JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Joseph COHEN et Jack SONN

A cyclotomic generalization of the sequence $\gcd(a^n - 1, b^n - 1)$

Tome 27, n° 1 (2015), p. 53-65.

<http://jtnb.cedram.org/item?id=JTNB_2015__27_1_53_0>

Journal de Théorie des Nombres
de Bordeaux **27** (2015), 53–65

A cyclotomic generalization of the sequence $\gcd(a^n - 1, b^n - 1)$

par Joseph COHEN et Jack SONN

Résumé. Les propriétés des suites $\gcd(a^n - 1, b^n - 1)$, $n = 1, 2, 3, ...$, où a, b sont des éléments fixés (multiplicativement indépendants) dans $\mathbb{Z}, \mathbb{C}[T]$ ou $\mathbb{F}_q[T]$, ont été étudiées depuis des décennies. Dans le cas de $\mathbb{Z}$, Bugeaud, Corvaja et Zannier ont obtenu une borne supérieure $\exp(\epsilon n)$ pour tout $\epsilon > 0$ donné et tout n grand, et montrent que la borne est optimale en extrayant la borne inférieure $\exp(\exp(c\frac{\log n}{\log\log n}))$, pour une infinité de n (où c est une constante absolue), d'un article d'Adleman, Pomerance, et Rumely. Silverman a montré une borne inférieure analogue $\deg\gcd(a^n - 1, b^n - 1) \geq cn$ pour une infinité de n, pour l'anneau $\mathbb{F}_q[T]$. Ce travail généralise le théorème de Silverman à $\gcd(\Phi_m(a^n), \Phi_m(b^n))$ pour tout entier positif m, où $\Phi_m(x)$ est le $m$ième polynôme cyclotomique, le résultat de Silverman correspondant au cas $m = 1$. Sur $\mathbb{Z}$, la borne inférieure a été montrée dans la thèse du premier auteur dans le cas $m = 2$, i.e. pour la suite $\gcd(a^n + 1, b^n + 1)$. Ici nous montrons que la borne inférieure est valide sur $\mathbb{Z}$ pour tout m, sous GRH.

Abstract. There has been interest during the last decade in properties of the sequence $\gcd(a^n - 1, b^n - 1)$, $n = 1, 2, 3, ...$, where a, b are fixed (multiplicatively independent) elements in one of $\mathbb{Z}, \mathbb{C}[T]$, or $\mathbb{F}_q[T]$. In the case of $\mathbb{Z}$, Bugeaud, Corvaja and Zannier have obtained an upper bound $\exp(\epsilon n)$ for any given $\epsilon > 0$ and all large n, and demonstrate its sharpness by extracting from a paper of Adleman, Pomerance, and Rumely a lower bound $\exp(\exp(c\frac{\log n}{\log\log n}))$ for infinitely many n, where c is an absolute constant. Silverman has proved an analogous lower bound $\deg\gcd(a^n - 1, b^n - 1) \geq cn$ for infinitely many n, over $\mathbb{F}_q[T]$. This paper generalizes Silverman's theorem to $\gcd(\Phi_m(a^n), \Phi_m(b^n))$ for any positive integer m, where $\Phi_m(x)$ is the mth cyclotomic polynomial, Silverman's result being the case $m = 1$. Over $\mathbb{Z}$, the lower bound has been proved in the first author's Ph.D. thesis for the case $m = 2$, i.e. for $\gcd(a^n + 1, b^n + 1)$. Here we prove a conditional

Manuscrit reçu le 12 septembre 2013, accepté le 23 mai 2014.
Mots clefs. Greatest common divisor, sequence, cyclotomic polynomial.
Mathematics Subject Classification. 11A05, 11R47,11N37.

result that the lower bound for arbitrary m holds over $\mathbb{Z}$ under GRH (the generalized Riemann Hypothesis).

1. Background

In recent years there has been interest [3],[2],[15] in sequences of the form

$$\gcd(a^n - 1, b^n - 1), \quad n = 1, 2, 3, \ldots.$$

where a, b are fixed elements in one of $\mathbb{Z}, \mathbb{C}[T]$, or $\mathbb{F}_q[T]$. Motivated by recurrence sequences and the Hadamard quotient theorem, Bugeaud, Corvaja and Zannier [3] bounded the cancellation in the sequence $\frac{b^n-1}{a^n-1}$ by proving the following upper bound result:

Theorem 1.1. [3] *Let a, b be multiplicatively independent positive integers, $\epsilon > 0$. Then*

$$\log \gcd(a^n - 1, b^n - 1) < \epsilon n$$

for all sufficiently large n.

Moreover, it is conjectured in [2] that if the additional (necessary) condition $\gcd(a-1, b-1) = 1$ holds, then $\gcd(a^n - 1, b^n - 1) = 1$ for infinitely many n.

