Divisors of terms of recurrence sequences

C.L. Stewart
cstewart@uwaterloo.ca

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada

International Number Theory Conference in Memory of Alf van der Poorten

To the Memory of Alf

Let $r_1, \dots, r_k$ and $u_0, \dots, u_{k-1}$ be integers and put

$$u_n = r_1 u_{n-1} + \cdots + r_k u_{n-k}, \tag{1}$$

for $n = k,\ k+1, \dots$. The sequence $(u_n)_{n=0}^{\infty}$ is a linear recurrence sequence.

It is well known that

$$u_n = f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n, \tag{2}$$

where $f_1, \ldots, f_t$ are non-zero polynomials with degrees less than $\ell_1, \ldots, \ell_t$ respectively and with coefficients from $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ where $\alpha_1, \ldots, \alpha_t$ are the non-zero roots of the characteristic polynomial

$$X^k - r_1 X^{k-1} - \cdots - r_k,$$

and $\ell_1, \ldots, \ell_t$ are their respective multiplicities.

The sequence $(u_n)_{n=0}^{\infty}$ is said to be non-degenerate if $t > 1$ and α_i/α_j is not a root of unity for $1 \leq i < j \leq t$.

In 1935 Mahler proved that if u_n is the n-th term of a non-degenerate linear recurrence sequence then

$$|u_n| \to \infty \quad \text{as } n \to \infty.$$

(3)

For any integer m let $P(m)$ denote the greatest prime factor of m with the convention that $P(0) = P(\pm 1) = 1$.

van der Poorten and Schlickewei and ,independently, Evertse proved, by means of a p-adic version of Schmidt's Subspace Theorem due to Schlickewei , that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate linear recurrence sequence then

$$P(u_n) \to \infty \quad \text{as } n \to \infty.$$

(4)

Estimates (3) and (4) are both ineffective.

On the other hand if one of the roots of the characteristic polynomial has modulus strictly larger than the others, say

$$|\alpha_1| > |\alpha_i|, \quad i = 2, \ldots, t, \tag{5}$$

then

$$|u_n| > c_1 n^{\ell_1} |\alpha_1|^n,$$

for $n > c_2$ where c_1 is one half of the absolute value of the coefficient of x^{ℓ_1} in the polynomial f_1 and where c_2 is a positive number which is effectively computable in terms of $\alpha_1, \ldots, \alpha_t$ and $f_1, \ldots, f_t$.

Shparlinski and independently S. obtained effective lower bounds for the greatest prime factor of u_n when there is a dominant root.

S.(2008)There exist positive numbers C_1 and C_2 such that If $u_n \neq f_1(n)\alpha_1^n$, then, for n greater than C_2

$$P(u_n) > C_1 \log n \frac{\log \log n}{\log \log \log n}. \qquad (6)$$

For binary recurrence sequences, so $k = 2$ in (1), stronger estimates apply.

If u_n is the n-th term of a binary recurrence sequence, then, for $n \geq 0$,

$$u_n = a\alpha^n + b\beta^n, \tag{7}$$

where α and β are the roots of $x^2 - r_1 x - r_2$ and

$$a = \frac{u_0\beta - u_1}{\beta - \alpha} \quad \text{and} \quad b = \frac{u_1 - u_0\alpha}{\beta - \alpha},$$

whenever $\alpha \neq \beta$.

The binary recurrence sequence $(u_n)_{n=0}^{\infty}$ is non-degenerate whenever $ab\alpha\beta \neq 0$ and α/β is not a root of unity.

In 1967 Schinzel proved that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence then there exist positive numbers $c_7,\ c_8$ and c_9 such that

$$P(u_n) > c_7 n^{c_8} (\log n)^{c_9},$$

where $c_8 = 1/84$ and $c_9 = 7/12$ if α and β are integers while $c_8 = 1/133$ and $c_9 = 7/19$ otherwise and where c_7 is effectively computable in terms of $r,\ s,\ u_0$ and u_1.

In 1982 S. proved that if u_n, as in (11), is the n-th term of a non-degenerate binary recurrence sequence then

$$P(u_n) > c_{10}\left(\frac{n}{\log n}\right)^{1/(d+1)}, \tag{8}$$

where d denotes the degree of α over the rationals.

