

ON ZSIGMONDY PRIMES

MOSHE ROITMAN

(Communicated by Ronald M. Solomon)

ABSTRACT. We present simple proofs of Walter Feit's results on large Zsigmondy primes.

We present simple proofs of known results related to Zsigmondy primes. We recall that if a, n are integers greater than 1, then a prime p is called a *Zsigmondy prime* for $\langle a, n \rangle$ if $p \nmid a$ and the order of $a \pmod{p}$ equals n (see [2], [4, §5], and Theorem 3 below). If p is a Zsigmondy prime for $\langle a, n \rangle$, then $n \mid p - 1$; thus $p \geq n + 1$. A Zsigmondy prime p for $\langle a, n \rangle$ is called a *large Zsigmondy prime* for $\langle a, n \rangle$ if $p > n + 1$ or p^2 divides $a^n - 1$ (equivalently, a prime p is a large Zsigmondy prime for $\langle a, n \rangle$ iff p is a Zsigmondy prime for $\langle a, n \rangle$ satisfying $|a^n - 1|_p > n + 1$. See [2]). Zsigmondy primes are used in finite group theory (see, e.g., [1]). For applications of large Zsigmondy primes to finite groups see [3] and [4].

The main results that we reprove here are Theorem 3 (Zsigmondy's Theorem) and Theorem 10 (due to Walter Feit).

We now recall some basic properties of cyclotomic polynomials, which we will use below (see, e.g., [6, Preliminaries, sec. 1]). For $n \geq 1$ the cyclotomic polynomial $\Phi_n(X)$ is defined as

$$\Phi_n(X) = \prod_{i=1}^{\varphi(n)} (X - \epsilon_i),$$

where $\epsilon_1, \dots, \epsilon_{\varphi(n)}$ are the primitive roots of unity of order n and $\varphi(n)$ is Euler's totient function. If $n > 1$, then $\Phi_n(a) > 0$ for all real a since $\Phi_2(X) = X + 1$, and for $n > 2$, $\Phi_n(X)$ is a monic polynomial over the integers with no real roots. Moreover, if $n > 1$ and $a > 1$ are integers, then $\Phi_n(a) > 1$ since $\Phi_n(a) = \prod_{i=1}^{\varphi(n)} |a - \epsilon_i| > (a - 1)^{\varphi(n)} \geq 1$.

Except for such basic facts, the paper is self-contained. Some of the proofs included here are the usual ones.

Lemma 1. *Let $a > 1$ and $n = q^i r$ be integers, where q is a prime, $i \geq 1$ and r is a positive integer not divisible by q . Let $b = a^{q^{i-1}}$. Then*

$$\Phi_n(a) > (b^{q-2}(b-1))^{\varphi(r)}.$$

Received by the editors December 19, 1995.

1991 *Mathematics Subject Classification.* Primary 11A41.

I thank Yakov Berkovich for suggesting this subject and for useful discussions concerning it.

Proof. We have

$$\Phi_n(a) = \frac{\Phi_r(a^{q^i})}{\Phi_r(a^{q^{i-1}})} = \frac{\Phi_r(b^q)}{\Phi_r(b)} = \frac{\prod_{i=1}^{\varphi(r)}(b^q - \epsilon_i)}{\prod_{i=1}^{\varphi(r)}(b - \epsilon_i)} > \left(\frac{b^q - 1}{b + 1}\right)^{\varphi(r)},$$

where the ϵ_i 's are roots of unity. Since $b^q - 1 \geq b^{q-2}(b^2 - 1)$ the lemma follows. \square

Remark. In the notation of the previous lemma we have the inequality

$$\Phi_n(a) \geq \left(\frac{b^q + 1}{b + 1}\right)^{\varphi(r)}.$$

If q is a Zsigmondy prime for the pair $\langle a, n \rangle$, then q divides $a^n - 1 = \prod_{d|n} \Phi_d(a)$; thus q divides $\Phi_n(a)$. The next proposition characterizes the Zsigmondy primes among the prime factors of $\Phi_n(a)$.

Proposition 2 (cf. [5, Satz 1]). *Let $a > 1$ and $n > 1$ be integers. Let q be a prime factor of $\Phi_n(a)$. Then q is a non Zsigmondy prime for $\langle a, n \rangle$ iff q divides n . In this case q is the largest prime factor of n , and $n = q^i r$, where r is a positive integer dividing $q - 1$; moreover, q^2 does not divide $\Phi_n(a)$ unless $q = n = 2$.*

Thus, if there are no Zsigmondy primes for $\langle a, n \rangle$, then $\Phi_n(a)$ is a power of q ; if also $n > 2$ then $\Phi_n(a) = q$.

