#A62 INTEGERS 24 (2024)

LARGE ZSIGMONDY PRIMES

Ömer Avcı
Department of Mathematics, Boğaziçi University, Istanbul, Turkey
omeravci372742@gmail.com

Received: 7/11/23, Revised: 3/7/24, Accepted: 6/13/24, Published: 7/8/24

Abstract

If $a > b$ and $n > 1$ are positive integers, and a and b are relatively prime integers, then a *large Zsigmondy prime* for (a, b, n) is a prime p such that $p \mid a^n - b^n$ but $p \nmid a^m - b^m$ for $1 \leq m < n$, and either $p^2 \mid a^n - b^n$ or $p > n + 1$. We classify all triples of integers (a, b, n) for which no large Zsigmondy prime exists.

1. Introduction

Let $a > b$ be relatively prime positive integers and n be a positive integer. A *Zsigmondy prime* for (a, b, n) is defined as a prime p such that $p \mid a^n - b^n$ but $p \nmid a^m - b^m$ for $1 \leq m < n$. Zsigmondy's theorem asserts that Zsigmondy primes exist for all triples (a, b, n) except when $(a, b, n) = (2, 1, 6)$ or $n = 2$ and $a + b = 2^k$ for some positive integer k (see [7]).

In [2], Feit deals with the special case of Zsigmondy's theorem when $b = 1$ and defines a large Zsigmondy prime for the pair (a, n) as a prime p such that $p \mid a^n - 1$ but $p \nmid a^m - 1$ for $1 \leq m < n$ and either $p^2 \mid a^n - 1$ or $p > n + 1$. In our paper, we present a generalized version of Feit's result.

Theorem 1. *If $a > b$ are relatively prime positive integers and n is an integer greater than 1, then there exists a large Zsigmondy prime for (a, b, n) except in the following cases:*

(i) $n = 2$ *and* $a + b = 2^s$ *or* $a + b = 3 \cdot 2^s$ *where s is a non-negative integer.*

(ii) $n = 4$ *and* (a, b) *is* $(2, 1)$ *or* $(3, 1)$.

(iii) $n = 6$ *and* (a, b) *is one of* $(2, 1), (3, 1), (3, 2), (5, 1), (5, 4)$.

(iv) $n = 10$ *and* (a, b) *is* $(2, 1)$ *or* $(3, 2)$.

(v) $n = 12$ *and* $(a, b) = (2, 1)$.

DOI: 10.5281/zenodo.12685673

(vi) $n = 18$ *and* $(a, b) = (2, 1)$.

Artin's results about orders of linear groups in [1] inspired Feit's work on the existence of large Zsigmondy primes. The motivation for Feit's work comes from the theory of finite groups [3]. Feit proved the existence of large Zsigmondy primes in all cases except for finitely many, as stated in [4], for the special case $a \geq 3$. Later on, he came up with a simpler proof of his result, which also includes the case where $a = 2$, as presented in [2]. Roitman also provided a nice proof of Feit's result in [5].

For relatively prime positive integers $a > b$, we can generalize the definition of a large Zsigmondy prime as a prime p such that $p \mid a^n - b^n$, but $p \nmid a^m - b^m$ for $1 \leq m < n$, and either $p^2 \mid a^n - b^n$ or $p > n + 1$. We show that there exists a large Zsigmondy prime for (a, b, n) except in the cases presented in Theorem 1. Our proof is inspired by the elegant proof of Zsigmondy's theorem given by Yan Sheng Ang in [6].

2. Preliminaries

Lemma 1 ([2])**.** *For any positive integer n, where $\phi(n)$ denotes Euler's totient function, it holds that*

$$\phi(n) \geq \frac{1}{2}\sqrt{n}.$$

Lemma 2. *For a prime p and a positive integer n, let $v_p(n)$ denote the exponent of p in the prime factorization of n. Let x and y be integers such that $x \equiv y \not\equiv 0 \pmod{p}$.*

(1) If $p \geq 3$, then

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

(2) If $p = 2$, then

$$v_2(x^n - y^n) = \begin{cases} v_2(x^2 - y^2) + v_2(n) - 1 & \text{if } n \text{ is even,} \\ v_2(x - y) & \text{if } n \text{ is odd.} \end{cases}$$

Definition 1. For any positive integer n, the n-th *cyclotomic polynomial* $\Phi_n(x)$ is given by:

$$\Phi_n(x) = \prod_{\substack{\gcd(k,n)=1 \\ 1 \leq k \leq n}} (x - e^{2i\pi \frac{k}{n}}).$$

It is known that $\Phi_n(x)$ is a monic polynomial with integer coefficients.