Returning to [3], in order to show that Theorem 1.1 is close to best possible, it is remarked in [3] that one can derive from a paper of Adleman, Pomerance, and Rumely [1] a lower bound result:

Theorem 1.2. [3] *For any two positive integers a, b, there exist infinitely many positive integers n for which*

$$\log \gcd(a^n - 1, b^n - 1) > \exp(c \frac{\log n}{\log \log n}),$$

where c is an absolute constant.

The result in [1] from which this is derived is an improvement of a result of Prachar [13]:

Theorem 1.3. [13] *Let $\delta(n)$ denote the number of divisors of n of the form $p - 1$, with p prime. Then there exist infinitely many n such that*

$$\delta(n) > \exp(c \log n / (\log \log n)^2).$$

The improvement in [1] (with a similar proof) removes the exponent 2 (and the $p - 1$ are squarefree):

Theorem 1.4. [1] *Let $\delta(n)$ denote the number of divisors of n of the form $p - 1$, with p prime and $p - 1$ squarefree. Then there exist infinitely many n such that*

$$\delta(n) > \exp(c \log n / \log \log n).$$

It is interesting to note that in [13], Prachar was motivated by a paper of Nöbauer [12] which dealt with the group of invertible polynomial functions on $\mathbb{Z}/n\mathbb{Z}$ and particularly the subgroup of functions of the form x^k, whereas in [1], Adleman, Pomerance and Rumely were motivated by the computation of a lower bound on the running time of a primality testing algorithm.

In [4], the first author tested the robustness of these results and asks what happens to Theorem 1.2 if $\gcd(a^n-1,b^n-1)$ is replaced by $\gcd(a^n+1,b^n+1)$ or by $\gcd(a^n+1,b^n-1)$, and proceeded to prove the analogous results for these sequences, using [1]:

Theorem 1.5. [4] *For any two positive nonsquare integers a, b, there exist infinitely many positive integers n for which*

$$\log\gcd(a^n+1,b^n+1) > \exp(c\frac{\log n}{\log\log n})$$

where c is a constant depending on a and b. The same result holds for $\gcd(a^n+1,b^n-1)$.

(The corresponding analogues of Theorem 1.1 follow immediately from $x^n \pm 1 | x^{2n}-1$.)

If one observes that the polynomials $x-1$ and $x+1$ are the first and second cyclotomic polynomials $\Phi_m(x)$, $m=1,2$, we ask if Theorems 1.1 and 1.2 also hold for $\gcd(\Phi_m(a^n),\Phi_m(b^n))$ for any positive integer m, or even for $\gcd(\Phi_u(a^n),\Phi_v(b^n))$ for suitable positive integers u, v. For Theorem 1.1, this is immediate from $\Phi_m(x)|x^m-1$. In this paper we are interested in this “cyclotomic polynomial generalization" for Theorems 1.2 (and 1.5).

It should be remarked that Corvaja and Zannier have made far-reaching generalizations of Theorem 1.1 in several directions, including function fields [5], [6], [7]. See also Luca [11].

Silverman [15] proved an analogue of Theorem 1.2 for the global function fields $\mathbb{F}_q(T)$:

Theorem 1.6. *Let $\mathbb{F}_q$ be a finite field and let $a(T), b(T) \in \mathbb{F}_q(T)$ be nonconstant monic polynomials. Fix any power q^k of q and any congruence class $n_0+q^k\mathbb{Z} \in \mathbb{Z}/q^k\mathbb{Z}$. Then there is a positive constant $c=c(a,b,q^k)>0$ such that*

$$\deg(\gcd(a(T)^n-1,b(T)^n-1)) \geq cn$$

for infinitely many $n \equiv n_0 \pmod{q^k}$.

In Section 2 we prove the “cyclotomic polynomial generalization" of Silverman's theorem for any positive integer m, with an explicit constant c, using an effective version of the Chebotarev density theorem for function fields. In Section 3 we give a similar but conditional proof of the cyclotomic polynomial generalization of Theorem 1.2 for any positive integer m, using an effective version of the Chebotarev density theorem for number fields which is contingent on the Generalized Riemann Hypothesis (GRH).

Acknowledgment. We are grateful to Zeev Rudnick, Ram Murty and Jeff Lagarias for helpful discussions at various stages of the preparation of this paper. We also thank Joe Silverman for helpful comments on the initial draft. Finally, we are grateful to the referee for suggesting that we produce an explicit constant in Theorem 2.1.

2. The case $a = a(T), b = b(T) \in \mathbb{F}_q(T)$

In this section we will generalize Silverman's Theorem 1.6 [15] above.

