#A30 INTEGERS 10 (2010), 357-363

FLAT CYCLOTOMIC POLYNOMIALS OF ORDER FOUR AND HIGHER

Nathan Kaplan
Department of Mathematics, Harvard University, Cambridge, MA
nkaplan@math.harvard.edu

Received: 7/15/09, Revised: 3/12/10, Accepted: 3/18/10, Published: 7/19/10

Abstract

In this article we prove a result about sets of coefficients of cyclotomic polynomials. We then give corollaries related to flat cyclotomic polynomials and establish the first known infinite family of flat cyclotomic polynomials of order four. We end with some questions related to flat cyclotomic polynomials of order four and five.

1. Introduction

The nth cyclotomic polynomial is the monic polynomial whose roots are the primitive nth roots of unity. It is defined by

$$\Phi_n(x) = \prod_{\substack{a=1 \\ (a,n)=1}}^{n} (x - e^{2\pi i a/n}).$$

The degree of Φ_n is $\phi(n)$, where ϕ is the Euler totient function. We say that the order of a cyclotomic polynomial is the number of odd primes dividing n.

We can factor

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

The following proposition allows us to focus on odd squarefree values of n for the rest of the paper. See [8] for a proof of this and for other general results about cyclotomic polynomials.

Proposition 1. *Let p be a prime.*
If $p \mid n$ then $\Phi_{pn}(x) = \Phi_n(x^p)$.
If $p \nmid n$ then $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.
If $n > 1$ is odd then $\Phi_{2n}(x) = \Phi_n(-x)$.

Let $\Phi_n(x) = \sum_{k=0}^{\phi(n)} a_n(k)x^k$. We put $a_n(k) = 0$ if $k < 0$ or $k > \phi(n)$. Let $V_n = \{a_n(k) : 0 \le k \le \phi(n)\}$ denote the set of coefficients of $\Phi_n(x)$. It is easy to verify from the definition of $\Phi_n(x)$ that for $n > 1$, $\Phi_n(x) = x^{\phi(n)}\Phi_n(x^{-1})$. This implies that for $n > 1$, $V_n = \{a_n(k) : 0 \le k \le \frac{\phi(n)}{2}\}$. We say that $A(n) = \max_k\{|a_n(k)|\}$ is the height of $\Phi_n(x)$. Several recent papers have studied n for which $A(n)$ is large, for example, [1, 6]. It is also interesting to attempt to classify n such that $A(n)$ is small. If $A(n) = 1$ we say that $\Phi_n(x)$ is flat. It is easy to show that, for odd primes $p < q$, we have $V(p) = \{1\}$ and $V(pq) = \{-1, 0, 1\}$ and therefore $A(p) = A(pq) = 1$. Bachman gave the first infinite family of flat cyclotomic polynomials of order three [3], and this family was expanded by Kaplan [7], who proved the following.

Theorem 2. ([7]) *Let $p < q < r$ be primes such that $r \equiv \pm 1 \pmod{pq}$. Then $A(pqr) = 1$.*

There exist flat cyclotomic polynomials of order three that are not of this form. It would be an interesting and difficult problem to classify them. Beiter has classified all flat cyclotomic polynomials of the form $\Phi_{3qr}(x)$ [4], but not much is known about flat cyclotomic polynomials of the form $\Phi_{pqr}(x)$ for $p \ge 5$ or flat cyclotomic polynomials of order greater than three.

Recently, Broadhurst [5] has made some conjectures about flat cyclotomic polynomials of order three. Let $p < q < r$ be odd primes with w the unique integer $0 < w \le \frac{pq-1}{2}$ satisfying $r \equiv \pm w \pmod{pq}$.

(i) If $w = 1$ then we say that $[p, q, r]$ is of Type 1.

(ii) If $w > 1$, $q \equiv 1 \pmod{pw}$, and $p \equiv 1 \pmod{w}$ then we say that $[p, q, r]$ is of Type 2.

