An exponential diophantine equation related to odd perfect numbers

Tomohiro Yamada

Mar 3, 2018

Introduction

The main theme in this talk is the equation

$$\frac{x^\ell - 1}{x - 1} = p^m q, m \geq 0, \qquad (1)$$

where ℓ, p, q are given primes such that $p \equiv q \equiv 1 \pmod{\ell}$.

(1) is a specialization of a Thue-Mahler equation:

$$\frac{x^\ell - y^\ell}{x - y} = p^m q^n, m, n \geq 0. \qquad (2)$$

One of Evertse's celebrated results implies that this equation has at most $2 \times 7^{7(\ell-1)^3}$ solutions (Corollary 2 of Evertse, 1984).

Background

Our background is a problem on perfect numbers - integers N satisfying $\sigma(N) = 2N$, where $\sigma(N)$ denotes the sum of divisors of N as usual.

Though it is not known whether or not an odd perfect number exists, many conditions which must be satisfied by such a number are known.

Suppose N is an odd perfect number.

Euler: $N = p^{\alpha} q_1^{2\beta_1} \cdots q_t^{2\beta_t}$ for distinct odd primes $p, q_1, \cdots, q_t$ with $p \equiv \alpha \equiv 1 \pmod 4$.

The special case: $\beta_1 = \cdots = \beta_t = \beta$.

We do not know a proof of the nonexistence of odd perfect numbers even in this case!

Steuerwald (1937): $\beta \neq 1$.

Kanold (1941): $(2\beta+1)^4 \mid N$ and $\beta \neq 2$. Moreover, if $2\beta + 1$ is a power l^k of a prime l, then $p \equiv 1 \pmod{l}$ (esp. $p \neq l$).

McDaniel (1970), Hagis and McDaniel (1972), McDaniel and Hagis (1975), Cohen and Williams (1985), Fletcher, Nielsen and Ochem (2012):
$\beta \geq 9$, $\beta \not\equiv 1 \pmod 3, \not\equiv 2 \pmod 5$, $\beta \neq 11, 14, 18, 24$.

Conjecture (Hagis and McDaniel, 1972): $\beta_1 = \cdots = \beta_t = \beta$ does not occur.

A partial result (Y, 2005):

$\omega(N) \leq 4\beta^2 + 2\beta + 3, N \leq 2^{4^{4\beta^2+2\beta+3}}$.

So that, for each FIXED β, there are only finitely many OPNs with $\beta_1 = \cdots = \beta_t = \beta$.

We note that $N < 2^{4^{\omega(N)}}$ for any odd OPN N(Nielsen, 2003).

A further improvement (Y, to appear in Colloq. Math., arXiv:1706.09341):

$\omega(N) \leq 2\beta^2 + 8\beta + 4, N \leq 2^{4^{2\beta^2+8\beta+4}}$. Moreover, if $\beta \geq 29$ or β is composite, then $\omega(N) \leq 2\beta^2 + 7\beta + 4, N \leq 2^{4^{2\beta^2+7\beta+4}}$.

This result rests on a diophantine lemma:

If ℓ, p, q are given primes such that $\ell \geq 19$ and $p \equiv q \equiv 1 \pmod{\ell}$, then (1) has at most six integer solutions (x, m) such that x is a prime below $2^{4^{\ell^2}}$ if ℓ is a prime ≥ 59 and at most five such solutions if ℓ is a prime ≥ 59.

with Gauss decompositions of cyclotomic polynomials.

For example:

$$\frac{4(x^{23}-1)}{x-1}$$
$$=(2x^{11}+x^{10}-5x^9-8x^8-7x^7-4x^6+4x^5+7x^4+8x^3+5x^2-x-2)^2$$
$$+23(x^{10}+x^9-x^7-2x^6-2x^5-x^4+x^2+x)^2.$$

(Quoted from Section 357, p. 444 of Gauss, Disquisitiones Arithmeticae)

The main result (Y, 2018): If ℓ, p, q are given primes such that $\ell \geq 19$ and $p \equiv q \equiv 1 \pmod{\ell}$, then (1) has at most four positive integral solutions (x, m). Moreover, if (1) has five integral solutions (x_i, m_i) with $m_5 > m_4 > \cdots > m_1 \geq 0$, then $m_1 = 0$ and $x_2 = x_1^r$ for some integer $r \geq 1$.