Theorem 2.1. *Let $\mathbb{F}_q$ be a finite field, and let m be a positive integer prime to q, $m = \ell_1^{j_1} \cdots \ell_s^{j_s}, \ell_1 < \ell_2 < \cdots < \ell_s$, the factorization of m into primes. Let $a(T), b(T) \in \mathbb{F}_q(T)$ be nonconstant monic polynomials which are not ℓ_ith powers in $\mathbb{F}_q(T)$ for $i = 1, ..., s$. Fix a power q^k of q, and any congruence class $n_0 + q^k\mathbb{Z} \in \mathbb{Z}/q^k\mathbb{Z}$. Then there is an explicit constant $c = c(m, q^k) > 0$ such that*

$$\deg(\gcd(\Phi_m(a(T)^n), \Phi_m(b(T)^n)) \geq cn$$

for infinitely many $n \equiv n_0$ (mod q^k). The constant c may be taken as

$$c := \frac{1}{2} m q^{-k} \prod_i (1 - \frac{1}{\ell_i})^2.$$

Proof. Assume first that $(n_0, q) = 1$. Choose the smallest positive integer r such that $(r, m) = 1$ and $rmn_0 \equiv -1$ $(mod\ q^k)$. Let $Q = q^t$, where $t \geq k$ and $q^t \equiv 1 \bmod mr$ (e.g. $t = k\phi(mr)$). Let $n = \frac{Q^N - 1}{mr}$, where N is a positive integer. Let $\pi = \pi(T)$ be a monic irreducible polynomial of degree N in $\mathbb{F}_Q[T]$ not dividing $a(T)b(T)$ (this holds e.g. if $\deg(\pi) > \deg(a(T)b(T))$). Then, writing $a = a(T), b = b(T)$, $\pi | \Phi_m(a^n)$ if and only if a^n is a primitive mth root of unity mod π, i.e. $a^{nm} \equiv 1 \bmod \pi$ and $a^{mn/\ell} \not\equiv 1 \bmod \pi$ for every prime $\ell | m$. Substituting $n = \frac{Q^N - 1}{mr}$, this holds $\Leftrightarrow$

$$a^{\frac{Q^N - 1}{r}} \equiv 1\ (mod\ \pi)$$

and

$$a^{\frac{Q^N - 1}{r\ell}} \not\equiv 1\ (mod\ \pi)$$

for all primes $\ell | m$. The first condition holds $\Leftrightarrow$ there exists $A \in \mathbb{F}_Q[T]$ such that $a \equiv A^r$ $(mod\ \pi)$. For such an A, the second condition is equivalent to

$$A^{\frac{Q^N-1}{\ell}} \not\equiv 1\ (mod\ \pi)$$

which is equivalent to saying that A is not an ℓth power mod π, and since $(r, \ell) = 1$, this is equivalent to saying that a is not an ℓth power mod π. It follows that the two conditions hold together $\Leftrightarrow$ a is an rth power mod π and a is not an ℓth power mod π for all ℓ dividing m. We conclude that $\pi | \Phi_m(a^n)$ if and only if a is an rth power mod π and a is not an ℓth power mod π for all ℓ dividing m. Similarly, $\pi | \Phi_m(b^n)$ if and only if b is an rth power mod π and b is not an ℓth power mod π for all ℓ dividing m.

To count the number of π dividing $\gcd(\Phi_m(a^n), \Phi_m(b^n))$, we will use an effective version of Chebotarev's density theorem for global function fields [8], p. 119, Prop. 6.4.8. For this purpose, let

$$F := \mathbb{F}_{Q^N}(T)(\sqrt[r]{a}, \sqrt[r]{b})$$

and let

$$E := \mathbb{F}_{Q^N}(T)(\sqrt[\ell_1]{a}, \sqrt[\ell_1]{b}, ..., \sqrt[\ell_s]{a}, \sqrt[\ell_s]{b}).$$

Since $\deg \pi = N$, π splits completely in $\mathbb{F}_{Q^N}(T)$. Therefore a and b are rth powers mod π if and only if π splits completely in F. Furthermore, a and b are not ℓth powers mod π for any ℓ dividing m if and only if π does not split completely in $\mathbb{F}_{Q^N}(T)(\sqrt[\ell]{a})$ nor in $\mathbb{F}_{Q^N}(T)(\sqrt[\ell]{b})$ for any ℓ dividing m. Accordingly, consider the Galois extension $EF/\mathbb{F}_Q(T)$ with Galois group G_N, and let

$$C_N = G(EF/F) \setminus \{[\bigcup_i G(EF/F(\sqrt[\ell_i]{a}))] \bigcup [\bigcup_i G(EF/F(\sqrt[\ell_i]{b}))]\}.$$

(C_N is the complement in the first group you see in the display, of the union of all the other (sub)groups you see in the display.)

