PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 102, Number 1, January 1988

ON LARGE ZSIGMONDY PRIMES

WALTER FEIT

(Communicated by Donald Passman)

ABSTRACT. If a and m are integers greater than 1, then a large Zsigmondy prime is a prime l such that $l \mid a^m - 1$, $l \nmid a^i - 1$ for $1 \leqslant i \leqslant m - 1$ and either $l^2 \mid a^m - 1$ or $l > m + 1$. The main result of this paper lists all the pairs (a, m) for which no large Zsigmondy prime exists.

1. Introduction. Let a and m be integers greater than 1. A *Zsigmondy prime for* (a, m) is a prime l such that $l \mid a^m - 1$ but $l \nmid a^i - 1$ for $1 \leqslant i \leqslant m - 1$. A well-known theorem of Zsigmondy asserts that Zsigmondy primes exist except if $(a, m) = (2, 6)$ or $m = 2$ and $a = 2^k - 1$ (see [**5**]). This paper contains a refinement of this result.

Observe that if l is a Zsigmondy prime for (a, m), then a has order m modulo l and so $l \equiv 1 \pmod{m}$. Thus $l \geqslant m + 1$. A prime l is a *large Zsigmondy prime for* (a, m) if l is a Zsigmondy prime for (a, m) and either $l > m + 1$ or $l^2 \mid a^m - 1$.

THEOREM A. *If a and m are integers greater than* 1, *then there exists a large Zsigmondy prime for* (a, m) *except in the following cases.*

(i) $m = 2$ *and* $a = 2^s 3^t - 1$ *for some natural number* s, *and* $t = 0$ *or* 1.

(ii) $a = 2$ *and* $m = 4, 6, 10, 12$ *or* 18.

(iii) $a = 3$ *and* $m = 4$ *or* 6.

(iv) $(a, m) = (5, 6)$.

If n is a natural number and l is a prime, let $|n|_l$ denote the l-part of n. In other words $|n|_l = l^k$ where $l^k \mid n$ but $l^{k+1} \nmid n$. Thus a Zsigmondy prime l for (a, m) is large if and only if $|a^m - 1|_l > m + 1$.

An argument similar to that used to prove Theorem A also yields the following result.

THEOREM B. *Let N be a positive integer. Then for all but a finite number of pairs of integers* (a, m) *with* $a > 1$ *and* $m > 2$, *there exists a Zsigmondy prime l with* $|a^m - 1|_l > mN + 1$.

The proof of Theorem B actually yields a bound which can be used to find the exceptions in Theorem B. This method is used to prove Theorem A.

Received by the editors August 27, 1986 and, in revised form, September 22, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A05; Secondary 11A07.
The work on this paper was partly supported by NSF grant #DMS-8512904.

Zsigmondy's Theorem was independently, but later, discovered by Birkhoff and Vandiver [**2**]. Of course it follows from Theorem A by checking that in cases (ii), (iii), and (iv) a Zsigmondy prime exists except when $(a, m) = (2, 6)$.

Artin gave an elegant proof of the original result in [**1**]. The proof of Theorem A given here uses his approach and is based on his work.

The special case of Theorem A for $a \geqslant 3$ was proved in [**3**]. However there is no appreciable simplification in handling the general case rather than the case $a = 2$, so the proof given here is independent of earlier work and is self-contained.

The motivation for Theorem A comes from the theory of finite groups and is needed for some forthcoming work [**4**]. The relevance of Theorem A and Zsigmondy's Theorem for the theory of finite groups can also be seen for instance in [**1, 3**].

I am indebted to the referee for suggesting Lemma 2.1. This is stronger than my earlier result and shortens some of the arguments below.

2. Some preliminary results. For any natural number m let $\Phi_m(x)$ denote the mth cyclotomic polynomial and let $P(m)$ denote the largest prime which divides m. Let $\varphi(m) =$ degree of $\Phi_m(x)$ denote the Euler function.