In 1995 Yu and Hung improved (8). They proved that if u_n is the n-th term of a non-degenerate binary recurrence sequence then

$$P(u_n) > c_{12}n^{1/(d+1)}.$$

There is a special class of binary recurrence sequences which have more structure and for which stronger estimates can be obtained.These are Lucas sequences and their divisibility properties have been investigated by Euler , Lagrange ,Gauss, Dirichlet and many others.

Let α and β be complex numbers such that $\alpha + \beta$ and $\alpha\beta$ are non-zero coprime integers and α/β is not a root of unity. Put

$$u_n = (\alpha^n - \beta^n)/(\alpha - \beta) \quad \text{for } n \geq 0.$$

The integers u_n are known as Lucas numbers.

In 1876 Lucas announced several new results concerning Lucas sequences $(u_n)_{n=0}^{\infty}$ and in a substantial paper in 1878 he gave a systematic treatment of the divisibility properties of Lucas numbers and indicated some of the contexts in which they appeared.

Much later Matijasevic appealed to these properties in his solution of Hilbert's 10th problem.

In 1912 Carmichael proved that if α and β are real and $n > 12$ then

$$P(u_n) \geq n - 1. \tag{9}$$

Results of this character had been established earlier for integers of the form $a^n - b^n$ where a and b are integers with $a > b > 0$. Indeed Zsigmondy in 1892 and Birkhoff and Vandiver in 1904 proved that for $n > 2$

$$P(a^n - b^n) \geq n + 1, \tag{10}$$

while in the special case that $b = 1$ the result is due to Bang in 1886.

In 1930 Lehmer showed that the divisibility properties of Lucas numbers hold in a more general setting. Suppose that $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime non-zero integers with α/β not a root of unity and, for $n > 0$, put

$$\tilde{u}_n = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{for } n \text{ odd,} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{for } n \text{ even.} \end{cases}$$

Integers of the above form have come to be known as Lehmer numbers.

Observe that Lucas numbers are also Lehmer numbers up to a multiplicative factor of $\alpha+\beta$ when n is even.

In 1955 Ward proved that if α and β are real then for $n > 18$,

$$P(\tilde{u}_n) \geq n - 1, \tag{11}$$

and four years later Durst observed that (11) holds for $n > 12$.

A prime number p is said to be a primitive divisor of a Lucas number u_n if p divides u_n but does not divide $(\alpha - \beta)^2 u_2 \cdots u_{n-1}$.

Similarly p is said to be a primitive divisor of a Lehmer number $\tilde{u}_n$ if p divides $\tilde{u}_n$ but does not divide $(\alpha^2 - \beta^2)^2 \tilde{u}_3 \cdots \tilde{u}_{n-1}$.

For any integer $n > 0$ and any pair of complex numbers α and β, we denote the n-th cyclotomic polynomial in α and β by $\Phi_n(\alpha, \beta)$, so

$$\Phi_n(\alpha, \beta) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (\alpha - \zeta^j \beta),$$

where ζ is a primitive n-th root of unity.

One may check that $\Phi_n(\alpha, \beta)$ is an integer for $n > 2$ if $(\alpha + \beta)^2$ and $\alpha\beta$ are integers.

If, in addition, $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime non-zero integers, α/β is not a root of unity and $n > 4$ and n is not 6 or 12 then $P(n/(3,n))$ divides $\Phi_n(\alpha,\beta)$ to at most the first power and all other prime factors of $\Phi_n(\alpha,\beta)$ are congruent to 1 or -1 modulo n.

The last assertion can be strengthened to all other prime factors of $\Phi_n(\alpha,\beta)$ are congruent to $1 \pmod{n}$ in the case that α and β are coprime integers.

Since

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta), \tag{12}$$

$\Phi_1(\alpha, \beta) = \alpha - \beta$ and $\Phi_2(\alpha, \beta) = \alpha + \beta$ we see that if n exceeds 2 and p is a primitive divisor of a Lucas number u_n or Lehmer number $\tilde{u}_n$ then p divides $\Phi_n(\alpha, \beta)$.

Further, a primitive divisor of a Lucas number u_n or Lehmer number $\tilde{u}_n$ is not a divisor of n and so it is congruent to $\pm 1 \pmod{n}$.

Estimates (9), (10) and (11) follow as consequences of the fact that the n-th term of the sequences in question possesses a primitive divisor.