It is easily verified that C_N is G_N-invariant under conjugation, i.e. a union of conjugacy classes in G_N. Then:

π splits completely in F and π does not split completely in $\mathbb{F}_{Q^N}(T)(\sqrt[\ell]{a})$ nor in $\mathbb{F}_{Q^N}(T)(\sqrt[\ell]{b})$ for any ℓ dividing m, if and only if the Artin symbol $(\pi, EF/\mathbb{F}_Q(T)) \subseteq C_N$.

In the course of the proof we will make use of the following

Lemma 2.2. $|G_N| = Nr_0 \prod_i \ell_i^{e_i}$*, where* $r_0 = [F : \mathbb{F}_{Q^N}(T)] | r^2$*, and* $e_i = 1$ *or* 2 (depending on multiplicative dependence of a, b mod ℓ_ith powers in $\mathbb{F}_{Q^N}(T)$). $|C_N| = \prod_i (\ell_i - 1)^{e_i}$.

Proof. The first assertion $|G_N| = Nr_0 \prod_i \ell_i^{e_i}$ is evident, so it suffices to show $|C_N| = \prod_i (\ell_i - 1)^{e_i}$. We can view $G(EF/F)$ as a direct product of

$e := \sum e_i$ cyclic groups of (varying) prime order. The e subgroups in the union (appearing in the definition of C_N), with respect to a suitable basis of $G(EF/F)$, are those obtained by deleting one of the basis elements. The union consists of all vectors (with respect to this basis) having at least one zero coordinate, hence the complement consists of all elements with no zero coordinate, hence of order $\prod(\ell_i - 1)^{e_i}$. □

We introduce some additional notation:

$M := [EF : \mathbb{F}_{Q^N}(T)]$,

$d_0 := \deg a(T)b(T)$,

$g := g_{EF}$, the genus of EF.

We now apply the Chebotarev density theorem [8], p. 119, Prop. 6.4.8.[1] Observing that a conjugacy class can be replaced by any union of conjugacy classes in that theorem, we get

$$||\{\pi \in \mathbb{F}_Q[T],\ \text{monic irred. deg. } N :\ (\pi, EF/\mathbb{F}_Q(T)) \subseteq C_N\}| - \frac{|C_N|}{|G_N|}Q^N| < \frac{2|C_N|}{|G_N|}[(M+g)Q^{N/2} + MQ^{N/4} + g + M]$$

(genus of $\mathbb{F}_Q(T)$ is 0).

From this,

$$|\{\pi \in \mathbb{F}_Q[T] : \pi \text{ monic irreducible of degree } N,\ (\pi, EF/\mathbb{F}_Q(T)) \subseteq C_N\}| > \frac{|C_N|}{|G_N|}Q^N - \frac{2|C_N|}{|G_N|}[(M+g)Q^{N/2} + MQ^{N/4} + g + M].$$

Using $|G_N| = MN$ and enlarging the preceding (negative) term in square brackets, this last expression exceeds

$$\frac{|C_N|}{N}[\frac{1}{M} - (4g+6)Q^{-N/2}]Q^N.$$

We now impose the condition that the last term in square brackets exceed $\frac{1}{2M}$, i.e.

$$Q^{N/2} > 8g + 12.$$

When this condition holds, we deduce the inequality

$$\begin{aligned}&\deg(\gcd(\Phi_m(a(T)^n), \Phi_m(b(T)^n))\\ &\geq N|\{\pi \in \mathbb{F}_Q[T] : \pi \text{ monic irreducible of degree } N,\ (\pi, EF/\mathbb{F}_Q(T)) \subseteq C_N\}|\\ &> \frac{|C_N|}{2M}Q^N > cn\end{aligned}$$

[1] This is an effective Chebotarev density theorem for global function fields, implied by the Riemann Hypothesis for curves over finite fields, which is a theorem.

for all sufficiently large N, with $c = \frac{|C_N|mr}{2M}$, using $n = \frac{Q^N-1}{mr}$. To obtain the form of the constant c appearing in the statement of the theorem, we apply Lemma 2.2 for the explicit expression for $|C_N|$, $M = r_0 \prod \ell^i$, replace r with its lower bound 1, and replace r_0 with its upper bound q^k.

