)^n \prod_{cd=n} \prod_{j=1}^{r} \prod_{\gcd(l, d) = 1} \prod_{1 \leq l \leq d} (x_j - \exp(2\pi il/d))
\]

\[
= (-1)^n \prod_{d|n} F_d .
\]

**Theorem 1.** \( Q_n \) is an integer for all \( n \geq 0 \).

**Proof.** Follows immediately from lemma 1. Let

\[ G_m(f) = \{ n \in \mathcal{X}_m(f) \mid \text{if } d \nmid n \text{ and } d|n, \text{ then } d \notin \mathcal{X}_m(f) \} . \]

**Theorem 2.** \( n \in \mathcal{X}_m(f) \) iff \( q \mid n \) for some \( q \in G_m(f) \).

**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 \( \mathcal{X}_m \) consists of the multiples of the set of generators \( G_m \).

Since \( Q_n \equiv 0 \pmod{\prod_{i=1}^{s} p_i^{n_i}} \) iff \( Q_n \equiv 0 \pmod{p_i^{n_i}} \) for \( i = 1, 2, \ldots, s \), we will from now on only consider \( m = p^s \), 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 \( \psi(x) = \varphi_n(x) \cdot \psi_1(x) \) 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 \( \Psi \) 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 \( \mathcal{G}_p \), 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 \( Q_n \neq 0 \pmod{p} \). Let \( n = p^b n_1 \) where \( p \nmid n_1 \). We show that
\[
(-1)^{r_{pn}^n}Q_{p^n_{n_1}} \equiv (-1)^{r_{n_1}}Q_{n_1} \pmod{p} \quad \text{for all } \alpha \geq 0 .
\]
Let \( d \mid n_1 \). Then \( Q_d \equiv 0 \pmod{p} \). Hence by lemma 2 (i) and Fermat's theorem, \( F_{pd} \equiv 1 \pmod{p} \). By lemma 2 (ii), \( F_{p^d} \equiv 1 \pmod{p} \) for all \( \beta \geq 1 \). By lemma 1 (i)
\[
(-1)^{r_{pn}^n}Q_{p^n_{n_1}} = \prod_{d \mid n_1} F_d = \prod_{d \mid n_1} \prod_{\beta = 0}^\alpha F_{p^\beta d} \equiv \prod_{d \mid n_1} F_d = (-1)^{r_{n_1}^n}Q_{n_1} \pmod{p} ,
\]
Hence
\[
(-1)^{r_{pn}}Q_{pn} \equiv (-1)^{r_{n_1}}Q_{n_1} \equiv (-1)^nQ_n \pmod{p} .
\]
If \( p \) is odd, then \( (-1)^{r_{pn}} = (-1)^r \), and if \( p = 2 \), then \( (-1)^{2r} = 1 \equiv (-1)^r \pmod{2} \).

**Theorem 4.** If \( Q_n \equiv 0 \pmod{p^\alpha} \) for some \( \alpha \geq 1 \), 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), \( F_{d_i} \equiv 0 \pmod{p} \) for some \( d_i \mid n_1 \) and so \( F_{p^{\alpha+1}d_i} \equiv 0 \pmod{p} \). Since \( Q_n \cdot F_{p^{\alpha+1}d_i} \mid Q_{pn} \) and \( p^{\alpha+1} \mid Q_n F_{p^{\alpha+1}d_i} \), the theorem follows.
Let

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

and

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

**Lemma 3.** (i) For $n \geq 0$ we have $Q_n = (-1)^{(n+1)} f_n(1)$,

(ii) $S_k = -ka_k - \sum_{j=1}^{k-1} a_j S_{k-j}$ for $1 \leq k < r$,

(iii) $S_k = -\sum_{j=1}^{r} a_j S_{k-j}$ for $k \geq r$.

(iv) For $j=1,2,\ldots,r$ there exist polynomials $A_j$ with integral coefficients such that

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

**Proof.** (i) $Q_n = \prod_{k=1}^{n} \prod_{j=1}^{r} (\exp(2\pi ik/n) - x_j)$

$$= (-1)^n \prod_{j=1}^{r} \prod_{k=1}^{n} (x_j - \exp(2\pi ik/n))$$

$$= (-1)^n \prod_{j=1}^{r} (x_j^n - 1)$$

$$= (-1)^{(n+1)} \prod_{j=1}^{r} (1 - x_j^n) = (-1)^{(n+1)} f_n(1).$$

(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 $K_m \geq 0$ and $q_m > 0$ such that if $k \geq K_m$, then $S_{k+q_m} \equiv S_k \pmod{m}$. If $\gcd(m,a_r)=1$, then $K_m=0$.

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

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

for $n \geq K_m$.