Proof. If $q | n$, then $a^{\frac{n}{q}} \equiv a^n \equiv 1 \pmod{q}$; thus q is not a Zsigmondy prime for $\langle a, n \rangle$ (actually, we have already proved this above).

Conversely, assume that q is not a Zsigmondy prime for $\langle a, n \rangle$. Then there exists a prime factor p of n such that $a^{n/p} \equiv 1 \pmod{q}$. Since $\Phi_n(X)$ divides $\frac{X^n - 1}{X^{n/p} - 1}$ we obtain, for $c = a^{n/p}$, that q divides $\frac{c^p - 1}{c - 1} = \sum_{i=0}^{p-1} c^i \equiv p \pmod{q}$. Thus $q = p$ divides n . Moreover, since $a^{n/p} \not\equiv 1 \pmod{q}$ for any prime factor $p \neq q$ of n , it follows that the order of $a \pmod{q}$ is of the form n/q^i for some $i \geq 1$, and so $r := n/q^i$ divides $q - 1$. Thus q is the largest prime factor of n .

Let $c = a^{n/q}$.

If $q > 2$ let $d = c - 1$; thus $q | d$. We have

$$\frac{a^n - 1}{a^{\frac{n}{q}} - 1} = \frac{c^q - 1}{c - 1} = \frac{(1 + d)^q - 1}{d} = q + \sum_{i=2}^{q-1} \binom{q}{i} d^{i-1} \equiv q \pmod{q^2}.$$

Thus $q^2 \nmid \Phi_n(a)$.

If $q = 2$ and $n > 2$, then n is a power of 2 and $n \geq 4$. We have $\frac{c^2 - 1}{c - 1} = c + 1$. Since a is odd and $\frac{n}{2}$ is even, we obtain $c = a^{n/2} \equiv 1 \pmod{4}$; thus $c + 1 \equiv 2 \pmod{4}$. Hence $4 \nmid \Phi_n(a)$ as claimed. \square

Theorem 3 (Zsigmondy's Theorem). *Let a and n be integers greater than 1. There exists a prime divisor q of $a^n - 1$ such that q does not divide $a^j - 1$ for all j , $0 < j < n$, except exactly in the following cases:*

- (1) $n = 2$, $a = 2^s - 1$, where $s \geq 2$.
- (2) $n = 6$, $a = 2$.

Proof. It is easy to verify that if one of the conditions (1) or (2) holds, then there is no q satisfying our requirements.

Assume that there is no prime q such that the order of a modulo q is n .

If $n = 2$, then by Proposition 2, $\Phi_n(a) = a + 1 = 2^s$ for some integer s , and case (1) holds.

Assume that $n > 2$. By Proposition 2, $\Phi_n(a) = q$, where q is the largest prime factor of n .

If $q = 2$, then $n = 2^s$ and $\Phi_n(a) = a^{2^{s-1}} + 1 > 2$, a contradiction.

Thus $q \geq 3$. Let $n = q^i r$, where r is an integer not divisible by q . Set $b = a^{q^{i-1}}$. By Lemma 1, $b^{q-2} < q$. Hence $q = 3$ and $b = 2, a = 2$ (indeed, $2^{q-2} < q$ implies $q = 3$. Thus $b < 3$, that is, $b = 2$). Since 7 is a Zsigmondy prime for $\langle 2, 3 \rangle$, we see that $n = qr > 3$. Since n divides $q(q - 1) = 6$, we conclude that $n = 6$. \square

For a proof of Zsigmondy's Theorem in a stronger form see [6, (P1.7)]. For previous proofs see the references in [6], and especially [5]. For the present proof I have used a proof of Zsigmondy's Theorem based on [1] due to Yakov Berkovich and Gregory Freiman.

We now turn to the proof of Feit's results on Zsigmondy primes.

From Proposition 2 we obtain:

Corollary 4. *Let a, n be integers greater than 1. Let q be the largest prime factor of n . Assume that there are Zsigmondy primes for $\langle a, n \rangle$, but no large Zsigmondy primes. Then $n + 1$ is the unique Zsigmondy prime for $\langle a, n \rangle$. If $n > 2$, then either $\Phi_n(a) = n + 1$ or $\Phi_n(a) = q(n + 1)$.*

Corollary 4 shows that for $a > 1$ and $n > 1$, the largest prime factor of $a^n - 1$ is $\geq n + 1$. For a short review of far reaching generalizations of this remark see [7, Chapter 2, Section II.G]. Especially see [8-11].