LEMMA 2.1. *Let a, m be integers with $a > 1$ and $m > 2$. Let S be the set of all Zsigmondy primes for (a, m). Let $Z = \prod_{l \in S} |\Phi_m(a)|_l$. Then*

$$\Phi_m(a) \mid ZP(m). \tag{2.1}$$

PROOF. This is a direct consequence of [**1**, Lemma 1]. □

LEMMA 2.2. *Let a, m be integers with $a > 1$ and $m > 2$. Let N be a positive integer. Suppose that if l is a Zsigmondy prime for (a, m) then $|a^m - 1|_l \leqslant Nm + 1$. Then*

$$|\Phi_m(a)| \leqslant (Nm + 1)^N P(m). \tag{2.2}$$

PROOF. There are at most N Zsigmondy primes $l \leqslant Nm + 1$. Thus if Z is defined as in Lemma 2.1 then $Z \leqslant (Nm + 1)^N$. The result follows from Lemma 2.1. □

LEMMA 2.3. *Let a, m be integers with $a > 1$ and $m > 2$. Suppose there exists no large Zsigmondy prime for (a, m). Then*

$$|\Phi_m(a)| \leqslant (m + 1)P(m). \tag{2.3}$$

PROOF. Let $N = 1$ in Lemma 2.2. □

The proofs of Theorems A and B are based on the fact that (2.2) and (2.3) only hold for a finite number of cases.

For any positive real number r define

$$L_m(r) = \min_{|u| = r} |\Phi_m(u)|. \tag{2.4}$$

Here u ranges over all complex numbers with $|u| = r$. Since this set is compact, the minimum exists.

LEMMA 2.4. *Let $m = nt$, where n is relatively prime to t. Let r be a positive real number. Then $L_m(r) \geqslant (L_n(r))^{\varphi(t)}$.*

PROOF. Let u be a complex number with $|u| = r$. Then

$$|\Phi_m(u)| = \left| \prod_{\varepsilon} \Phi_n(u\varepsilon) \right|,$$

where ε ranges over all the primitive tth roots of 1. As $|u\varepsilon| = |u|$, this implies that $|\Phi_m(u)| \geqslant |L_n(r)|^{\varphi(t)}$. The result follows as u was arbitrary with $|u| = r$. □

The next two elementary results will be needed later.

LEMMA 2.5. *Let m be a natural number. Then $\varphi(m) \geqslant \frac{1}{2}\sqrt{m}$.*

PROOF. If p is a prime then $\varphi(p^b) = (p-1)p^{b-1}$ for any natural number b. Thus $\varphi(p^b) \geqslant p^{b/2}$ if $p \geqslant 2$ and $\varphi(2^b) \geqslant 2^{b/2-1}$. This proves the result as $\varphi(nt) = \varphi(n)\varphi(t)$ for n, t relatively prime. □

LEMMA 2.6. *Let $0 < n < m$. Then $f(x) = (x^m - 1)/(x^n + 1)$ is monotone increasing for $x > 0$.*

PROOF. If $x > 0$ then

$$f'(x) = \frac{(m-n)x^{m+n-1} + mx^{m-1} + nx^{n-1}}{(x^n+1)^2} > 0. \qquad \square$$

3. The proof of Theorem B.

LEMMA 3.1. *Let $r \geqslant 2$ be a real number. Let m, N be natural numbers. suppose that $L_m(r) \leqslant (Nm+1)^N P(m)$. Then $(r-1) \leqslant (2N+1)^{2(N+1)}$.*

PROOF. By Lemma 2.4

$$(Nm+1)^N P(m) \geqslant L_m(r) \geqslant L_1(r)^{\varphi(m)} = (r-1)^{\varphi(m)}.$$

If $(r-1) > (2N+1)^{2(N+1)}$ this implies that

$$(Nm+1)^{N+1} > (Nm+1)^N m \geqslant (Nm+1)^N P(m) > (2N+1)^{2(N+1)\varphi(m)}.$$

Hence by Lemma 2.5

$$(Nm+1) > (2N+1)^{2\varphi(m)} \geqslant (2N+1)^{\sqrt{m}}$$

which is impossible for $m \geqslant 1$. □

LEMMA 3.2. *Let $r \geqslant 2$ be a real number. Let m, N be natural numbers such that $m > 1$ and $m \neq 2n$ with n odd. Suppose that*

$$L_m(r) \leqslant 2^N (Nm+1)^N P(m).$$

Then there exists $C = C(N)$, depending only on N, with $m < C$.