It is desirable to make the condition on N explicit as well, by giving an explicit upper bound on g. To this end we apply the Riemann-Hurwitz formula [8], p. 69, to the field extension $EF/\mathbb{F}_{Q^N}(T)$:

$$2g-2 = -2M + \sum_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} (e_{\mathfrak{P}/\mathfrak{p}} - 1) \deg \mathfrak{P}$$

where $\mathfrak{p}$ runs through primes of $\mathbb{F}_{Q^N}(T)$. The number of ramified primes is bounded by $d_0 = \deg a(T)b(T)$ so the sum is bounded by d_0M. Hence $g \leq 1+d_0M/2 = 1+d_0r_0\prod_i \ell_i^{e_i} \leq 1+d_0q^{2k}m^2$. It follows from what we have seen that the constant c given in the theorem is valid for all N satisfying

$$Q^{N/2} > 8(1+d_0q^{2k}m^2)+12,$$

hence for all

$$n = \frac{Q^N-1}{mr} > [8(1+d_0q^{2k}m^2)+12]^2/m.$$

This proves Theorem 2.1 when $(n_0, q) = 1$. The case $(n_0, q) \neq 1$ follows from the case $(n_0, q) = 1$ as in [15]. □

Remarks. It is notable that the constant c is independent of $a(T)$ and $b(T)$. Also, the hypothesis in Theorem 2.1 that $a(T)$ and $b(T)$ are not ℓ_ith powers in $\mathbb{F}_q(T)$ is a technical one, used in the proof, but we do not know if it is necessary.

The proof of Theorem 2.1 can be generalized to yield the following

Theorem 2.3. *Let $\mathbb{F}_q$ be a finite field, u, v be positive integers, $d = \gcd(u,v)$, and assume $\gcd(u/d, d) = \gcd(v/d, d) = 1$. Let $a = a(T)$, resp. $b = b(T) \in \mathbb{F}_q[T]$ be monic nonconstant polynomials which are not ℓth powers in $\mathbb{F}_q[T]$ for all $\ell|u$, resp. $\ell|v$. Fix a power q^k of q, and any congruence class $n_0 + q^k\mathbb{Z} \in \mathbb{Z}/q^k\mathbb{Z}$. Then there is a positive constant c such that*

$$\deg(\gcd(\Phi_u(a(T)^n), \Phi_v(b(T)^n)) \geq cn$$

for infinitely many $n \equiv n_0 \pmod{q^k}$.

The details are omitted.

3. The case $a, b \in \mathbb{Z}$

In this section we prove the generalization of Theorem 1.2 for any positive integer m under the Generalized Riemann Hypothesis (GRH), which enters the picture when the generalization of Prachar's argument in this situation leads to an application of the effective Chebotarev density theorem to a tower of Galois extensions $L_d/\mathbb{Q}$. The exceptional zeros of the corresponding zeta functions of the L_d are required to be bounded away from 1 as d goes to infinity [2]. Since we do not know if the exceptional zeros in our tower are bounded away from 1, we apply the stronger GRH version of the effective Chebotarev density theorem in which there are no exceptional zeros. In this section we make a change of notation, using N instead of m for the subscript of the cyclotomic polynomial, and m is used for a different purpose.

Theorem 3.1 (contingent on GRH)**.** *Let N be a positive integer, $N = \ell_1^{s_1}\cdots\ell_r^{s_r}, \ell_1 < \ell_2 < \cdots < \ell_r$, the factorization of N into primes. Let a, b be positive integers, relatively prime to N, which are not ℓ_ith powers in $\mathbb{Q}$ for $i = 1, ..., r$. Then there exist infinitely many positive integers n such that*

$$\log\gcd(\Phi_N(a^n), \Phi_N(b^n)) > \exp(\frac{c\log n}{\log\log n}),$$

where c is a positive constant depending only on a, b, N.

Proof. Suppose p is a prime congruent to 1 mod N such that neither a nor b is a ℓ_ith power mod p for $i = 1, ..., r$. Suppose also that n is a positive integer prime to N and divisible by $\frac{p-1}{N}$. Then $p \mid \gcd(\Phi_N(a^n), \Phi_N(b^n))$. Indeed, $(a^n)^N \equiv 1 \pmod{p}$. The orders of $a_1 := a^{\frac{p-1}{N}}$ and of a^n mod p are equal and divide N. If a_1 has order mod p less than N, then there is a prime $\ell|N$ such that $a_1^{N/\ell} \equiv 1$ mod p, so $a^{(p-1)/\ell} \equiv 1$ mod p, whence a is an ℓth power mod p, contrary to hypothesis. Thus a_1 and a^n both have order N mod p, $p|\Phi_N(a^n)$. Similarly $p|\Phi_N(b^n)$.

The idea of the proof of the theorem, a generalization of the proof in Prachar's paper, is to use the pigeonhole principle to produce, for large x, an $n \le x^2$ with more than $\exp(c\frac{\log x}{\log\log x})$ divisors of the form $\frac{p-1}{N}$, p prime, c an absolute constant. The result then follows.

Fix $0 < \delta < 1$. Let x be a positive real number and let $K = K_\delta(x)$ be the product of all the primes $p \le \delta\log x$, $p \nmid N$. Let A be the set of pairs (m, p), m a positive integer, p a prime, $m \le x$, $p \le x$, $\gcd(m, N) = 1$, $p \equiv 1 \pmod{N}$, $p \not\equiv 1 \pmod{N\ell_i}$, $i = 1, ..., r$, neither a nor b is an ℓ_ith power mod p, $i = 1, ..., r$, and $K|m\frac{p-1}{N}$.