This gives:

$\omega(N) \leq 2\beta^2 + 6\beta + 4, N \leq 2^{4^{2\beta^2+6\beta+4}}$.

Our proof combines:

Gaps for solutions

and

Upper bounds for the sizes of solutions.

A related result (Y, arXiv:1712.02199).

If $D > 0$ is a positive integer and $p_2 > p_1$ are given primes, then

$$x^2 + D = 2^s p_1^k p_2^l \tag{3}$$

has at most 63 integral solutions (x, s, k, l) with $x, k, l \geq 0$ and $s \in \{0, 2\}$ (Theorem 2 of Evertse (1984) gives 3×7^{14}).

The proof uses Padé approximation technique introduced by Beukers instead of upper bounds for the sizes of solutions.

However, this method does not seem to work for (1) since (1) implies relatively weaker approximation than (3).

Notations and a preliminary lemma

$\Phi_d(x)$: The d-th cyclotomic polynomial.

(So that $\sigma(q^{l-1}) = (q^l - 1)/(q - 1) = \Phi_l(q)$ for q, l prime)

ℓ: a prime ≥ 17 and $D = (-1)^{\frac{\ell-1}{2}} l$, so that always $D \equiv 1 \pmod 4$.

$\mathcal{K}, \mathcal{O}$: $\mathbf{Q}(\sqrt{D})$ and its ring of integers $\mathbf{Z}[(1 + \sqrt{D})/2]$ respectively.

h: the class number of $\mathcal{O}$.

$\epsilon, R = \log \epsilon$: the fundamental unit and the regulator in $\mathcal{K}$ respectively if $D > 0$. In the case $D < -4$, we set $\epsilon = -1$ and $R = \pi i$.

(We note that neither $D = -3$ nor -4 occurs since we have assumed that $\ell \geq 17$)

We use the overline symbol to express the conjugate in $\mathcal{K}$.

Lemma 1(Zsigmondy, 1882, Kanold, 1941, etc.)

Suppose p is a prime and n is a positive integer. If $d \mid (n+1)$, $d > 1$ and (p, d) satisfies neither $(p, d) = (2, 6)$ nor $(p, d) = (2^m - 1, 2)$ for some integer m, then there exists a prime q with $q \equiv 1 \pmod{d}$ and $q \mid F_d(p)$.

Lemma 2A

If x is an integer $> 3^{\lfloor(\ell+1)/6\rfloor}$, then $\Phi_\ell(x)$ can be written in the form $X^2 - DY^2$ for some coprime integers X and Y with $0.3791/x < \left|Y/(X - Y\sqrt{D})\right| < 0.6296/x$.

Let p, q be primes $\equiv 1 \pmod{\ell}$. Then, we can factorize $[p] = \mathfrak{p}\overline{\mathfrak{p}}$ and $[q] = \mathfrak{q}\overline{\mathfrak{q}}$ into prime ideals in $\mathcal{O}$.

Lemma 2B

If p, q are primes $\equiv 1 \pmod{\ell}$ and $\Phi_\ell(x) = p^m q$ for some integer m, then,

$$\left[\frac{X + Y\sqrt{D}}{X - Y\sqrt{D}}\right] = \left(\frac{\overline{\mathfrak{p}}}{\mathfrak{p}}\right)^{\pm m} \left(\frac{\overline{\mathfrak{q}}}{\mathfrak{q}}\right)^{\pm 1}. \qquad (4)$$

Lemma 3A

Assume that ℓ is a prime ≥ 17. If $x_2 > x_1 > 0$ are two multiplicatively independent integers and $\Phi_\ell(x_i) = p^{m_i}q$ for $i = 1, 2$, then $x_2 > x_1^{\lfloor(\ell+1)/6\rfloor}$.

The following lemma is a complementary result of Lemma 3A.

Lemma 3B (Y, 2018)

Assume that ℓ is a prime ≥ 17. If $x_2 > x_1 > 0$ are multiplicatively dependent integers and $\Phi_\ell(x_i) = p^{m_i}q$ for $i = 1, 2$, then $m_1 = 0$ and $x_2 = x_1^r$ for some prime r.