PROOF. Suppose first that $m = p^b$ is a prime power. By assumption, $p^b > 2$. There exists a complex number u with $|u| = r$ such that

$$4^N(Np^b+1)^N p \geqslant \left|\frac{u^{p^b}-1}{u^{p^{b-1}}-1}\right| \geqslant \frac{r^{p^b}-1}{r^{p^{b-1}}+1} \geqslant \frac{1}{3}\frac{r^{p^b}-1}{r^{p^{b-1}}-1}$$
$$\geqslant \frac{1}{3}r^{p^b-p^{b-1}} \geqslant \frac{1}{3}r^{p^b/2} \geqslant \frac{1}{3}2^{p^b/2}.$$

This implies the existence of $C_0 = C_0(N) > 10^{20}$, depending only on N, such that $p^b < C_0$.

We will now prove the result with $C = C_0^k$, where $k = \pi(C_0)$ is the number of primes $p < C_0$.

Suppose $m > C$. Then $m = p^b t$ for some prime p with $p^b \geqslant C_0$ and $p \nmid t$. Therefore

$$L_{p^b}(r) > 2^N(Np^b + 1)^N p.$$

Hence Lemma 2.4 implies that

$$2^N(Np^b t + 1)^N pP(t) \geqslant L_m(r) \geqslant \{L_{p^b}(r)\}^{\varphi(t)} > \{2^N p(Np^b + 1)^N\}^{\varphi(t)}.$$

By assumption, $t > 2$ and so $\varphi(t) \geqslant 2$. Thus

$$2^N pt(2Np^b t)^N > 2^{2N} p^2 (Np^b)^{N\varphi(t)}.$$

Hence

$$t(2Np^b t)^N > 2^N p(Np^b)^{N\varphi(t)} > \{2(Np^b)^{\varphi(t)}\}^N.$$

After taking Nth roots, Lemma 2.5 implies that

$$Np^b t^2 > (Np^b)^{\varphi(t)} \geqslant (Np^b)^{\sqrt{t}/2}. \tag{3.1}$$

Let $y = Np^b$. By (3.1) $yt^2 > y^{\sqrt{t}/2}$. As $y \geqslant p^b > C_0 > 10^{20}$ this implies that if $t \geqslant 5$ then $25y > y^{\sqrt{5}/2}$. Hence

$$25 > y^{(\sqrt{5}-1)/2} > y^{1/10} > 100$$

which is not the case. Since $t \neq 2t_0$ with t_0 odd, (3.1) implies that one of the following holds:

$$t = 4 \quad \text{and} \quad 16y > y^2, \qquad t = 3 \quad \text{and} \quad 9y > y^2.$$

None of these can hold as $y > 10^{20}$. □

LEMMA 3.3. *Let $a \geqslant 2$ be a natural number. Let m, N be natural numbers with $m > 2$. Suppose that*

$$|\Phi_m(a)| \leqslant (Nm + 1)^N P(m).$$

Then there exists $C = C(N)$, depending only on N, with $m < C$.

PROOF. If $m \neq 2n$ with n odd this follows directly from Lemma 3.2. Suppose that $m = 2n$ with n odd. Then $\Phi_m(u) = \Phi_n(-u)$ for any complex number u and $P(m) = P(n)$. Thus $L_m(a) = L_n(a)$. Hence Lemma 3.2 implies that if no such $C = C(N)$ exists then

$$\begin{aligned} |\Phi_m(a)| &\geqslant L_n(a) > 2^N(Nn + 1)^N P(n) \\ &> (2Nn + 1)^N P(n) = (Nm + 1)^N P(m). \qquad \square \end{aligned}$$

PROOF OF THEOREM B. This is an immediate consequence of Lemmas 2.2, 3.1, and 3.3. □

4. The proof of Theorem A. The proof of Theorem A is analogous to that of Theorem B but the relevant inequalities need to be considered more precisely.