It was not until 1962 that this approach was extended to the case where α and β are not real by Schinzel . He proved, by means of an estimate for linear forms in two logarithms of algebraic numbers due to Gelfond , that there is a positive number C, which is effectively computable in terms of α and β, such that if n exceeds C then $\tilde{u}_n$ possesses a primitive divisor.

In 1974 Schinzel employed an estimate of Baker for linear forms in the logarithms of algebraic numbers to show that C can be replaced by a positive number C_0, which does not depend on α and β, and in 1977 we showed C_0 could be taken to be $e^{452}4^{67}$.

This was subsequently refined by Voutier to 30030. In addition we proved that C_0 can be taken to be 6 for Lucas numbers and 12 for Lehmer numbers with finitely many exceptions and that the exceptions could be determined by solving a finite number of Thue equations.

This program was successfully carried out by Bilu, Hanrot and Voutier and as a consequence they were able to show that for $n > 30$ the n-th term of a Lucas or Lehmer sequence has a primitive divisor. Thus (9) and (11) hold for $n > 30$ without the restriction that α and β be real.

In 1962 Schinzel asked if there exists a pair of integers a, b with ab different from $\pm 2c^2$ and $\pm c^h$ with $h \geq 2$ for which $P(a^n - b^n)$ exceeds $2n$ for all sufficiently large n.

In 1965 Erdős conjectured that

$$\frac{P(2^n - 1)}{n} \to \infty \quad \text{as } n \to \infty.$$

Thirty five years later Murty and Wong showed that Erdős' conjecture is a consequence of the *abc* conjecture . They proved, subject to the *abc* conjecture, that if ε is a positive real number and a and b are integers with $a > b > 0$ then

$$P(a^n - b^n) > n^{2-\varepsilon},$$

provided that n is sufficiently large in terms of a, b and ε.

In 2004 Murata and Pomerance proved, subject to the Generalized Riemann Hypothesis, that

$$P(2^n - 1) > n^{4/3} / \log\log n \tag{13}$$

for a set of positive integers n of asymptotic density 1.

In 1962 Schinzel proved that if a and b are coprime and ab is a square or twice a square then

$$P(a^n - b^n) \geq 2n + 1$$

provided that one excludes the cases $n = 4, 6, 12$ when $a = 2$ and $b = 1$.

To prove this result he appealed to an Aurifeuillian factorization of Φ_n.

In 1975 we proved that if κ is a positive real number with $\kappa < 1/\log 2$ then $P(a^n - b^n)/n$ tends to infinity with n provided that n runs through those integers with at most $\kappa \log\log n$ distinct prime factors,

Subsequently,with Tarlok Shorey, we extended the result to Lucas and Lehmer numbers.

Theorem 1. Let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero integers and α/β is not a root of unity. There exists a positive number C, which is effectively computable in terms of $\omega(\alpha\beta)$ and the discriminant of $\mathbb{Q}(\alpha/\beta)$, such that for $n > C$,

$$P(\Phi_n(\alpha,\beta)) > n\exp(\log n/104\log\log n). \tag{14}$$

This answers the question of Schinzel and proves the conjecture of Erdős. Specifically, if a and b are integers with $a > b > 0$ then

$$P(a^n - b^n) > n \exp(\log n / 104 \log\log n), \tag{15}$$

for n sufficiently large in terms of the number of distinct prime factors of ab.

The factor 104 which occurs on the right hand side of (15) has no arithmetical significance.

The proof depends upon estimates for linear forms in the logarithms of algebraic numbers in the complex and the p-adic case. In particular it depends upon recent work of Kunrui Yu where improvements upon the dependence on the parameter p in the lower bounds for linear forms in p-adic logarithms of algebraic numbers are established.

This allows us to estimate directly the order of primes dividing $\Phi_n(\alpha, \beta)$. The estimates are non-trivial for small primes and, coupled with an estimate from below for $|\Phi_n(\alpha, \beta)|$, they allow us to show that we must have a large prime divisor of $\Phi_n(\alpha, \beta)$ since otherwise the total non-archimedean contribution from the primes does not balance that of $|\Phi_n(\alpha, \beta)|$.