Remark 1. There is a generalization of cyclotomic polynomials into two variables:

$$\Phi_n(a,b) = b^{\phi(n)}\Phi_n\left(\frac{a}{b}\right).$$

We can also express $\Phi_n(a,b)$ as

$$\Phi_n(a,b) = \prod_{\substack{\gcd(k,n)=1\\ 1\le k\le n}} (\, a - b\, e^{2i\pi \frac{k}{n}}\,).$$

It is clear that $\Phi_n(x,y)$ is a two variable polynomial with integer coefficients.

Lemma 3 ([6])**.** *Let $a > b$ and n be positive integers. Then*

(i) $a^n - b^n = \prod_{d|n} \Phi_d(a,b)$;

(ii) $(a-b)^{\phi(n)} \le \Phi_n(a,b) \le (a+b)^{\phi(n)}$;

(iii) *if p is a prime then*

$$\Phi_{pn}(a,b) = \begin{cases} \Phi_n(a^p,b^p) & \text{if } p \mid n, \\ \frac{\Phi_n(a^p,b^p)}{\Phi_n(a,b)} & \text{if } p \nmid n; \end{cases}$$

(iv) *if p is an odd prime not dividing a and b, and if k is the smallest positive integer satisfying $p \mid a^k - b^k$ then*

$$v_p(\Phi_n(a,b)) = \begin{cases} v_p(a^k-b^k) & \text{if } n = k, \\ 1 & \text{if } n = p^\beta k,\ \beta \ge 1, \\ 0 & \text{otherwise;} \end{cases}$$

(v) *if a and b are odd, then*

$$v_2\left(\Phi_n(a,b)\right) = \begin{cases} v_2(a-b) & \text{if } n = 1, \\ v_2(a+b) & \text{if } n = 2, \\ 1 & \text{if } n = 2^\beta,\ \beta \ge 2, \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 1. *Let p be a prime, a and b be distinct positive integers, and $n = p^\beta k$ for some positive integers β, k with $p \nmid k$. Then*

$$\Phi_n(a,b) = \Phi_{pk}(a^{p^{\beta-1}}, b^{p^{\beta-1}}) = \frac{\Phi_k(a^{p^\beta}, b^{p^\beta})}{\Phi_k(a^{p^{\beta-1}}, b^{p^{\beta-1}})}.$$

3. Results on Zsigmondy Primes

In this section, we prove Lemmas 8-11, then use these results to prove our main theorem (Theorem 1).

Lemma 4. *Let $a > b$ be two relatively prime positive integers, n be a positive integer, p be a prime divisor of $\Phi_n(a, b)$, and k be the smallest positive integer satisfying $p \mid a^k - b^k$. Let $\operatorname{gpf}(n)$ denote the largest prime divisor of n, then one of the following holds:*

(i) $p = 2$ *and* $n = 2^\beta$ *for some* $\beta \geq 1$.

(ii) $p \geq 3$ *and* $n = k$ *thus* p *is a Zsigmondy prime for* (a, b, n).

(iii) $p = \operatorname{gpf}(n) > 2$ *and* $n = p^\beta k$ *for some* $\beta \geq 1$ *and* $v_p(\Phi_n(a, b)) = 1$.

Proof. If $p = 2$, by Lemma 3, it follows that $n = 2^\beta$ for some $\beta \geq 1$. If $p > 2$, according to Lemma 3, there are two possibilities. Either $n = k$ or $n = p^\beta k$ holds. When $n = k$, it implies that $p \nmid a^m - b^m$ for all $1 \leq m < n$, which means that p is a Zsigmondy prime for (a, b, n). Since k is defined as the smallest positive integer such that $p \mid a^k - b^k$, it is evident that $k \mid p-1$ holds. Moreover, it is clear that any prime divisor of k must be smaller than p. Consequently, when $n = p^\beta k$, we can conclude that $p = \operatorname{gpf}(n)$ since no prime divisor of n can be greater than p. Furthermore, according to Lemma 3, we have $v_p(\Phi_n(a, b)) = 1$ in the case $n = p^\beta k$. □