LEMMA 4.1. *Suppose that $m = nt$ with $n > 1$ and n relatively prime to t. Assume that $m \not\equiv 2 \pmod 4$. Let r be a real number such that $L_n(r) > 2(n+1)P(n)$. Then $L_m(r) > 2(m+1)P(m)$.*

PROOF. By induction on the number of primes dividing t it may be assumed that $t = p^b$ for some prime p. By assumption $n, t \neq 2 \pmod 4$ and so $t > 2$ and $n > 2$.

Suppose the result is false. Then by Lemma 2.4

$$2(np^b + 1)pP(n) \geqslant L_m(r) \geqslant L_n(r)^{p^b - p^{b-1}} > \{2(n+1)P(n)\}^{p^b - p^{b-1}}.$$

Thus

$$\begin{aligned} 4np^{2b} > 2(np^b + 1)p &> \{2(n+1)\}^{p^b - p^{b-1}} P(n)^{p^b - p^{b-1} - 1} \\ &\geqslant \{2(n+1)\}^{p^b - p^{b-1}} 2^{p^b - p^{b-1} - 1}. \end{aligned} \tag{4.1}$$

Let $y = \frac{1}{2}p^b$. As $p^b - p^{b-1} \geqslant \frac{1}{2}p^b$, (4.1) implies that $16ny^2 > 2^{2y-1}(n+1)^y$. Hence

$$16y^2 > 2^{2y-1}(n+1)^{y-1} \geqslant 2^{2y-1}4^{y-1} = 2^{4y-3}.$$

Thus $p^b = y^2 < 7$. Hence $p^b = 3, 4$ or 5 contrary to (4.1). □

LEMMA 4.2. *Let $r \geqslant 2$ be a real number. Let m be an integer such that $m \neq 2n$ for n odd and $m > 1$. Then*

$$L_m(r) > 2(m+1)P(m) \tag{4.2}$$

except possibly in the following cases.

(i) $m = 3$ *and* $r < 6$.
(ii) $m = 4$ *and* $r < 5$.
(iii) $m = 12$ *and* $r < 4$.
(iv) $r < 3$ *and* $m = 5, 7, 8, 9, 15$ *or* 20.

PROOF. Assume that m does not satisfy the conclusions of the lemma. In particular (4.2) does not hold.

Suppose first that $m = p^b > 2$ for some prime p. Then for suitable u with $|u| = r$, Lemma 2.6 implies that

$$2(p^b + 1)p \geqslant \left| \frac{u^{p^b} - 1}{u^{p^{b-1}} - 1} \right| \geqslant \frac{r^{p^b} - 1}{r^{p^{b-1}} + 1} \geqslant \frac{2^{p^b} - 1}{2^{p^{b-1}} + 1}. \tag{4.3}$$

Suppose that $m = p$ is a prime. Then (4.3) implies that $6p(p+1) \geqslant 2^p - 1$. Hence $p < 11$. Thus $p = 3, 5$ or 7 and (4.3) implies that

$$2p(p+1) \geqslant \frac{r^p - 1}{r + 1}.$$

If $p = 7$ this yields that $112 \geqslant (r^7 - 1)/(r+1)$ and so $r < 3$. If $p = 5$ then $60 \geqslant (r^5 - 1)/(r+1)$ and so $r < 3$. If $p = 3$ then $24 \geqslant (r^3 - 1)/(r+1)$ and so $r < 6$.

Suppose that $m = p^b$ with $b > 1$. Then $r^{p^{b-1}} \geqslant 4$ and so $r^{p^{b-1}} - 1 \geqslant \frac{1}{2}(r^{p^{b-1}} + 1)$. Hence (4.3) implies that

$$2(p^b + 1)p \geqslant \frac{1}{2}\frac{r^{p^b} - 1}{r^{p^{b-1}} - 1} \geqslant \frac{1}{2}r^{p^b - p^{b-1}}. \tag{4.4}$$

Let $y = \frac{1}{2}p^b$. Then $y \leqslant p^b - p^{b-1}$. Thus (4.4) yields that

$$2(2y+1)y \geqslant 2^{y-1}.$$

Hence $y \leqslant 9$ and so $p^b \leqslant 18$. Thus $p^b = 4, 8, 9$ or 16.