Now for each $d|K$, let A_d be the subset of A consisting of pairs $(m, p) \in A$ such that $(m, K) = K/d$ and $d|\frac{p-1}{N}$. Let $N_0 := \ell_1\cdots\ell_r$. We first bound $|A_d|$ from below by bounding the following subset of A_d of the form $A'_d \times A''_d$, where

$$A'_d = \{m \le x : (m, N_0K) = K/d\}$$

[2] The 2-part of $[L_d : \mathbb{Q}]$ is unbounded as $d \to \infty$ so the results of Stark and of Odlyzko and Skinner do not seem to apply.

and

$$A''_d = \{p \le x : p \equiv 1 \mod N,\ p \not\equiv 1 \mod N\ell_i,\ i = 1, ..., r,\ d \mid \frac{p-1}{N},$$

$$\text{and neither } a \text{ nor } b \text{ is an } \ell_i\text{th power mod } p,\ i = 1, ..., r\}.$$

To bound $|A'_d \times A''_d|$ from below, it suffices to bound each of $|A'_d|, |A''_d|$ from below and take the product of the two lower bounds.

First, writing $d' = K/d$,

$$|A'_d| = |\{m \le x : d'|m, (m/d', N_0K/d') = 1\}|$$

$$= |\{m/d' \le x/d' : (m/d', N_0K/d') = 1\}|$$

$$\ge \phi(N_0K/d')[\frac{x/d'}{N_0K/d'}] = \phi(N_0d)[x/N_0K]$$

where ϕ denotes Euler's ϕ-function and $[-]$ the integer part.

To bound $|A''_d|$ from below we use the effective form of Chebotarev's density theorem due to Lagarias and Odlyzko [10] as formulated by Serre [14] under the generalized Riemann Hypothesis (GRH).

The condition $d \mid \frac{p-1}{N}$ is equivalent to $p \equiv 1 \pmod{Nd}$, which is equivalent to p splits completely in $\mathbb{Q}(\mu_{Nd})$, where μ_n denotes the group of nth roots of unity. The condition a is an ℓth power mod p (ℓ prime) is equivalent to the condition $x^\ell - a$ has a root mod p, which for $p \equiv 1$ modulo ℓ is equivalent to the condition $x^\ell - a$ splits into linear factors mod p, which is equivalent to the condition p splits completely in (the Galois extension) $\mathbb{Q}(\mu_\ell, \sqrt[\ell]{a})$ of $\mathbb{Q}$, which for $p \equiv 1 \pmod{Nd}$ and $\ell \mid N$ is equivalent to p splits completely in $\mathbb{Q}(\mu_{Nd}, \sqrt[\ell]{a})$.

Consider the Galois extension $F_d = \mathbb{Q}(\mu_{NN_0d},\ \sqrt[N_0]{a},\ \sqrt[N_0]{b})$ of $\mathbb{Q}$, with Galois group $G_d = G(F_d/\mathbb{Q})$, and the subset

$$C_d = G(F_d/\mathbb{Q}(\mu_{Nd})) \setminus \{[\bigcup_i G(F_d/\mathbb{Q}(\mu_{Nd},\ \sqrt[\ell_i]{a}))] \bigcup [\bigcup_i G(F_d/\mathbb{Q}(\mu_{Nd},\ \sqrt[\ell_i]{b}))]$$

$$\bigcup [\bigcup_i G(F_d/\mathbb{Q}(\mu_{Nd\ell_i}))]\}$$

of G_d.

It follows from the definition of C_d that

$$A''_d = \{p \le x : p \text{ unramified in } F_d, (p, F_d/\mathbb{Q}) \subseteq C_d\}$$

where $(p, F_d/\mathbb{Q})$ denotes the Artin symbol. Set

$$\pi_{C_d}(x) := |A''_d| = |\{p \le x : p \text{ unramified in } F_d, (p, F_d/\mathbb{Q}) \subseteq C_d\}|.$$

By the effective Chebotarev density theorem cited above, under GRH for the Dedekind zeta function of F_d,

$$R_d(x) := |\pi_{C_d}(x) - \frac{|C_d|}{|G_d|}Li(x)| \leq c_1 \frac{|C_d|}{|G_d|} x^{1/2}(\log D_{F_d} + n_{F_d} \log x)$$

where c_1 is an absolute constant, D_{F_d} is the discriminant of F_d, $n_{F_d} = [F_d : \mathbb{Q}]$ is the degree of F_d over $\mathbb{Q}$, and $Li(x)$ is the logarithmic integral $\int_2^x \frac{dt}{\log t}$.