Lemma 4

If $\Phi_\ell(x_i) = p^{m_i} q_j$ for three integers $x_3 > x_2 > x_1 > 0$ with $x_2 > x_1^{\lfloor (\ell+1)/6 \rfloor}$, then $m_3 > 0.397\,|R|\,x_1$.

Matveev's result:

Let $a_1, a_2, \ldots, a_n$ be nonzero algebraic integers in $\mathcal{K}$ such that $\log a_1, \ldots, \log a_n$ are not all zero. For each $j = 1, \ldots, n$, let $A_j \geq \max\{2h(a_j), \log a_j\}$, where $h(a_j)$ denotes the logarithmic absolute height of a_j.

Put

$$
\begin{aligned}
B &= \max\{1, |b_1|\, A_1/A_n, |b_2|\, A_2/A_n, \ldots, |b_n|\}, \\
\Omega &= A_1 A_2 \ldots A_n, \\
C_0 &= 1 + \log 3 - \log 2, \\
C_1(n) &= \frac{16}{n!} e^n (2n+3)(n+2) \\
&\quad \times (4(n+1))^{n+1} (\frac{1}{2} en) \\
&\quad \times (4.4n + 5.5 \log n + 7)
\end{aligned}
\tag{5}
$$

Lemma 5 (Matveev, 2000)

Let $\Lambda = b_1 \log a_1 + \ldots + b_n \log a_n$. Then, under the above notations, we have, $\Lambda = 0$ or

$$\log |\Lambda| > -C_1(n)(C_0 + \log B) \max\left\{1, \frac{n}{6}\right\} \Omega. \tag{6}$$

Upper bounds

for the sizes of solutions

We begin by obtaining an upper bound for the size of a solution of (1).

Assume that $\Phi_\ell(x) = p^m q$. Then we have the following upper bounds for m:

i) If $h \log q > h \log p \geq |R|$, then

$$\begin{aligned} m <& 4.56 C(3) \ell h^2 |R| (\log q) \\ & \times (\log(8C(3)\ell h^2 |R|) + \log\log p). \end{aligned} \tag{7}$$

ii) If $h \log q \geq |R| \geq h \log p$, then

$$\begin{aligned} m <& 4.56 C(3) \frac{\ell}{\log(2\ell)} h \, |R|^2 \, (\log q) \\ & \times \log \left(\frac{8 C(3) \ell \, |R|^3}{2\ell} \right). \end{aligned} \tag{8}$$

iii) If $h \log p > h \log q \geq |R|$, then

$$\begin{aligned} m <& 4.56 C(3) \ell h^2 \, |R| \, (\log q) \\ & \times (\log(4 C(3) \ell h^2 \, |R|) + \log \log q). \end{aligned} \tag{9}$$

iv) If $h \log p \geq |R| \geq h \log q$, then

$$m < 4.56 C(3) \ell h \, |R|^2 \log(4 C(3) \ell h \, |R|^2). \quad (10)$$

v) If $|R| \geq h \log \max\{p, q\}$, then

$$m < 4.56 C(3) \ell \, |R|^3 \, \frac{\log(8 C(3) \ell \, |R|^3)}{\log \ell}. \quad (11)$$

Lemma 2 yields that there exist two integers X, Y such that

$$\left[\frac{X + Y\sqrt{D}}{X - Y\sqrt{D}}\right] = \left(\frac{\bar{\mathfrak{p}}}{\mathfrak{p}}\right)^{\pm m} \left(\frac{\bar{\mathfrak{q}}_j}{\mathfrak{q}_j}\right)^{\pm 1}, \qquad (12)$$

with $0 < \left|Y/(X - Y\sqrt{D})\right| < 0.6296/x$.

Taking the h-th powers, we have

$$\left(\frac{X+Y\sqrt{D}}{X-Y\sqrt{D}}\right)^h = \epsilon^u \left(\frac{\bar{\pi}}{\pi}\right)^{\pm m} \left(\frac{\bar{\eta}}{\eta}\right)^{\pm 1} \neq 1 \quad (13)$$

for some integer u.