If $p^b = 16$ then (4.3) implies that $68 \geqslant (2^{16}-1)/(2^8+1) = 2^8 - 1$ which is not the case.

If $p^b = 9$ then (4.4) implies that $120 \geqslant r^6$ and so $r < 3$.

If $p^b = 8$ then (4.3) implies that $36 \geqslant (r^8-1)/(r^4+1) = r^4 - 1$ and so $r < 3$.

If $p^b = 4$ then (4.3) implies that $20 \geqslant (r^4-1)/(r^2+1) = r^2 - 1$ and so $r < 5$.

In summary, we have shown that if $m = p^b$, then m satisfies the conclusion of the lemma. In particular (4.2) holds unless $m = 4, 8, 3, 9, 5$ or 7. Hence Lemma 4.1 implies that

$$m \mid 2^3 \cdot 3^2 \cdot 5 \cdot 7.$$

Suppose that $m = 7t$. Then $t \mid 2^3 \cdot 3^2 \cdot 5$. As (4.2) does not hold, Lemma 2.4 implies that for suitable u with $|u| = r$.

$$14(7t+1) \geqslant \left|\frac{u^7-1}{u-1}\right|^{\varphi(t)} \geqslant \left(\frac{r^7-1}{r+1}\right)^{\varphi(t)}. \tag{4.5}$$

This yields the following inequalities.

If $t = 5$ then $14 \cdot 36 \geqslant ((r^7-1)/(r+1))^4$.

If $t = 9$ then $14 \cdot 64 \geqslant ((r^7-1)/(r+1))^6$.

If $t = 8$ then $14 \cdot 57 \geqslant ((r^7-1)/(r+1))^4$.

None of these can hold for $r \geqslant 2$. Hence $5 \nmid t$, $9 \nmid t$, and $8 \nmid t$ by Lemma 4.1. Thus $t \mid 12$. As $t \not\equiv 2 \pmod 4$ either $t = 3$ or $4 \mid t$.

Suppose $t = 4$; then (4.5) becomes $14 \cdot 29 \geqslant ((r^7-1)/(r+1))^2$, which is impossible for $r \geqslant 2$. Thus $4 \nmid t$ by Lemma 4.1 and so $t = 3$. Now (4.5) becomes $14 \cdot 22 \geqslant ((r^7-1)/(r+1))^2$, which is impossible for $r > 2$.

Therefore it may be assumed that

$$m \mid 2^3 \cdot 3^2 \cdot 5.$$

Suppose that $m = 5t$. Then $t \mid 2^3 \cdot 3^2$. As (4.2) does not hold, Lemma 4.1 implies that for suitable u with $|u| = r$.

$$10(5t+1) \geqslant \left|\frac{u^5-1}{u+1}\right|^{\varphi(t)} \geqslant \left(\frac{r^5-1}{r+1}\right)^{\varphi(t)}. \tag{4.6}$$

This yields the following inequalities.

If $t = 9$ then $460 \geqslant ((r^5-1)/(r+1))^6$.

If $t = 8$ then $410 \geqslant ((r^5-1)/(r+1))^4$.

Neither of these can hold for $r \geqslant 2$. Thus Lemma 4.1 implies that $9 \nmid t$ and $8 \nmid t$. Hence $t \mid 12$ and so $t = 3, 4$, or 12.

If $t = 12$ then (4.6) becomes $610 \geqslant ((r^5-1)/(r+1))^4$, which is impossible for $r \geqslant 2$.

If $t = 4$ then (4.6) becomes $210 \geqslant ((r^5-1)/(r+1))^2$. Hence $r < 3$.

If $t = 3$ then (4.6) becomes $160 \geqslant ((r^5-1)/(r+1))^2$. Hence $r < 3$.