(iii) If $w > p$, $q > p(p-1)$, $q \equiv \pm 1 \pmod{p}$ and $w \equiv \pm 1 \pmod{p}$, and in the case where $w \equiv 1 \pmod{p}$ we have $wp \nmid q + 1$ and $wp \nmid q - 1$, then we say that $[p, q, r]$ is of Type 3.

Conjecture. ([5])

(i) *If $[p, q, r]$ is of Type 1 or 2, then $A(pqr) = 1$.*

(ii) *If $[p, q, r]$ is not of Type 1,2, or 3, then $A(pqr) > 1$.*

(iii) *If $[p, q, r]$ is of Type 3, then $A(pqr) = 1$ if and only if $\frac{\Phi_{pq}(x^s)}{\Phi_{pq}(x)}$ is flat for the smallest positive integer s such that $s \equiv 1 \pmod{p}$ and $s \equiv \pm r \pmod{pq}$.*

Note that Theorem 2 states that if $[p, q, r]$ is of Type 1, then $A(pqr) = 1$. This conjecture, if true, goes a long way towards a complete classification of flat cyclotomic polynomials of order three. It would remain to give conditions on $[p, q, r]$ of

Type 3 for which $\frac{\Phi_{pq}(x^s)}{\Phi_{pq}(x)}$ is flat for the s described in the conjecture. Broadhurst has also conjectured bounds on the number of $[p, q, r]$ of Type 3 which give flat cyclotomic polynomials [5].

The main result of this paper, Theorem 4, is a natural generalization of Theorem 2 in [7].

Theorem 3. (Kaplan, 2007) *Let $p < q < r < s$ be primes such that $r \equiv \pm s \pmod{pq}$. Then $A(pqr) = A(pqs)$.*

Let

$$\Psi_n(x) = \frac{x^n - 1}{\Phi_n(x)} = \sum_{k=0}^{n-\phi(n)} c_k x^k$$

denote the nth inverse cyclotomic polynomial. We can easily see that $\deg(\Psi_n(x)) = n - \phi(n)$. We put $c_k = 0$ if $k < 0$ or $k > n - \phi(n)$. These polynomials have been studied recently by Moree [10]. They will be used in the proof of Theorem 4.

2. The Main Result

In this paper we will prove the following result which applies to cyclotomic polynomials of arbitrary order, but requires slightly stronger assumptions than Theorem 3.

Theorem 4. *Let $2 < p_1 < p_2 < \cdots < p_r$ be primes and $n = p_1 \cdots p_r$. Let s, t be primes satisfying $n < s < t$ and $s \equiv t \pmod{n}$. Then $V_{ns} = V_{nt}$.*

Proof. We may suppose that $r \geq 2$ and therefore $n \geq 15$ since for any odd primes $p < q$ we have $V(pq) = \{-1, 0, 1\}$.

For simplicity we will change our notation slightly. Let

$$\Phi_{ns}(x) = \sum_{i=0}^{(p_1-1)\cdots(p_r-1)(s-1)} b_i x^i,$$

and

$$\Phi_{nt}(x) = \sum_{i=0}^{(p_1-1)\cdots(p_r-1)(t-1)} d_i x^i.$$

We will first show that $V_{ns} \subseteq V_{nt}$ by showing that for any coefficient $b_l \in V_{ns}$, there is a coefficient $d_m \in V_{nt}$ with $d_m = b_l$.

We have

$$\Phi_{ns}(x) = \frac{\Phi_n(x^s)}{\Phi_n(x)} = \frac{\left(\frac{x^n-1}{\Phi_n(x)}\right)\Phi_n(x^s)}{x^n-1} = \frac{\Psi_n(x)\Phi_n(x^s)}{x^n-1}.$$

Note that $\deg(\Psi_n(x)) = n - \phi(n) = n - (p_1-1)\cdots(p_r-1)$. We have assumed that $s > \deg(\Psi_n(x))$.