Now the logarithmic form

$$\begin{aligned}\Lambda &= u \log \epsilon \pm m \log \left(\frac{\bar{\pi}}{\pi}\right) \pm \left(\frac{\bar{\eta}}{\eta}\right) \\ &= h \log \left(\frac{X + Y\sqrt{D}}{X - Y\sqrt{D}}\right)\end{aligned} \tag{14}$$

satisfies

$$0 < |\Lambda| < \frac{2hY\sqrt{D}}{X - Y\sqrt{D}} < \frac{1.2588h}{x}. \tag{15}$$

We can easily see that $h \log p \leq A(\bar{\pi}/\pi) \leq h \log p +$ $|R|$, $h \log q \leq A(\bar{\eta}/\eta) \leq h \log q + |R|$ and $A(\epsilon) \leq$ $|R|$.

The case $h \log q > h \log p > |R|$.

In this case, $A(\bar{\pi}/\pi) < h \log p + |R| < 2h \log p$, $A(\bar{\eta}/\eta) < h \log q + |R| < 2h \log q$ and $B \leq 2m \log p / \log q$.

Moreover,

$$\frac{uA(\epsilon)}{A(\bar{\eta}/\eta)} = \frac{|u \log \epsilon|}{2A(\bar{\eta}/\eta)} < \frac{2m\,|R|}{\log q} \qquad (16)$$

and

$$\frac{mA(\bar{\pi}/\pi)}{A(\bar{\eta}/\eta)} \leq \frac{m(\log p + |R|)}{\log q} \leq \frac{2m \log p}{\log q}. \qquad (17)$$

Matveev's theorem gives

$$\begin{aligned}\log x - \log(1.2588h) &< -\log|\Lambda| \\ &< C(3)(2h)^2 \\ &\quad \times \log\left(\frac{2m\log p}{\log q}\right)|R|\,(\log p)(\log q).\end{aligned} \tag{18}$$

Taking it into account that $C(3) > 10^{10}$, we may assume that $(2m \log p)/\log q > 10^{10}$. Now, using $h < \ell^{1/2} \log(4\ell)$ (Faisant, 1991), we obtain

$$\begin{aligned} \frac{2m \log p}{\log q} <& 4(2C(3)+1)\ell h^2 |R| \\ & \times \log\left(\frac{2m \log p}{\log q}\right)(\log p) \qquad (19) \\ =:& U \log\left(\frac{2m \log p}{\log q}\right). \end{aligned}$$

Since $2C(3) + 1 > 3.6 \times 10^{10}$, we have

$$\begin{aligned} \frac{m \log p}{\log q} &< 0.569 U \log U \\ &< 4.56 C(3) \ell h^2 |R| (\log p) \\ &\quad \times (\log(8C(3)\ell h^2 |R|) + \log\log p). \end{aligned} \tag{20}$$

We can prove for other cases in similar ways.

Outline of the proof of the main result

Assume that $\Phi_\ell(x_i) = p^{m_i}q$ has five solutions $0 < m_1 < m_2 < m_3 < m_4 < m_5$.

It is clear that $x_1 \geq \max\{q^{1/\ell}, 2\}$.

Since we have assumed that $m_1 > 0$, Lemma 3A yields that $x_3 \geq \max\{q, 2^\ell\}^{\lfloor(\ell+1)/6\rfloor^2/\ell}$.

Now Lemma 4 yields that

$$
\begin{aligned}
m_5 &> 0.397\pi x_3 \\
&> 0.397\pi \max\left\{ q^{\frac{\lfloor (\ell+1)/6 \rfloor^2}{\ell}}, 2^{\left\lfloor \frac{(\ell+1)}{6} \right\rfloor^2} \right\} \quad (21) \\
&:= M.
\end{aligned}
$$

The case $\ell \geq 47$.

With the aid of the upper bound $|R| < \ell^{1/2} \log(4\ell)$ (Faisant, 1991), (7)-(11) implies that $m_5 < M$, which contradicts to (21).

Hence, if $\ell \geq 47$, then $\Phi_\ell(x) = p^m q$ with $m > 0$ has at most four solutions.

The case $\ell = 43$.

We must have $x_1 \geq 3$ since $2^{43} - 1 = 431 \times 9719 \times 2099863$ has three distinct prime factors.

Thus we must have $m_5 > 0.397\pi \max\{q^{49/43}, 3^{49}\}$.

However, (7)-(11) would yield that, if $q < 3^{43}$, then $m < 4.7 \times 10^{16} < 0.397\pi \times 3^{49}$ and, if $q > 3^{43}$, then $m < 2.8 \times 10^{13}(\log q)(\log\log q + 32) < 0.397\pi q^{49/43}$.