Therefore it may be assumed that

$$m \mid 2^3 \cdot 3^2.$$

Suppose that $m = 9t$ with $t = 4$ or 8. As (4.2) does not hold, Lemma 4.1 implies that for suitable u with $|u| = r$

$$6(9t+1) \geqslant \left|\frac{u^9-1}{u^3-1}\right|^{\varphi(t)} \geqslant \left(\frac{r^9-1}{r^3+1}\right)^{\varphi(t)}. \tag{4.7}$$

This yields the following inequalities.

If $t = 8$ then $6 \cdot 73 \geqslant ((2^9-1)/9)^4$.

If $t = 4$ then $6 \cdot 37 \geqslant ((2^9-1)/9)^2$.

Neither of these holds and so $9 \nmid m$. Thus $m \mid 24$. Hence $m = 12$ or 24.

If $m = 24$ and (4.2) does not hold, Lemma 4.1 implies that for suitable u with $|u| = r$,

$$150 \geqslant \left|\frac{u^8-1}{u^4-1}\right|^2 = |u^4+1|^2 \geqslant (r^4-1)^2.$$

This is impossible for $r \geqslant 2$.

If $m = 12$ and (4.2) does not hold, Lemma 4.1 implies that for suitable u with $|u| = r$,

$$78 \geqslant \left|\frac{u^4-1}{u^2-1}\right|^2 = |u^2+1|^2 \geqslant (r^2-1)^2.$$

Thus $r < 4$.

LEMMA 4.3. *Suppose that a, m are integers with $a \geqslant 2$ and $m \geqslant 3$. Then*

$$|\Phi_m(a)| > (m+1)P(m) \tag{4.8}$$

except possibly in the following cases.

(i) $m = 3$ *or* 6 *and* $a < 6$.

(ii) $m = 4$ *and* $a < 5$.

(iii) $m = 12$ *and* $a < 4$.

(iv) $a < 3$ *and* $m = 5, 7, 8, 9, 10, 14, 15, 18, 20$ *or* 30.

PROOF. If $m \neq 2n$ with n odd, then the result follows directly from Lemma 4.2. Suppose that $m = 2n$ with n odd. Then $\Phi_m(u) = \Phi_n(-u)$ for any complex number u and $P(m) = P(n)$. Thus $L_m(a) = L_n(a)$. Hence if (4.2) holds for n then

$$|\Phi_m(a)| \geqslant L_n(a) > 2(n+1)P(n) = (2n+2)P(m) > (m+1)P(m).$$

Suppose that (4.2) does not hold for n. By Lemma 4.2 one of the following cases must occur:

$$n = 3, \quad m = 6, \quad \text{and} \quad a < 6.$$
$$a < 3 \quad \text{and} \quad n = 5, 7, 9 \text{ or } 15.$$

Thus $m = 10, 14, 18$ or 30. □

PROOF OF THEOREM A. Suppose that $m = 2$. Since 2 is the greatest common divisor of $a-1$ and $a+1$ it follows that any odd prime dividing $a+1$ is a Zsigmondy prime. This implies the result for $m = 2$. Suppose now that $m \geqslant 3$.

Assume that there exists no large Zsigmondy prime for (a, m). By Lemmas 2.3 and 4.3 (a, m) is one of the cases listed in Lemma 4.3. We will exhibit a large Zsigmondy prime l in each case that is not listed in the statement of Theorem A. This will conclude the proof.

$m = 3$,

a	2	3	4	5
l	7	13	7	31

$m = 6$,

a	4
l	13

$m = 4$,

a	4
l	17

$m = 12$,

a	3
l	73

$a = 2$,

m	5	7	8	9	14	15	20	30
l	31	127	17	73	43	151	41	331

□

References

1. E. Artin, *The orders of the linear groups*, Comm. Pure Appl. Math. **8** (1955), 355–366.

2. G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math. (2) **5** (1904), 173–180.

3. W. Feit, *Extensions of cuspidal characters of* $\mathrm{GL}_m(q)$ (to appear).

4. W. Feit and G. Seitz (to appear).

5. K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsch. Math. Phys. **3** (1892), 265–284.

Department of Mathematics, Yale University, New Haven, Connecticut 06520