Lemma 5. *For $n \geq 1, n \neq 6$ we have $2^{\varphi(n)} \geq n$; thus for all $n \geq 1$ we have $2^{\varphi(n)} \geq \frac{2}{3}n$.*

Proof. Let $n > 1$. First let n be odd. Then $2^{\varphi(n)} \equiv 1 \pmod n$. Thus $2^{\varphi(n)} = kn + 1$ for some $k \geq 1$. It follows that $2^{\varphi(n)} > n$. If $k = 1$, let $s = \varphi(n)$. The s numbers 2^i for $0 \leq i \leq s - 1$ are coprime with $n = \varphi(2^s - 1)$ and are between 1 and n . Since $1 \leq 2^s - 2 \leq n$ and $(2^s - 2, n) = 1$, we have $2^s - 2 = 2^i$ for some $0 \leq i \leq s - 1$. Hence $2^{s-1} - 1 = 2^{i-1}$; so, $2^{s-1} - 1 = 1$ and $n = 3$. It follows that $2^{\varphi(n)} > 3n$ holds for odd $n > 3$.

For an even $n > 1$, let $n = 2^i m$, where m is odd. If $m = 1$, then $2^{\varphi(n)} = 2^{2^{i-1}} \geq 2^i = n$. If $i = 1$ and $m > 3$, then $2^{\varphi(n)} = 2^{\varphi(m)} > 2m = n$. If $i > 1$ and $m \geq 3$, then $2^{\varphi(n)} = 2^{2^{i-1}\varphi(m)} \geq 2^{i\varphi(m)} \geq 2^{i+\varphi(m)} > 2^i m = n$ since a product of two integers greater than 1 is greater than or equal to their sum. \square

As seen from the proof of the previous lemma, we have equality $2^{\varphi(n)} = n$ iff $n = 2, 4$.

Theorem 6 [2, Theorem A]. *If a and n are integers greater than 1, then there exists a large Zsigmondy prime for $\langle a, n \rangle$ except exactly in the following cases:*

- (1) $n = 2$ and $a = 2^s 3^t - 1$ for some natural $s \geq 0$ and $t = 0, 1$ with $s \geq 2$ if $t = 0$.
- (2) $a = 2$ and $n = 4, 6, 10, 12$ or 18.
- (3) $a = 3$ and $n = 4$ or 6.
- (4) $\langle a, n \rangle = \langle 5, 6 \rangle$.

Proof. It is easy to show that in each case there are no large Zsigmondy primes for $\langle a, n \rangle$.

For the converse, by Theorem 3 we may assume that there are Zsigmondy primes for $\langle a, n \rangle$, but no large Zsigmondy primes. First let $n = 2$. As in [2], since the greatest common divisor of $a - 1$ and $a + 1$ is at most 2 it follows that any odd prime factor of $a + 1$ is a Zsigmondy prime and so it equals $n + 1 = 3$. Hence case (1) holds.

Now assume that $n > 2$. By Corollary 4, $\Phi_n(a)$ equals either $n + 1$ or $q(n + 1)$, and $n + 1$ is prime. Thus n is even.

◦ Let n be a power of 2: $n = 2^i, i \geq 2$.

If $\Phi_n(a) = n + 1$ then

$$a^{2^{i-1}} = 2^i.$$

Since $2^i \leq a^i \leq a^{2^{i-1}} = 2^i$, we obtain $a = 2, 2^{i-1} = i$, and $i = 2$, that is $n = 4$.

If $\Phi_n(a) = 2(n + 1)$, then $a^{2^{i-1}} + 1 = 2(2^i + 1)$; thus $a^{2^{i-1}} = 2^{i+1} + 1$, and $a \geq 3$. If $i = 2$, then $a = 3$ and $n = 4$. If $i > 2$, then $a^{2^{i-1}} \geq 3^{i+1} > 2^{i+1} + 1$, a contradiction.

◦ Assume that n is not a power of 2. Let q be the largest prime factor of n and let $n = q^i r$, where r is an integer not divisible by q . Thus r is even. Set $b = a^{q^{i-1}}$.

• First assume that

$$\Phi_n(a) = q(n + 1).$$

By Lemma 1

$$(b^{q-2}(b - 1))^{\varphi(r)} < \Phi_n(a) = q(rq^i + 1) \leq q(rq(b - 1) + 1).$$

Divide by $b - 1$ to obtain

$$(1) \quad b^{(q-2)\varphi(r)} < q(rq + 1).$$

By Proposition 2, we have $q(rq + 1) \leq q((q - 1)q + 1) < q^3$, and thus

$$(2) \quad b^{(q-2)\varphi(r)} < q^3.$$

If $q = 3$, then $r = 2$ by Proposition 2, and $b < 21$ by (1); thus $i = 1, 2$. Hence $n = 6, 18$. Since $q(n + 1) = \Phi_n(a) = b^2 - b + 1$, we obtain for $n = 6$ that $b = a = 5$ and for $n = 18$ that $b = 8, a = 2$.