Let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero integers and α/β is not a root of unity. We shall assume, without loss of generality, that

$$|\alpha| \geq |\beta|.$$

Observe that

$$\alpha = \frac{\sqrt{r}+\sqrt{s}}{2}, \quad \beta = \frac{\sqrt{r}-\sqrt{s}}{2}$$

where r and s are non-zero integers with $|r| \neq |s|$. Further $\mathbb{Q}(\alpha/\beta) = \mathbb{Q}(\sqrt{rs})$. Note that $(\alpha^2-\beta^2)^2 = rs$ and we may write rs in the form m^2d with m a positive integer and d a square-free integer so that $\mathbb{Q}(\sqrt{rs}) = \mathbb{Q}(\sqrt{d})$.

For any algebraic number γ let $h(\gamma)$ denote the absolute logarithmic height of γ. In particular if $a_0(x-\gamma_1)\cdots(x-\gamma_d)$ in $\mathbb{Z}[x]$ is the minimal polynomial of γ over $\mathbb{Z}$ then

$$h(\gamma) = \frac{1}{d}\left(\log a_0 + \sum_{j=1}^{d} \log \max(1, |\gamma_j|)\right).$$

Notice that

$$\alpha\beta(x-\alpha/\beta)(x-\beta/\alpha)=\alpha\beta x^2-((\alpha+\beta)^2-2\alpha\beta)x+\alpha\beta$$

is a polynomial with integer coefficients and so either α/β is rational or the polynomial is a multiple of the minimal polynomial of α/β. Therefore we have

$$h(\alpha/\beta)\leq\log|\alpha|. \tag{16}$$

Lemma 1. Suppose that $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime. If $n > 4$ and $n \neq 6, 12$ then $P(n/(3n))$ divides $\Phi_n(\alpha, \beta)$ to at most the first power. All other prime factors of $\Phi_n(\alpha, \beta)$ are congruent to $\pm 1 \pmod{n}$.

Let K be a finite extension of $\mathbb{Q}$ and let $\wp$ be a prime ideal in the ring of algebraic integers $\mathcal{O}_K$ of K. Let $\mathcal{O}_\wp$ consist of 0 and the non-zero elements α of K for which $\wp$ has a non-negative exponent in the canonical decomposition of the fractional ideal generated by α into prime ideals. Then let P be the unique prime ideal of $\mathcal{O}_\wp$ and put $\overline{K_\wp} = \mathcal{O}_\wp / P$. Further for any α in $\mathcal{O}_\wp$ we let $\overline{\alpha}$ be the image of α under the residue class map that sends α to $\alpha + P$ in $\overline{K_\wp}$.

Our next result is motivated by work of Lucas and Lehmer .

Lemma 2. Let d be a square-free integer different from 1, θ be an algebraic integer of degree 2 over $\mathbb{Q}$ in $\mathbb{Q}(\sqrt{d})$ and let θ' denote the algebraic conjugate of θ over $\mathbb{Q}$. Suppose that p is a prime which does not divide $2\theta\theta'$. Let $\wp$ be a prime ideal of the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$ lying above p. The order of $\overline{\theta/\theta'}$ in $(\overline{\mathbb{Q}(\sqrt{d})}_{\wp})^{\times}$ is a divisor of 2 if p divides $(\theta^2 - \theta'^2)^2$ and a divisor of $p - (d/p)$ otherwise.

Lemma 3. If $1 \leq n < x$ and $(n, \ell) = 1$ then

$$\pi(x, n, \ell) < 3x/(\varphi(n)\log(x/n)).$$

Lemma 4. Let d be a squarefree integer with $d \neq 1$ and let p_k denote the k-th smallest prime of the form $N\pi_k = p_k$ where N denotes the norm from $\mathbb{Q}(\sqrt{d})$ to $\mathbb{Q}$ and π_k is an algebraic integer in $\mathbb{Q}(\sqrt{d})$. Let ε be a positive real number. There is a positive number C, which is effectively computable in terms of ε and d, such that if k exceeds C then

$$\log p_k < (1 + \varepsilon)\log k.$$

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and put $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ and $d = [K : \mathbb{Q}]$. Let $\wp$ be a prime ideal of the ring $\mathcal{O}_K$ of algebraic integers in K lying above the prime number p. Denote by $e_\wp$ the ramification index of $\wp$ and by $f_\wp$ the residue class degree of $\wp$. For α in K with $\alpha \neq 0$ let $\mathrm{ord}_\wp \alpha$ be the exponent to which $\wp$ divides the principal fractional ideal generated by α in K and put $\mathrm{ord}_\wp 0 = \infty$. For any positive integer m let $\zeta_m = e^{2\pi i/m}$ and put $\alpha_0 = \zeta_{2^u}$ where $\zeta_{2^u} \in K$ and $\zeta_{2^{u+1}} \notin K$.