Lemma 5. *Let a and b be distinct, relatively prime positive integers, and let $n \geq 2$ be an integer. If p is a Zsigmondy prime for (a, b, n), then $p \mid \Phi_n(a, b)$.*

Proof. From Corollary 3 we have

$$a^n - b^n = \prod_{d \mid n} \Phi_d(a, b).$$

Therefore, such a p divides $\Phi_d(a, b)$ for some $d \mid n$. If $d < n$, then $p \mid \Phi_d(a, b)$, which implies $p \mid a^d - b^d$. This contradicts p being a Zsigmondy prime for (a, b, n). We conclude that $d = n$, and hence $p \mid \Phi_n(a, b)$.

□

Lemma 6. *Let $a > b$ be relatively prime positive integers, and $n \geq 2$ be an integer. If q is a Zsigmondy prime for (a, b, n) but not a large Zsigmondy prime for (a, b, n), then $n = q - 1$.*

Proof. Since q is a Zsigmondy prime for (a, b, n), we have $n \mid q - 1$. If $q > n + 1$, then it is a large Zsigmondy prime. Consequently, $n = q - 1$. □

Lemma 7. *Let a and b be distinct, relatively prime positive integers, and let $n \geq 3$ be an integer. Then there is a large Zsigmondy prime for (a, b, n) if $(n+1)\operatorname{gpf}(n) < \Phi_n(a, b)$.*

Proof. Let us analyze the proof in two cases.

`Case 1:` If $\Phi_n(a, b)$ is even, then $n = 2^\beta$ for some $\beta \geq 2$, and $4 \nmid \Phi_n(a, b)$ from Lemma 3. Since $\Phi_n(a, b) > 2(n + 1) > 2$, it has at least one odd prime divisor. Let p be the greatest prime divisor of $\Phi_n(a, b)$. Since $p > 2$ and $p \nmid n$, we obtain $n \mid p-1$ from Lemma 3. If $p > n+1$, then p is a large Zsigmondy prime for (a, b, n). If $p = n + 1$, then the only odd prime divisor of $\Phi_n(a, b)$ is p. Since $4 \nmid \Phi_n(a, b)$, and $\Phi_n(a, b) > 2(n + 1)$ we conclude that $p^2 \mid \Phi_n(a, b)$, and therefore p is a large Zsigmondy prime for (a, b, n).

`Case 2:` If $\Phi_n(a, b)$ is odd, according to Lemma 3, for any prime $p \mid \Phi_n(a, b)$, there are two cases: either p is a Zsigmondy prime, so $n \mid p - 1$, or $p = \operatorname{gpf}(n)$ and $p^2 \nmid \Phi_n(a, b)$. If there exist two different Zsigmondy primes for (a, b, n), then the larger one is a large Zsigmondy prime since it is greater than $n + 1$. This implies that if there is no large Zsigmondy prime for (a, b, n), then $\Phi_n(a, b)$ can have at most two different prime divisors, one being $n+1$ and the other being $\operatorname{gpf}(n)$. Also, each of them can divide $\Phi_n(a, b)$ at most once. But this contradicts the fact that $(n + 1)\operatorname{gpf}(n) < \Phi_n(a, b)$. $\square$

Lemma 8. *Let $n > 1$ be a positive integer. If n is not equal to any of the numbers $\{2, 4, 6, 10, 12, 18\}$, then for any relatively prime positive integers $a > b$, there exists a large Zsigmondy prime for (a, b, n).*

Proof. Consider positive integers $a > b$ and $n > 1$ with $\gcd(a, b) = 1$. Let us assume that there is no large Zsigmondy prime for (a, b, n). If there is no Zsigmondy prime for (a, b, n), we can determine the possible values of (a, b, n) based on Zsigmondy's theorem. We will specifically investigate the case where there is a Zsigmondy prime for (a, b, n) but no large Zsigmondy prime for (a, b, n).

