On the greatest prime factor of $2^n - 1$

C.L. Stewart
cstewart@uwaterloo.ca

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

Erdős Centennial 2013, Budapest

For any integer m let $P(m)$ denote the greatest prime factor of m with the convention that $P(m) = 1$ when m is 1, 0 or -1.

In 1965 Erdős conjectured that

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

Let a and b be integers with $a > b > 0$. Zsigmondy in 1892 and Birkhoff and Vandiver in 1904 proved that for $n > 2$

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

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

For any integer $n > 0$ and any pair of integers a and b, we denote the n-th cyclotomic polynomial in a and b by $\Phi_n(a,b)$, so

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

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

The first unconditional refinement of (1) was obtained by Schinzel in 1962. He 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 Stewart 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.

Further if p is a prime then for p sufficiently large

$$P(a^p - b^p) \geq (1/2)p(\log p)^{1/4}.$$

In 1976 Erdős and Shorey proved that there is a positive number *c* such that for p sufficiently large

$$P(a^p - b^p) \geq cp \log p.$$

Further they proved that for almost all primes p

$$P(a^p - b^p) \geq p(\log p)^2/(\log \log p)^3.$$

Let $f(n)$ be a real valued function that tends to infinity with n. We proved in 1977 that for almost all positive integers n

$$P(a^n - b^n) \geq n(\log n)^2/f(n)\log\log n.$$

Let $\sigma(n)$ denote the sum of the positive divisors of n.

Then

$$\sigma(n) = n \sum_{d|n} 1/d.$$

It is easy to show that there is a positive number c_0 such that

$$\sigma(n) > c_0 n \log \log n.$$

for infinitely many positive integers n.

In 1971 Erdős proved that there is a positive number c_1 such that

$$\sigma(2^n - 1)/(2^n - 1) < c_1 \log\log n.$$

In particular

$$\sum_{d|2^n-1} 1/d < c_1 \log\log n.$$

In addition Erdős showed that there is a positive number c_2 such that

$$\sum_{p|2^n-1} 1/p < \log\log\log n + c_2.$$

Both estimates are best possible up to determination of the constants.

Put

$$g(n) = \sum_{p|2^n-1} 1/p.$$

$g(n)$ may be arbitrarily small.In 1991 Erdős Kiss and Pomerance showed that there are infinitely many pairs of consecutive integers for which $g(n)$ and $g(n+1)$ are both large.They showed that for infinitely many positive integers n

$$min(g(n), g(n+1)) > \log\log\log\log n.$$

On the other hand they showed that there is a positive number c_3 such that

$$min(g(n), g(n+1)) < c_3(\log\log\log n)^{2/3}(\log\log\log\log n)^{1/3}$$

for all sufficiently large n.

In 2009 Ford, Luca and Shparlinski proved that the series

$$\sum_{n\geq 1} 1/P(2^n - 1)$$

is convergent.

In 2000 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

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

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

For any integer $n > 0$ and any pair of complex numbers α and β, recall that the n-th cyclotomic polynomial in α and β is given by

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

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

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta), \tag{3}$$

an estimate from below for $P(\Phi_n(\alpha, \beta))$ gives an estimate from below for the greatest prime factor of the n-th term of a Lucas or a Lehmer sequence and in the case that $\alpha = a$ and $\beta = b$ are positive integers gives an estimate from below for

$$P(a^n - b^n).$$

Theorem

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 $n > C$,

$$P(\Phi_n(\alpha,\beta)) > n\exp(\log n/104\log\log n). \tag{4}$$

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

$$P(a^n - b^n) > n \exp(\log n / 104 \log\log n), \tag{5}$$

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 (5) 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 $|\Phi_n(\alpha, \beta)|$.

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

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

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 $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent $\wp$-adic units in K. Let $\overline{\alpha_0}, \overline{\alpha_1}, \ldots, \overline{\alpha_n}$ be the images of $\alpha_0, \alpha_1, \ldots, \alpha_n$ 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 $\langle \overline{\alpha_0}, \overline{\alpha_1}, \ldots, \overline{\alpha_n} \rangle$ be the subgroup of $(\overline{K}_\wp)^\times$ generated by $\overline{\alpha_0}, \overline{\alpha_1}, \ldots, \overline{\alpha_n}$.

We define δ by

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

and

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

if

$$[K(\alpha_0^{1/2}, \alpha_1^{1/2}, \ldots, \alpha_n^{1/2}) : K] = 2^{n+1}. \tag{6}$$

Denote $\log \max(x, e)$ by $\log^* x$.

Lemma (K. Yu)

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

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

The key new feature is the dependence on the parameter p in the above estimate of Kunrui Yu.

Thank you.