Similarly, we have

$$\Phi_{nt}(x) = \frac{\Phi_n(x^t)}{\Phi_n(x)} = \frac{\Psi_n(x)\Phi_n(x^t)}{x^n-1}.$$

By expanding $\frac{1}{x^n-1} = -(1+x^n+x^{2n}+\cdots)$, we have

$$\Phi_{ns}(x) = -\Psi_n(x)\Phi_n(x^s)(1+x^n+x^{2n}+\cdots),$$

and

$$\Phi_{nt}(x) = -\Psi_n(x)\Phi_n(x^t)(1+x^n+x^{2n}+\cdots).$$

Let

$$\Phi_n(x) = \sum_{j=0}^{(p_1-1)\cdots(p_r-1)} a_j x^j, \quad \text{and} \quad \Psi_n(x) = \sum_{i=0}^{n-\phi(n)} c_i x^i.$$

The terms of $\Psi_n(x)\Phi_n(x^s)$ are of the form $c_i a_j x^{i+js}$. Similarly the terms of $\Psi_n(x)\Phi_n(x^t)$ are of the form $c_i a_j x^{i+jt}$. Since $s \equiv t \pmod{n}$, $i+js \equiv i+jt \pmod{n}$.

For a fixed l, consider the set of (i,j) such that $c_i \neq 0$ and $i+js = l$. Since $c_i \neq 0$ implies that $0 \le i \le n-\phi(n) < s$, there is at most one pair (i,j) in this set. Similarly for a fixed m, the set of (i,j) such that $c_i \neq 0$ and $i+jt = m$ has at most one element.

We see that

$$b_l = -\sum_{(i,j)} c_i a_j,$$

where the sum is taken over all pairs (i,j) such that $i+js \le l$, $i+js \equiv l \pmod{n}$, and $c_i \neq 0$. Similarly,

$$d_m = -\sum_{(i,j)} c_i a_j,$$

where the sum is taken over all pairs (i,j) such that $i+jt \le m$, $i+jt \equiv m \pmod{n}$, and $c_i \neq 0$.

For any integer l with $0 \leq l \leq \deg(\Phi_{ns}(x)) = \phi(n)(s-1)$, we can write $l = ks+\alpha$ where $k, \alpha \in \mathbb{Z}$ and $0 \leq \alpha < s$, in a unique way. Note that $k < \phi(n)$. Now let $m = kt + \alpha$. Since $ks + \alpha \leq \phi(n)(s-1)$, we have

$$kt + \alpha \leq \phi(n)(s-1) + k(t-s) < \phi(n)(s-1) + \phi(n)(t-s) = \deg(\Phi_{nt}(x)).$$

Suppose $c_i \neq 0$. We have $i + js \leq ks + \alpha$ if and only if $j \leq k + \frac{\alpha - i}{s}$. Since j is always an integer we have $i+js \leq ks+\alpha$ if and only if $j \leq k+\lfloor \frac{\alpha-i}{s} \rfloor$. If $\alpha \geq i$, then $\lfloor \frac{\alpha-i}{s} \rfloor = 0$. Since $\alpha \geq 0$ and $c_i \neq 0$ implies $i \leq n - \phi(n) < s$, we have $\lfloor \frac{\alpha-i}{s} \rfloor = -1$ for $\alpha < i$.

Similarly $i + jt \leq kt + \alpha$ if and only if $j \leq k + \lfloor \frac{\alpha-i}{t} \rfloor$. Since $-t < -s < -i \leq \alpha - i \leq \alpha < s < t$ we see that $\lfloor \frac{\alpha-i}{s} \rfloor = \lfloor \frac{\alpha-i}{t} \rfloor$. Therefore $i + js \leq ks + \alpha$ if and only if $i + jt \leq kt + \alpha$, and $b_l = d_m$. So for any coefficient b_l of $\Phi_{ns}(x)$, there is a coefficient d_m of $\Phi_{nt}(x)$ with $d_m = b_l$ and $V_{ns} \subseteq V_{nt}$.