Let $n \geq 3$ and let q be a Zsigmondy prime for (a, b, n) but that is not a large Zsigmondy prime for (a, b, n). It follows that $n = q - 1$ and $q^2 \nmid a^n - b^n$. From Lemma 5, we know that it is necessary for $q \mid \Phi_n(a, b)$ to hold. From Lemma 4, $\Phi_n(a, b)$ can have at most one non-Zsigmondy prime divisor p with the possibilities $p = 2$ or $p = \operatorname{gpf}(n)$. Now, we have three cases to consider:

`Case 1:` If $\Phi_n(a, b) = 2q$ and $n = 2^\beta$ where $\beta \geq 2$. In this case, we have $q = 2^\beta + 1$; therefore, it must be a Fermat prime, so $\beta = 2^s$ for some $s \geq 1$. From Corollary 1 we have

$$\Phi_n(a, b) = \Phi_2(a^{2^{\beta-1}}, b^{2^{\beta-1}}) = a^{2^{\beta-1}} + b^{2^{\beta-1}} \geq 2^{2^{\beta-1}} + 1.$$

For $\beta \geq 4$ we have $2^{2^{\beta-1}} + 1 > 2(2^\beta + 1)$ therefore $\Phi_n(a, b) > 2(n + 1) = 2q$, leading to a contradiction with our assumption. We are left with two possibilities: $n = 4$

or $n = 8$. However, if $n = 8$, then $q = n + 1$ cannot be a prime, and therefore, the only possibility is $n = 4$.

`Case 2:` If $\Phi_n(a, b) = pq$, where $p = \mathrm{gpf}(n) > 2$, is the greatest prime divisor of n. Then $n = p^\beta k$, where β is a positive integer and k is the smallest positive integer satisfying $p \mid a^k - b^k$. Clearly, $k \mid p - 1$. We can divide this case into two subcases.
`Case 2.a:` If $\beta \geq 2$, then by combining Corollary 1 and Corollary 3, we can get

$$\Phi_n(a, b) = \Phi_{pk}(a^{p^{\beta-1}}, b^{p^{\beta-1}}) \geq (a^{p^{\beta-1}} - b^{p^{\beta-1}})^{\Phi(pk)}.$$

Since $a > b$, we can derive the inequality

$$(a^{p^{\beta-1}} - b^{p^{\beta-1}})^{\Phi(pk)} \geq (2^{p^{\beta-1}} - 1)^{\Phi(pk)} \geq (2^{p^{\beta-1}} - 1)^{p-1} \geq (2^{p-1} - 1)^{p^{\beta-1}}.$$

Since $k < p$, we have

$$\Phi_n(a, b) = pq = p(p^\beta k + 1) < p^{\beta+2}.$$

Since $p \geq 3$, we have $2^{p-1} - 1 \geq p$, and thus,

$$\Phi_n(a, b) \geq (2^{p-1} - 1)^{p^{\beta-1}} \geq p^{p^{\beta-1}}.$$

Therefore, $\beta + 2 > p^{\beta-1}$ must hold, which is not possible when $\beta \geq 3$. Therefore, if $\beta \neq 2$, then a large Zsigmondy prime exists for (a, b, n). Let us investigate the case $\beta = 2$. By substituting $\beta = 2$ into our previous inequalities, we obtain

$$p^4 = p^{\beta+2} > \Phi_n(a, b) \geq (2^{p^{\beta-1}} - 1)^{p-1} = (2^p - 1)^{p-1} \geq (2^p - 1)^2.$$

It is not possible when $p \geq 5$. Moreover, there exists a large Zsigmondy prime for (a, b, n) when $p \geq 5$. So, in the second case, if there is no large Zsigmondy prime for (a, b, n), then $p = 3$, $\beta = 2$, and $k = 1$ or $k = 2$. Thus, the only exceptional values are $n = 18$ and $n = 9$. If $n = 9$, then $n + 1$ is not a prime, and $q = n + 1$ is not a Zsigmondy prime for (a, b, n). Therefore, the only possibility is $n = 18$. We will find the pairs (a, b) at the end of the proof.
`Case 2.b:` If $\beta = 1$, then by combining Corollary 1 and Corollary 3, we can obtain,

$$\Phi_n(a, b) = \Phi_{pk}(a, b) = \frac{\Phi_k(a^p, b^p)}{\Phi_k(a, b)} \geq \Big(\frac{a^p - b^p}{a + b}\Big)^{\phi(k)} \geq \Big(\frac{2^p - 1}{3}\Big)^{\phi(k)}.$$

In this case, $\Phi_n(a, b) = (pk + 1)p < p^3$ holds. Then either $\frac{2^p-1}{3} < p$ or $\phi(k) < 3$. Which means either $p \leq 3$ or $k \leq 6$. If $p = 3$, then $n = 6$. If $p > 3$, then $\phi(k) \leq 2$, thus $k = 1, 2, 3, 4$ or 6.