Suppose that $\alpha_1, \dots, \alpha_n$ are multiplicatively independent $\wp$-adic units in K. Let $\overline{\alpha_0}, \overline{\alpha_1}, \dots, \overline{\alpha_n}$ be the images of $\alpha_0, \alpha_1, \dots, \alpha_n$ respectively under the residue class map at $\wp$ from the ring of $\wp$-adic integers in K onto the residue class field $\overline{K}_\wp$ at $\wp$. For any set X let $|X|$ denote its cardinality. Let $\langle \overline{\alpha_0}, \overline{\alpha_1}, \dots, \overline{\alpha_n} \rangle$ be the subgroup of $(\overline{K}_\wp)^\times$ generated by $\overline{\alpha_0}, \overline{\alpha_1}, \dots, \overline{\alpha_n}$. We define δ by

$$\delta = 1 \quad \text{if} \quad [K(\alpha_0^{1/2}, \alpha_1^{1/2}, \dots, \alpha_n^{1/2}) : K] < 2^{n+1}$$

and

$$\delta = (p^{f_\wp} - 1)/|\langle \overline{\alpha_0}, \overline{\alpha_1}, \dots, \overline{\alpha_n} \rangle|$$

if

$$[K(\alpha_0^{1/2}, \alpha_1^{1/2}, \dots, \alpha_n^{1/2}) : K] = 2^{n+1}. \tag{17}$$

Lemma 5. Let p be a prime with $p \geq 5$ and let $\wp$ be an unramified prime ideal of $\mathcal{O}_K$ lying above p. Let $\alpha_1, \ldots, \alpha_n$ be multiplicatively independent $\wp$-adic units. Let $b_1, \ldots, b_n$ be integers, not all zero, and put

$$B = \max(5, |b_1|, \ldots, |b_n|).$$

Then

$$\mathrm{ord}_\wp(\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1) < Ch(\alpha_1) \cdots h(\alpha_n) \log B$$

where

$$C = 376(n+1)^{3/2} \left(7e\frac{p-1}{p-2}\right)^n d^{n+2} \log^* d \log(e^4(n+1)d) \cdot \max\left(\frac{p^{f_\wp}}{\delta}\left(\frac{n}{f_\wp \log p}\right)^n, e^n f_\wp \log p\right).$$

Let $(\alpha+\beta)^2$ and $\alpha\beta$ be non-zero integers with α/β not a root of unity. We may suppose that $|\alpha| \geq |\beta|$.

For any positive integer n let $\mu(n)$ denote the Möbius function of n. We have

$$\Phi_n(\alpha,\beta) = \prod_{d|n} (\alpha^{n/d} - \beta^{n/d})^{\mu(d)}. \tag{18}$$

Lemma 6. There exists an effectively computable positive number c_1 such that if n exceeds c_1 then

$$\log|\Phi_n(\alpha,\beta)| \geq \frac{\varphi(n)}{2}\log|\alpha|. \tag{19}$$

Lemma 7. Let n be an integer larger than 1, let p be a prime which does not divide $\alpha\beta$ and let $\wp$ be a prime ideal of the ring of algebraic integers of $\mathbb{Q}(\alpha/\beta)$ lying above p which does not ramify. Then there exists a positive number C, which is effectively computable in terms of $\omega(\alpha\beta)$ and the discriminant of $\mathbb{Q}(\alpha/\beta)$, such that if p exceeds C then

$$\mathrm{ord}_{\wp}((\alpha/\beta)^n - 1) < p \exp(-\log p/51.9 \log\log p) \log|\alpha| \log n.$$

Put $K = \mathbb{Q}(\alpha/\beta)$ and

$$\alpha_0 = \begin{cases} i & \text{if } i \in K \\ -1 & \text{otherwise.} \end{cases}$$

Let v be the largest integer for which

$$\alpha/\beta = \alpha_0^j \theta^{2^v}, \tag{20}$$

with $0 \leq j \leq 3$ and θ in K.