Now assume that $q > 3$.

If $r > 2$, then $\varphi(r) \geq 2$. By (2)

$$(3) \quad b^{2(q-2)} < q^3.$$

By induction we easily obtain that $2^{2(q-2)} > q^3$ for any integer $q \geq 6$. Thus $q = 5$. Since the inequality (3) does not hold for $b = 3$ and $q = 5$, it follows that $b = 2, i = 1, n = 5r$. Since $r \mid q - 1$, we obtain that $r = 4$. Thus $n + 1 = 21$ is not prime, a contradiction.

Let $r = 2$.

We have

$$\Phi_n(a) = \Phi_{2q^i}(a) = \frac{b^q + 1}{b + 1}.$$

Hence

$$b + 1 \equiv b^q + 1 \equiv 0 \pmod{q}.$$

Thus $b \geq q - 1$. By (1)

$$(q - 1)^{q-2} < q(2q + 1).$$

But for $q \geq 5$ we have $(q - 1)^{q-2} \geq (q - 1)^3 > q(2q + 1)$, since $q^3 - 5q^2 + 2q - 1 > 0$, a contradiction.

- Assume that $\Phi_n(a) = n + 1$.

Similarly to (1) we have

$$(4) \quad (b^{q-2})^{\varphi(r)} < rq + 1.$$

Divide by $2^{\varphi(r)}$ and use Lemma 5 to obtain

$$(5) \quad \left(\frac{b^{q-2}}{2}\right)^{\varphi(r)} < \frac{3}{2}q + 1.$$

Hence

$$(6) \quad b^{q-2} < 3q + 2.$$

For any integer $q \geq 7$ we show by induction that $2^{q-2} \geq 3q + 2$. Thus $q = 3, 5$.

Let $q = 3$.

Let $n = 2^j 3^i$. Since $r \neq 6$, by Lemma 5 we have $b^{q-2} < 2q + 2$ (cf. (6)), that is, $b < 8$. Hence $i = 1$. We have

$$\Phi_n(a) = \frac{\Phi_{2^j}(a^3)}{\Phi_{2^j}(a)} = \frac{c^3 + 1}{c + 1},$$

where $c = a^{2^{j-1}}$. Thus $c^2 - c + 1 = n + 1$, that is, $c(c - 1) = 2^j \cdot 3$. So $c = 3$ or $c - 1 = 3$. If $c = 3$ then $a = 3, n = 6$. If $c - 1 = 3$ then $4 = c = 2^j, j = 2, a = 2, n = 12$.

Let $q = 5$.

By (5) we obtain $2^{2\varphi(r)} < \frac{3}{2} \cdot 5 + 1$. Thus $4^{\varphi(r)} < 9$, which implies $\varphi(r) = 1, r = 2$. By (6), we have $b^3 < 17$, and so $b = a = 2, i = 1$, and $n = 10$. □

In the sequel we prove [2, Theorem B], but first some auxiliary results.

Lemma 7. *Let $a > 1$ and $n > 2$ be integers. Then*

$$\Phi_n(a) > a^{\varphi(n)/2}.$$

Proof. If n is a power of 2, $n = 2^m$, then

$$\Phi_n(a) = a^{2^{m-1}} + 1 > a^{2^{m-1}} = a^{\varphi(n)}.$$

Otherwise, let q be a prime odd factor of n . Set $n = q^i r$, where r is an integer not divisible by q . Set $b = a^{q^{i-1}}$. By Lemma 1, we have

$$\Phi_n(a) > (b^{q-2})^{\varphi(r)} \geq \left(b^{\frac{q-1}{2}}\right)^{\varphi(r)} = a^{\varphi(n)/2}.$$

□

Lemma 8 [2, Lemma 2.5]. *For $n \geq 1$ we have $\varphi(n) \geq \sqrt{n}/2$.*

Proof. If p is an odd prime and $m \geq 1$ then $\varphi(p^m) = (p-1)p^{m-1} \geq \sqrt{p^m}$. Also $\varphi(2^m) = 2^{m-1} \geq \sqrt{2^m}/2$. Since φ is a multiplicative function ($\varphi(mn) = \varphi(m)\varphi(n)$ for m, n coprime) the lemma follows. \square

As a result of Lemmas 7 and 8 we obtain:

Corollary 9. *For any integers $a > 1, n > 2$ we have*

$$\Phi_n(a) > a^{\frac{\sqrt{n}}{4}}.$$

Theorem 10 [2, Theorem B]. *Let N be a positive integer. Then for all but finitely many pairs of integers $\langle a, n \rangle$ with $a > 1$ and $n > 2$, there exists a Zsigmondy prime p with $|a^n - 1|_p > nN + 1$.*

Proof. Let $a > 1$ and $n > 2$ be positive integers such that there are no Zsigmondy primes p for $\langle a, n \rangle$ with $|a^n - 1|_p > nN + 1$. Since any Zsigmondy prime p satisfies $p \equiv 1 \pmod{n}$, there are at most N Zsigmondy primes satisfying $p \leq nN + 1$. Let q be the largest prime factor of n . Hence, by Proposition 2

$$\Phi_n(a) \leq q(nN + 1)^N.$$

By Corollary 9 this implies $a^{\frac{\sqrt{n}}{4}} < n(nN + 1)^N$. The theorem follows. \square

Finally, we recall that Zsigmondy's Theorem was used by Wedderburn in order to prove that any finite division ring is commutative [12]. We reproduce here one of the Wedderburn's proofs slightly revised. Let D be a finite division ring of dimension n over its prime subfield \mathbb{F}_p . First assume that there is a Zsigmondy prime q for $\langle p, n \rangle$. Let $g \in D \setminus \{0\}$ be an element of order q . Let F be the subring of D generated by g . Let $m = [F : \mathbb{F}_p]$. Since $g^{p^m - 1} = 1$ we have $q \mid p^m - 1$. Thus $m = n$ and so $D = F$ is commutative.

If there are no Zsigmondy primes for $\langle p, n \rangle$, then, by Zsigmondy's Theorem, either $n = 2$, or $n = 6$ and $p = 2$. If $n = 2$, then D is commutative since it is the subring generated by any element in $D \setminus \mathbb{F}_p$. If $n = 6$ and $p = 2$, then the order of 2 (mod 9) is 6. Since $D \setminus \{0\}$ contains a subgroup of order 9 (which is abelian), we can use the previous argument to complete the proof.

To obtain a uniform formulation of the proof for $n > 2$ note that Zsigmondy's Theorem implies that for any $n > 2$ and $a > 1$ there exists a prime p such that for $m = p$ or $m = p^2$, the order of a modulo m equals n .

Of course, there are simpler proofs of Wedderburn's Theorem. However, it is interesting that Wedderburn's Theorem is a simple consequence of Zsigmondy's Theorem.

REFERENCES

1. E. Artin, The orders of the linear groups, *Comm. Pure and Appl. Math.* 8 (1955), 355-365. Reprinted in *Collected Papers*, (edited by S. Lang and J. Tate), 387-397, Addison-Wesley, Reading, Mass., 1965. MR 17:12d
2. W. Feit, On large Zsigmondy primes, *Proc. Amer. Math. Soc.* 102 (1988), 29-36. MR 89b:11009
3. W. Feit, Extensions of cuspidal characters of $GL_m(q)$, *Publ. Math. Debrecen* 34 (1987), 273-297. MR 89d:20007
4. W. Feit, G.M. Seitz, On finite rational groups and related topics, *Illinois J. Math.* 33 (1988), 103-131. MR 90a:20016
5. H. Lüneburg, Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von $A^n - 1$, in *Geometries and Groups*, (edited by M. Aigner and D. Jungnickel), Lect. Notes in Math. 983, 219-222, Springer Verlag, New York, 1981. MR 84d:10006

6. P. Ribenboim, *Catalan's conjecture*, Academic Press, New York, 1994.
7. P. Ribenboim, *The Book of Prime Number Records*, Second Edition, Springer Verlag, New York, 1989. MR **90g**:11127
8. C. L. Stewart, The greatest prime factor of $a^n - b^n$, *Acta Arith.* , 26 (1975), 427-433. MR **53**:2844
9. C.L. Stewart, Primitive divisors of Lucas and Lehmer numbers, in *Transcendence Theory: Advances and Applications*, pp. 79-92, Academic Press, New York, 1977. MR **57**:16187
10. T.N. Shorey and C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. London Math. Soc.* 35 (1977), 425-447.
11. T.N. Shorey and C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, II, *J. London Math. Soc.* 23 (1981), 17-23. MR **82m**:10025
12. A.H. Wedderburn, A theorem on finite algebras, *Trans. Amer. Math. Soc.* 6 (1905), 349-352.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAIFA, MOUNT CARMEL, HAIFA 31905, ISRAEL
E-mail address: mroitman@mathcs2.haifa.ac.il