If $\phi(k) = 2$, then $k = 3, 4$ or 6, and

$$p^3 > \Phi_n(a, b) \geq \Big(\frac{2^p - 1}{3}\Big)^2$$

holds. This is not possible when $p \geq 7$. If $p = 5$, then $k = 4$ must hold since $k \mid p-1$. But then $n = 20$, so $q = n+1$ is not a Zsigmondy prime for (a, b, n).

If $\phi(k) = 1$, then $k = 1$ or $k = 2$. We have the inequality

$$p^3 > \Phi_n(a,b) \geq \frac{2^p - 1}{3}.$$

This is not possible when $p \geq 13$. If $k = 1$, then $n = p$, but then $q = n+1$ cannot be a prime number. If $k = 2$, then $n = 2p$. If $p = 11$, then $q = 23$, and $\Phi_n(a,b) = 253$. However, this contradicts the fact that $\Phi_{22}(a,b) \geq \frac{2^{11}-1}{3} > 253$. If $p = 7$, then $n = 14$, but then $q = n+1$ is not a prime number. Thus, $p = 5$ and $n = 10$ or $p = 3$ and $n = 6$ must hold. Ultimately, the only possible values are $n = 6$ and $n = 10$. Again, we will handle the determination of pairs (a, b) at the end of the proof.

`Case 3:` $\Phi_n(a,b) = q$, where $q = n+1$, is an odd prime number. So, n must be even. We will analyze this case in two steps.

If $q-1$ is divisible by 4, then from Corollary 3 and Corollary 1, we obtain

$$\Phi_n(a,b) = \Phi_{q-1}(a,b) = \Phi_{\frac{q-1}{2}}(a^2,b^2) \geq (a^2-b^2)^{\phi(\frac{q-1}{2})}.$$

We can further refine the inequality as follows:

$$q = \Phi_n(a,b) \geq (a^2-b^2)^{\phi(\frac{q-1}{2})} \geq 3^{\phi(\frac{q-1}{2})}.$$

From Lemma 1, we have $\phi(n) \geq \frac{1}{2}\sqrt{n}$. If we substitute this into the previous inequality, we get:

$$q \geq 3^{\phi\left(\frac{q-1}{2}\right)} \geq 3^{\frac{\sqrt{q-1}}{2\sqrt{2}}}.$$

This is only possible when $q \leq 179$. Substituting this back into the inequality, we obtain

$$3^5 > q \geq 3^{\phi\left(\frac{q-1}{2}\right)}.$$

This holds only when $\phi\left(\frac{q-1}{2}\right) \leq 4$, which is only possible if $q-1$ has no prime divisors greater than 5. By manually checking all the remaining possibilities of q, we can see that

$$q \geq 3^{\phi(\frac{q-1}{2})}$$

is satisfied only when $q \leq 13$. If we look at all the cases, we find $n = 4, 12$, with only $n = 12$ being new.

If $q-1$ is not divisible by 4, then from Corollary 1, we obtain

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

In this case, we need a stronger estimate than what we obtain in Corollary 3. It is easy to show that

$$\frac{|a^2 - b^2 e^{i\theta}|}{|a - be^{i\theta}|} \geq \frac{a^2+b^2}{a+b}.$$

Thus, we can derive the following estimate:

$$\frac{\Phi_{\frac{q-1}{2}}(a^2,b^2)}{\Phi_{\frac{q-1}{2}}(a,b)} \geq \left(\frac{a^2+b^2}{a+b}\right)^{\phi(\frac{q-1}{2})} \geq \left(\frac{5}{3}\right)^{\phi(\frac{q-1}{2})}.$$

We know that $\Phi_{q-1} = q$, so by using Lemma 1, we obtain

$$q \geq \left(\frac{5}{3}\right)^{\phi(\frac{q-1}{2})} \geq \left(\frac{5}{3}\right)^{\frac{\sqrt{q-1}}{2\sqrt{2}}}.$$

This is only possible when $q \leq 1667$. Substituting this back into the inequality, we obtain

$$\left(\frac{5}{3}\right)^{15} > q \geq \left(\frac{5}{3}\right)^{\phi\left(\frac{q-1}{2}\right)}.$$