**Proof.** By lemma 3, if $q=q_m$, then

$$r! f_{n+q}(1) = r! + \sum_{j=1}^{r} r! A_j(S_{n+q}, S_{2n+2q}, \ldots, S_{jn+jq}).$$
ON A CONJECTURE OF BRUCKMAN

\[ \equiv r! + \sum_{j=1}^{r} \frac{r!}{j!} A_j(S_{m}, S_{2n}, \ldots, S_{jn}) \]

\[ = r! f_n(1) \pmod{p^{a+y}}. \]

Hence

\[ f_{n+\vartheta}(1) \equiv f_n(1) \pmod{p^\vartheta}. \]

**Lemma 5.** Let \( m \) have the same meaning as in lemma 4. If \( n \in \mathcal{G}_{p^\alpha}(f) \), \( d = \gcd(n, q_m) \), and \( c \geq K_m/d \), then \( cd \in \mathcal{Z}_{p^\gamma}(f) \).

**Proof.** There exist integers \( a \) and \( b \) such that \( cd = an + bq_m \). We may assume that \( an \geq K_m \) since otherwise we replace \( a \) and \( b \) by \( a + blq_m \) and \( b - bln \) for some \( l \). Then by lemmata 3 and 4

\[ Q_{cd} = (-1)^{r(c+1)}f_{cd}(1) \equiv (-1)^{r(c+1)}f_{an}(1) \]

\[ = (-1)^{r(c+an)}Q_{an} \equiv 0 \pmod{p^\vartheta}. \]

**Theorem 5.** If \( p \nmid a_r \), then

(i) \( \mathcal{G}_{p^\alpha}(f) \neq \emptyset \) for all \( \alpha \geq 1 \),

(ii) if \( n \in \mathcal{G}_{p^\alpha}(f) \), then \( n \mid q_m \) where \( m = p^{a+y} \).

**Proof.** If \( p \nmid a_r \), then \( K_m = 0 \) and so

\[ Q_{qm} = (-1)^{r(a+1)}f_{qm}(1) \equiv (-1)^{r(a+1)}f_0(1) = 0 \pmod{p^\vartheta}. \]

This proves (i). Let \( n \in \mathcal{G}_{p^\alpha} \) and \( d = \gcd(n, q_m) \). Then, by lemma 5, \( d \in \mathcal{Z}_{p^\gamma} \).

Since \( d \mid n \), \( d = n \) by the definition of \( \mathcal{G}_{p^\alpha} \). Hence \( n = d \mid q_m \).

**Theorem 6.** If \( p \mid a_r \) and \( n \in \mathcal{G}_{p}(f) \), then \( n \mid q_m \) where \( m = p^{1+y} \).

**Proof.** Let \( d = \gcd(n, q_m) \) and choose \( \beta \) such that \( p^\beta d \geq K_m \). Then, by lemma 5, \( Q_{p^\beta d} \equiv 0 \pmod{p} \) and so, by theorem 3, \( Q_d \equiv 0 \pmod{p} \). Hence \( n = d \mid q_m \).

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 \( \mathcal{G}_{p^\gamma}(g) \) for a number of \( p^\alpha \)'s by first computing \( q_m \) and then testing \( Q_n \) for \( n \mid q_m \) to find if it is congruent to 0 modulo \( p^\vartheta \). 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

<table>
<thead>
<tr>
<th>$p^a$</th>
<th>$\mathcal{I}_{p^a}(g)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^a$, $1 \leq a \leq 9$</td>
<td>${15 \cdot 2^{[(a-1)/4]}}$</td>
</tr>
<tr>
<td>3</td>
<td>${1}$</td>
</tr>
<tr>
<td>$3^a$, $2 \leq a \leq 5$</td>
<td>${3^{a-1}, 13 \cdot 3^{[(a-2)/3]}}$</td>
</tr>
<tr>
<td>5</td>
<td>${4}$</td>
</tr>
<tr>
<td>$5^2$</td>
<td>${20, 124}$</td>
</tr>
<tr>
<td>$5^3$</td>
<td>${100, 124}$</td>
</tr>
<tr>
<td>7</td>
<td>${400}$</td>
</tr>
<tr>
<td>$7^2$</td>
<td>${400}$</td>
</tr>
<tr>
<td>11</td>
<td>${10}$</td>
</tr>
<tr>
<td>13</td>
<td>${2380}$</td>
</tr>
<tr>
<td>17</td>
<td>${16}$</td>
</tr>
<tr>
<td>19</td>
<td>${18}$</td>
</tr>
<tr>
<td>23</td>
<td>${11}$</td>
</tr>
<tr>
<td>29</td>
<td>${14}$</td>
</tr>
</tbody>
</table>

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

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

REFERENCE