We have $|G_d| = \phi(Nd)\prod_i \ell_i^{e_i}$, where $e_i = 2$ or 3 according to whether or not a, b are multiplicatively dependent mod ℓ_ith powers in $\mathbb{Q}(\mu_{NN_0d})$. The proof of Lemma 2.2 yields $|C_d| = \prod_i (\ell_i - 1)^{e_i}$. We conclude that

$$\frac{|C_d|}{|G_d|} = \frac{\prod_i (\ell_i - 1)^{e_i}}{\phi(Nd)\prod_i \ell_i^{e_i}}.$$

By [14], Prop. 5, p. 128,

$$\log D_{F_d} \leq (n_{F_d} - 1) \sum_{p|Nabd} \log p + n_{F_d} \log n_{F_d} |\{p : p|Nabd\}|.$$

Now

$$n_{F_d} = \phi(Nd)\prod_i \ell_i^{e_i} \leq \phi(Nd)N^3 = \phi(N)N^3\phi(d),$$

so

$$\begin{gathered}\log D_{F_d} \leq (\phi(N)N^3\phi(d) - 1)\log^2(Nabd) \\ +\phi(N)N^3\phi(d)\log(\phi(N)N^3\phi(d))\log(Nabd) \\ \leq \phi(N)N^3\phi(d)\log^2(Nabd) \\ +\phi(N)N^3\phi(d)\log(\phi(N)N^3\phi(d))\log(Nabd) \\ \leq 2(\phi(N)N^3ab)^3\phi(d)\log^2 d \\ = f(N,a,b)\phi(d)\log^2 d.\end{gathered}$$

It now follows that

$$\begin{gathered}|A_d| \geq |A'_d \times A''_d| = |A'_d||A''_d| = |A'_d|\pi_{C_d}(x) \\ \geq \phi(N_0d)[\frac{x}{N_0K}](\frac{|C_d|}{|G_d|}Li(x) - c_1\frac{|C_d|}{|G_d|}x^{1/2}(\log D_{F_d} + n_{F_d}\log x)) \\ \geq \phi(N_0d)[\frac{x}{N_0K}]\frac{|C_d|}{|G_d|}(Li(x) - c_1x^{1/2}(\log D_{F_d} + n_{F_d}\log x))\end{gathered}$$

where c_1 is an absolute constant. We now bound

$$Li(x) - c_1x^{1/2}(\log D_{F_d} + n_{F_d}\log x)$$

from below. First,

$$\begin{gathered}\log D_{F_d} + n_{F_d}\log x \leq f(N,a,b)\phi(d)\log^2 d + \phi(N)N^3\phi(d)\log x \\ \leq g(N,a,b)\phi(d)\log^2 x \leq g(N,a,b)x^\delta \log x \leq g(N,a,b)x^{\delta+\epsilon}\end{gathered}$$

(using $\phi(d) < d < K < x^\delta$ and $\log x < x^\epsilon$ for any given ϵ and sufficiently large x). From this,

$$Li(x) - c_1 x^{1/2}(\log D_{F_d} + n_{F_d}\log x) \geq \frac{x}{2\log x} - c_1 x^{\frac{1}{2}+\delta+\epsilon} g(N,a,b) \geq \frac{x}{4\log x}$$

(for sufficiently large x, using $Li(x) \sim \frac{x}{\log x}$). We then have

$$|A'_d|\pi_{C_d}(x) \geq \phi(N_0 d)[\frac{x}{N_0 K}]\frac{x}{4\log x}\frac{|C_d|}{|G_d|}$$

$$\geq \frac{1}{2}\phi(N_0 d)\frac{x}{N_0 K}\frac{x}{4\log x}\frac{\phi(N_0)^2}{\phi(N)N_0^2}\cdot\frac{1}{\phi(d)}$$

$$\geq \frac{1}{8}\frac{\phi(N_0)^3 x^2}{\phi(N)N_0^3 K\log x} = \frac{h(N)}{K}\frac{x^2}{\log x}.$$

It then follows that

$$|A| = \sum_{d|K}|A_d| \geq \frac{h(N)}{K}\frac{x^2}{\log x}\sum_{d|K}1 = \frac{h(N)}{K}\frac{x^2}{\log x}2^{\omega(K)}$$

$$\geq \frac{h(N)}{K}\frac{x^2}{\log x}2^{\frac{\frac{1}{4}\delta\log x}{\log\log x}}$$

where $\omega(K)$ denotes the number of primes dividing K. For the last inequality we use [9], 22.2, p. 341, and 22.10, p. 355:

$$\omega(K) \sim \frac{\log K}{\log\log K} \Rightarrow \omega(K) \geq \frac{\log K}{2\log\log K} \geq \frac{1}{4}\frac{\delta\log x}{\log\log x}.$$