Now we will show that $V_{nt} \subseteq V_{ns}$ by showing that for any coefficient $d_m \in V_{nt}$ there is a coefficient $b_l \in V_{ns}$ such that $b_l = d_m$. If $m \geq \frac{\deg(\Phi_{nt}(x))}{2}$ then $m' = \deg(\Phi_{nt}(x)) - m \leq \frac{\deg(\Phi_{nt}(x))}{2}$. Since $d_m = d_{m'}$, without loss of generality we may suppose that $m \leq \frac{\deg(\Phi_{nt}(x))}{2}$. Given m we can write $m = kt + \beta$ where $k, \beta \in \mathbb{Z}$ and $0 \leq \beta < t$ in a unique way. Note that $k < \frac{\phi(n)}{2}$. Suppose $c_i \neq 0$. As in the previous paragraphs we have $i + jt \leq kt + \beta$ if and only if $j \leq k + \lfloor \frac{\beta-i}{t} \rfloor$.

Let $\alpha \equiv \beta \pmod{n}$ with $0 \leq \alpha < n < s$. Now consider $l = ks + \alpha$. We have $ks + \alpha < (\frac{\phi(n)}{2} + 1)s \leq (\phi(n) - 1)s < \phi(n)(s-1) = \deg(\Phi_{ns}(x))$ since $4 \leq \phi(n)$ for all $n \geq 7$.

If $\beta < i$, then $\beta < n$ and so $\alpha = \beta$. We see that $\lfloor \frac{\beta-i}{t} \rfloor = \lfloor \frac{\alpha-i}{s} \rfloor = -1$ and $b_l = d_m$. Suppose that $\beta \geq i$. Then $\lfloor \frac{\beta-i}{t} \rfloor = 0$. Since $\alpha < n < s$, we have $\lfloor \frac{\alpha-i}{s} \rfloor \leq 0$. If $\lfloor \frac{\alpha-i}{s} \rfloor = 0$, then clearly $i + js \leq l$ if and only if $i + jt \leq m$, and $b_l = d_m$.

Suppose there exists a pair (i, j) such that $i + js \equiv l \pmod{n}$, $c_i \neq 0$, $i + jt \leq kt + \beta$, but $i + js > ks + \alpha$. This implies that $j \leq k$ and $j > k + \lfloor \frac{\alpha-i}{s} \rfloor$. Therefore $\lfloor \frac{\alpha-i}{s} \rfloor = -1$ and $j = k$. So $i + ks \equiv ks + \alpha \pmod{n}$ and $i > \alpha$. This implies $i - \alpha \equiv 0 \pmod{n}$. Since $i - \alpha > 0$ we have $i \geq n > n - \phi(n)$, which contradicts $c_i \neq 0$. This implies that such a pair (i, j) does not exist. So $i + jt \leq kt + \beta$ if and only if $i + js \leq ks + \alpha$, and therefore $b_l = d_m$. So for any coefficient d_m of $\Phi_{nt}(x)$, there is a coefficient b_l of $\Phi_{ns}(x)$ with $b_l = d_m$, and thus $V_{nt} \subseteq V_{ns}$. □

3. Some Consequences and Open Questions

Several corollaries follow directly from Theorem 4.

Corollary 5. *Let $2 < p_1 < p_2 < \cdots < p_r$ be primes and $n = p_1 \cdots p_r$. Let s, t be primes satisfying $n < s < t$ and $s \equiv t \pmod{n}$. We have $A(ns) = A(nt)$.*

It is unclear how much we can weaken the assumption in Theorem 4 that $n < s < t$. The result is not true if we simply require that $p_r < s < t$. For example $V(5 \cdot 7 \cdot 13 \cdot 17) \subsetneq V(5 \cdot 7 \cdot 13 \cdot 4567)$.