This condition holds only when $\phi\left(\frac{q-1}{2}\right) \leq 14$, which implies that $q-1$ has no prime divisors greater than 13. By further analysis, we find that this inequality is satisfied only when $q \leq 43$. When we manually check all the remaining possibilities of q, we observe that the inequality

$$q \geq \left(\frac{5}{3}\right)^{\phi(\frac{q-1}{2})}$$

is satisfied only when $q \leq 11$. After examining all cases, we find $n = 2, 6, 10$, but we have already found these values in other cases. □

Proof of Theorem 1. Now we will determine all the triples (a, b, n) such that there is no large Zsigmondy prime for (a, b, n). From Lemma 8, we know that if there is no large Zsigmondy prime for (a, b, n), then n must be equal to one of the numbers $\{2, 4, 6, 10, 12, 18\}$. From Lemma 7, we know that if there is no large Zsigmondy prime for (a, b, n), then $\Phi_n(a, b) \leq (n + 1)\,\mathrm{gpf}(n)$. Furthermore, from Lemma 4, we know that if there is no large Zsigmondy prime for (a, b, n), then $\Phi_n(a, b) = n + 1$ or $\Phi_n(a, b) = (n + 1)\,\mathrm{gpf}(n)$. We have to analyze the following six cases.

`Case 1:` If $n = 2$ and there is no large Zsigmondy prime for (a, b, n), then no prime greater than 3 can divide $a^2 - b^2$; furthermore, $9 \nmid a^2 - b^2$. Then $a + b = 2^s$ or $a + b = 3 \cdot 2^s$ for non-negative integer s. The first case is also an exceptional case of Zsigmondy's theorem.

`Case 2:` If $n = 4$, then $\Phi_4(a, b) = a^2 + b^2 \leq 10$ must hold. Furthermore, we have $a^2 + b^2 = 5, 10$. We can easily check that the only possible values for (a, b) are $(2, 1)$ and $(3, 1)$.

`Case 3:` If $n = 6$, then $\Phi_6(a, b) = a^2 - ab + b^2 \leq 21$ must hold. Furthermore, we have $\Phi_6(a, b) = 7, 21$. From this, we get $(3, 1), (3, 2), (5, 1)$ and $(5, 4)$ as suitable values for (a, b). Also, we have one exceptional case of Zsigmondy's theorem here when $(a, b) = (2, 1)$.

`Case 4:` If $n = 10$, then $\Phi_{10}(a, b) = a^4 - a^3b + a^2b^2 - ab^3 + b^4 \leq 55$ must hold. Furthermore, we have $\Phi_{10}(a, b) = 11, 55$. We can easily check that the only possible values for (a, b) are $(2, 1)$ and $(3, 2)$.

`Case 5:` If $n = 12$, then $\Phi_{12}(a, b) = a^4 - a^2b^2 + b^4 \leq 39$ must hold. Furthermore, we have $\Phi_{12}(a, b) = 13, 39$. We can easily check that the only possible value for (a, b) is $(2, 1)$.

`Case 6:` If $n = 18$, then $\Phi_{18}(a, b) = a^6 - a^3b^3 + b^6 \leq 57$ must hold. Furthermore, we have $\Phi_{18}(a, b) = 19, 57$. We can easily check that the only possible value for (a, b) is $(2, 1)$. □

With this we have completed the classification of all triples of integers (a, b, n) for which no large Zsigmondy prime exists.

References

[1] E. Artin, The orders of the linear groups, *Comm. Pure and Appl. Math.* **8** (3) (1955), 355-365.

[2] W. Feit, On large Zsigmondy primes, *Proc. Amer. Math. Soc.* **102** (1988), 29-36.

[3] W. Feit, G.M. Seitz, On finite rational groups and related topics, *Illinois J. Math.* **33** (1) (1988), 103-131.

[4] W. Feit, Extensions of cuspidal characters of $GL_m(q)$, *Publ. Math. Debrecen* **34** (3-4) (1987), 273-297.

[5] M. Roitman, On Zsigmondy primes, *Proc. Am. Math. Soc.* **125** (7) (1997), 1913-1919.

[6] Yan Sheng Ang, An elementary proof of Zsigmondy's theorem, preprint.
`https://angyansheng.github.io/blog/an-elementary-proof-of-zsigmondys-theorem`

[7] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsch. Math. Phys.* **3** (1892), 265-284.