Hence, $\Phi_\ell(x) = p^m q$ with $m > 0$ can never have five solutions.

The case $\ell \leq 41$, x_1: large.

If $x_1 \geq 3(\ell = 37, 41), 5(\ell = 29, 31),\ 13(\ell = 23), 68(\ell = 19),\ 63(\ell = 17)$, then m_5 exceeds the upper bounds given in (7)-(11).

Hence, m_5 cannot exist.

The case $\ell \leq 41$, x_1: small.

We checked all x_1 such that $(x_1^\ell - 1)/(x_1 - 1) = p^m q$ with $p \equiv q \equiv 1 \pmod{\ell}$ and $m > 0$.

In all cases, we have $m < 1.3 \times 10^{17}$, while $p \geq 47, x_2 > p^4 > 10^6$ and $m_5 > x_3 > x_2^4 > 10^{24}$.

Hence, m_5 cannot exist.

For example, in the case $\ell = 23$ (in this case, we have $h = 3$ and $R = \pi i$), if $x_1 \geq 13$, then we must have $m_5 > 0.397\pi \max\{q^{16/23}, 13^{16}\}$, which exceeds the upper bounds given in (7)-(11).

If $x_1 < 13$, then we must have $x_1 = 2, 3, 5$; $(10^{23} - 1)/9$ is prime and $(x^{23} - 1)/(x - 1)$ with $x = 4, 6, 7, 8, 9, 11$ or 12 has more than two distinct prime factors.

If $x_1 = 2, 3$ or 5, then $p, q \leq 332207361361$ and $m < 1.3 \times 10^{17}$. But, in any case, we have confirmed that $x_2 > p^4 > 10^6$. Hence, we must have $x_3 > x_2^4 > 10^{24}$ and $m_5 > x_3 > 10^{24}$, which is a contradiction.

Further extension?

A problem: determine all ℓ, p, q such that (1) has ≥ 3 solutions.

(Finiteness follows from the abc-conjecture if we limit $\ell \geq 5$)

References

A. S. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift Math. **5 IV** (1886), 70–80 and 130–137.

Graeme L. Cohen and Williams, R. J., *Extensions of some results concerning odd perfect numbers*, Fibonacci Quart. **23** (1985), 70–76.

L. E. Dickson, *On the cyclotomic function*, Amer. Math. Monthly **12** (1905), 86–89.

G. G. Dandapat, J. L. Hunsucker and Carl Pomerance, *Some new results on odd perfect numbers*, Pacific J. Math. **57** (1975), 359–364.

Peter Hagis Jr. and Wayne L. McDaniel, *A new result concerning the structure of odd perfect numbers*, Proc. Amer. Math. Soc. **32** (1972), 13–15.

H.-J. Kanold, *Untersuchungen über ungerade vollkommene Zahlen*, J. Reine Angew. Math. **183** (1941), 98–109.

H.-J. Kanold, *Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme, I*, J. Reine Angew. Math. **187** (1950), 169–182.

Wayne L. McDaniel, *The non-existence of odd perfect numbers of a certain form*, Arch. Math. (Basel) **21** (1970), 52–53.

Wayne L. McDaniel and P. Hagis Jr., *Some results concerning the non-existence of odd perfect numbers of the form* $p^a M^{2\beta}$, Fibonacci Quart. **13** (1975), 25–28.

E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180, Eng. trans., Izv. Math. **64** (2000), 127–169.

T. Nagell, *Introduction to Number Theory*, Second edition, Chelsea, New York, 1964.

Pace P. Nielsen, *An upper bound for odd perfect numbers*, Integers **3** (2003), #A14.

R. Steuerwald, *Verschärfung einer notwendigen Bedingung für die Existenz einen ungeraden vollkommenen Zahl*, S.-B. Bayer. Akad. Wiss. 1937, 69–72.

M. Waldschmidt, *Minorations de combinaisons linéaires de logarithmes de nombres algébriques*, Canadian J. Math. **45** (1993), 176–224.

K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. für Math. **3** (1882), 265–284.

MANY THANKS FOR YOUR ATTENTION

Tomohiro Yamada
Center for Japanese language and culture
Osaka University
562-8558
8-1-1, Aomatanihigashi, Minoo, Osaka
Japan
e-mail: tyamada1093@gmail.com