Notice that

$$h(\alpha/\beta) = 2^v h(\theta). \tag{21}$$

Further, by Kummer theory,

$$[K(\alpha_0^{1/2}, \theta^{1/2}) : K] = 4. \tag{22}$$

Furthermore since $p \nmid \alpha\beta$ and α and β are algebraic integers

$$\text{ord}_\wp((\alpha/\beta)^n - 1) \leq \text{ord}_\wp((\alpha/\beta)^{4n} - 1). \tag{23}$$

For any real number x let $[x]$ denote the greatest integer less than or equal to x. Put

$$k = \left[\frac{\log p}{51.8 \log\log p}\right]. \tag{24}$$

Then, for $p > c_2$, we find that $k \geq 2$ and

$$\max\left(p\left(\frac{k}{\log p}\right)^k, e^k \log p\right) = p\left(\frac{k}{\log p}\right)^k. \tag{25}$$

Our proof splits into two cases. We shall first suppose that $\mathbb{Q}(\alpha/\beta) = \mathbb{Q}$ so that α and β are integers. For any positive integer j with $j \geq 2$ let p_j denote the $j-1$-th smallest prime which does not divide $p\alpha\beta$. We put

$$m = n2^{v+2} \tag{26}$$

and

$$\alpha_1 = \theta/p_2 \cdots p_k.$$

Then

$$\theta^m - 1 = \left(\frac{\theta}{p_2 \cdots p_k}\right)^m p_2^m \cdots p_k^m - 1 = \alpha_1^m p_2^m \cdots p_k^m - 1 \tag{27}$$

and

$$\text{ord}_p((\alpha/\beta)^n - 1) \leq \text{ord}_p(\alpha_1^m p_2^m \cdots p_k^m - 1). \tag{28}$$

Note that $\alpha_1, p_2, \ldots, p_k$ are multiplicatively independent since α/β is not a root of unity and $p_2, \ldots, p_k$ are primes which do not divide $p\alpha\beta$. Further, since $p_2, \ldots, p_k$ are different from p and p does not divide $\alpha\beta$, we see that $\alpha_1, p_2, \ldots, p_k$ are p-adic units.

We now apply Lemma 5 with $\delta = 1$, $d = 1$, $f_{\wp} = 1$ and $n = k$ to conclude that

$$\operatorname{ord}_p(\alpha_1^m p_2^m \cdots p_k^m - 1) \le c_3(k+1)^3 \log p \left(7e\frac{p-1}{p-2}\right)^k \max\left(p\left(\frac{k}{\log p}\right)^k, e^k\right)(\log m)h(\alpha_1)\log p_2 \tag{29}$$

Put

$$t = \omega(\alpha\beta).$$

Let q_i denote the i-th prime number. Note that

$$p_k \le q_{k+t+1}$$

and thus

$$\log p_2 + \cdots + \log p_k \le (k-1)\log q_{k+t+1}.$$

By the prime number theorem with error term, for $k > c_4$,

$$\log p_2 + \cdots + \log p_k \le 1.001(k-1)\log k. \tag{30}$$

By the arithmetic geometric mean inequality

$$\log p_2 \cdots \log p_k \le \left(\frac{\log p_2 + \cdots + \log p_k}{k-1}\right)^{k-1}$$

and so,

$$\log p_2 \cdots \log p_k \le (1.001 \log k)^{k-1}. \tag{31}$$

Since $h(\alpha_1) \leq h(\theta) + \log p_2 \cdots p_k$ it follows that

$$h(\alpha_1) \leq c_5 h(\theta) k \log k. \tag{32}$$

Further $m = 2^{v+2} n$ is at most $n^{2^{v+2}}$ and so

$$h(\theta) \log m \leq 4h(\alpha/\beta) \log n \leq 4 \log |\alpha| \log n. \tag{33}$$

Thus

$$\mathrm{ord}_p((\alpha/\beta)^n - 1) < c_6 k^4 \log p \left(7e \frac{p-1}{p-2} 1.001 \frac{k \log k}{\log p} \right)^k p \log |\alpha| \log n.$$

Therefore, for $p > c_7$

$$\mathrm{ord}_p((\alpha/\beta)^n - 1) < p e^{-\frac{\log p}{51.9 \log \log p}} \log |\alpha| \log n. \tag{34}$$