Corollary 6. *Let $n = p_1 p_2 \cdots p_r$ be a product of distinct odd primes. If there exists a prime $s > n$ such that $\Phi_{ns}(x)$ is flat, then there are infinitely many flat cyclotomic polynomials of order $r+1$. In particular, $A(nt) = 1$ whenever t is a prime such that $t > n$ and $t \equiv s \pmod{n}$.*

This corollary follows from Dirichlet's theorem for primes in arithmetic progressions.

We note that $A(3 \cdot 5 \cdot 31 \cdot 929) = 1$.

Corollary 7. *There are infinitely many flat cyclotomic polynomials of order four. In particular, given any prime s congruent to -1 modulo 465, $A(3 \cdot 5 \cdot 31 \cdot s) = 1$.*

Recently Arnold and Monagan have introduced improved methods for quickly computing the heights of cyclotomic polynomials and have made much of their data available online [1, 2]. In particular, there are 1389 flat cyclotomic polynomials of order four with $n < 3 \cdot 10^8$. They are all of the form $n = pqrs$ where $q \equiv -1 \pmod{p}$, $r \equiv \pm 1 \pmod{pq}$ and $s \equiv \pm 1 \pmod{pqr}$. We suspect that all flat cyclotomic polynomials of order four are of this form. In our limited computations it appears that all of these polynomials are flat. We also have reason to believe the following.

Conjecture. *If $A(n) > 1$ then for any prime p, $A(pn) > 1$.*

It is unknown whether there are any flat cyclotomic polynomials of order greater than four. There are none of order five with $n < 6.26 \cdot 10^8$ [1, 2]. For primes (p, q, r, s, t) satisfying $q \equiv -1 \pmod{p}$, $r \equiv -1 \pmod{pq}$, $s \equiv -1 \pmod{pqr}$ and $t \equiv -1 \pmod{pqrs}$, $\Phi_{pqrst}(x)$ is not necessarily flat. Andrew Arnold recently computed the height of a cyclotomic polynomial satisfying these congruence conditions. For $(p, q, r, s, t) = (3, 5, 29, 2609, 2269829)$, $A(pqrst) = A(2576062979535) = 2$. Many of the above observations are based on computations done by Tiankai Liu [9].

Acknowledgments. I would like to thank Joe Gallian for running the University of Minnesota Duluth summer research program where I was first introduced to this topic. I would like to thank Tiankai Liu for performing calculations which were very helpful for the last section of this paper and Andrew Arnold for answering some computational questions. I would like to thank the referee for several useful comments and Sam Elder for helpful discussions related to this project.

References

[1] A. Arnold, M. Monagan, Calculating cyclotomic polynomials of very large height, submitted to Math. Comp.

[2] A. Arnold, M. Monagan, Data on the heights and lengths of cyclotomic polynomials, available: http://www.cecm.sfu.ca/∼ada26/cyclotomic/.

[3] G. Bachman, Flat cyclotomic polynomials of order three, Bull. London Math. Soc. **38** (2006), 53-60.

[4] M. Beiter, Coefficients of the cyclotomic polynomial, $F_{3qr}(x)$, Fibonacci Quart., **16** (1978), 302-306.

[5] D. Broadhurst, Flat ternary cyclotomic polynomials,
http://tech.groups.yahoo.com/group/primenumbers/message/20305.

[6] Y. Gallot, P. Moree, Ternary cyclotomic polynomials having a large coefficient, J. Reine Angew. Math. **632** (2009), 105-125.

[7] N. Kaplan, Flat cyclotomic polynomials of order three, J. Number Theory **127** (2007), 118-126.

[8] H.W. Lenstra, Vanishing sums of roots of unity, in: Proceedings, Bicentennial Congress Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978), Part II, 1979, pp. 249-268.

[9] T. Liu, personal communication.

[10] P. Moree, Inverse cyclotomic polynomials, J. Number Theory **129** (2009), 667-680.