Now the number of positive integers $n \leq x^2$ such that $K|n$ is at most $\frac{x^2}{K}$. Furthermore, for every pair $(m,p) \in A$, $m\frac{p-1}{N}$ is such an n. Therefore there exists an $n \leq x^2$ such that $K|n$ with at least

$$\frac{|A|}{x^2/K} > \frac{h(N)}{\log x}2^{\frac{\frac{1}{4}\delta\log x}{\log\log x}} = h(N)\exp(c_2\delta\frac{\log x}{\log\log x} - \log\log x) > \exp(c_3\frac{\log x}{\log\log x})$$

representations of the form $m\frac{p-1}{N}$, for x sufficiently large, where c_2, c_3 are absolute constants. It follows that $GCD(\Phi_N(a^n), \Phi_N(b^n))$ is a product of at least $\exp(c_3\frac{\log x}{\log\log x})$ primes, hence is itself at least $\exp\exp(c_4\frac{\log x}{\log\log x})$. As $n \leq x^2$ and $\frac{\log x}{\log\log x}$ is an increasing function (for $x > e^e$), the last expression is

$\geq \exp\exp(c_5\frac{\log n}{\log\log n})$. □

As with Theorem 2.3 at the end of the preceding section, the proof of Theorem 3.1 can be generalized to yield the following

Theorem 3.2 (contingent on GRH). *Let M, N be positive integers. Let $D = \gcd(M,N)$ and assume $\gcd(M/D, D) = \gcd(N/D, D) = 1$. Let $L = lcm(M,N) = \ell_1^{s_1} \cdots \ell_r^{s_r}, \ell_1 < \ell_2 < \cdots \ell_r$, the factorization of L into primes. Let a, b be positive integers, relatively prime to L, which are not ℓ_ith powers in $\mathbb{Q}$ for $i = 1, ..., r$. Then there exist infinitely many positive integers n such that*

$$\gcd(\Phi_M(a^n), \Phi_N(b^n)) > (\exp(\exp(\frac{c \log n}{\log \log n}))),$$

where c is a positive constant depending only on a, b, N.

The proof is similar to the proof of Theorem 3.1; we omit the details. Also here, the case $M = 1$, $N = 2$ was proved unconditionally in [4].

References

[1] L.M. Adleman, C. Pomerance and R.S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. Math. **117**, (1983), 173–206.

[2] N. Ailon and Z. Rudnick, *Torsion points on curves and common divisors of $a^k - 1, b^k - 1$*, Acta Arith. **113**, (2004), 31–38.

[3] Y. Bugeaud, P. Corvaja and U. Zannier, *An upper bound for the G.C.D. of $a^n - 1$ and* $b^n - 1$, Math. Zeit. **243**, (2003), 79–84.

[4] J. Cohen, *Primitive roots in algebraic number fields*, Ph.D. Thesis, Technion (2004).

[5] P. Corvaja and U. Zannier, *A lower bound for the height of a rational function at S-unit points*, Monatsh. Math. **144**, 3 (2005), 203–224.

[6] P. Corvaja and U. Zannier, *Some cases of Vojta's conjecture on integral points over function fields*, J. Algebraic Geom. **17**, (2008), 295–333.

[7] P. Corvaja and U. Zannier, *Greatest common divisors of $u - 1, v - 1$ in positive characteristic and rational points on curves over finite fields*, J. Eur. Math. Soc. (JEMS), **15**, 5 (2013), 1927–1942.

[8] M. Fried and M. Jarden, *Field Arithmetic*, Third Edition, Springer-Verlag , New York-Heidelberg, (2008).

[9] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers (Fifth Ed.)*, Oxford Univ. Press, Oxford, (1979).

[10] J. Lagarias and A.M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic Number Fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, 1975), Academic Press, London, (1977) 409–464.

[11] F. Luca, *On the greatest common divisor of $u - 1$ and $v - 1$ with u and v near S-units*, Monatsh. Math. **146** 3, (2005), 239–256.

[12] W. Nöbauer, *Über eine Gruppe der Zahlentheorie*, Monatsh. Math. **58**, (1954), 181–192.

[13] K. Prachar, *Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p - 1$ haben*, Monatsh. Math. **59**, (1955), 91–97.

[14] J.-P. Serre, *Quelques applications du theoreme de densite de Chebotarev*, Publ. Math. IHES **54**, (1982), 123–201.

[15] J. Silverman, *Common divisors of $a^n - 1$ and $b^n - 1$ over function fields*, New York J. Math. **10**, (2004), 37–43.

Joseph Cohen
Department of Mathematics
Technion — Israel Institute of Technology
Haifa, 32000
Israel
E-mail: coheny@tx.technion.ac.il

Jack Sonn
Department of Mathematics
Technion — Israel Institute of Technology
Haifa, 32000
Israel
E-mail: sonn@math.technion.ac.il