Publ. Math. Debrecen
56 / 3-4 (2000), 631–641

Some conjectures in the theory of exponential diophantine equations

By T. N. SHOREY (Mumbai)

Dedicated to Professor K. Győry on his 60th birthday

1. Conjecture on a hyperelliptic equation

For integers $a > 0$, $b > 0$ and $k \neq 0$, we recall Pillai's equation

$$ax^m - by^n = k \tag{1.1}$$

in integers $x > 1,\ y > 1,\ m > 1,\ n > 1$ with $mn \geq 6$.

Pillai [10] conjectured that (1.1) has only finitely many solutions. Now we formulate a conjecture which implies Pillai's Conjecture and a theorem of Schinzel and Tijdeman [12] that for a polynomial with integer coefficients and at least two distinct roots, there are only finitely many perfect powers in its values at integral points. For this, we introduce some notation. Let α be a rational number written as $\frac{a}{b}$ in its reduced form. We define

$$H(\alpha) = \max(|a|, |b|).$$

We observe that

$$H(\alpha^{-1}) = H(\alpha) \quad \text{for} \quad \alpha \neq 0$$

and

$$(H(\alpha))^{-1} \leq |\alpha| \leq H(\alpha) \quad \text{for} \quad \alpha \neq 0. \tag{1.2}$$

Mathematics Subject Classification: 11D61.

Let $f(X)$ be a polynomial of degree n with rational coefficients such that it has at least two distinct roots and $f(0) \neq 0$. Let L be the number of non-zero coefficients of f. For non-zero rational numbers

$$b_1, \ldots, b_L$$

with

$$n_1 > \cdots > n_L, \quad n_1 = n, \ n_L = 0,$$

let

$$f(X) = b_1 X^{n_1} + \cdots + b_{L-1} X^{n_{L-1}} + b_L.$$

Let H be a number satisfying

$$H \geq \max_{1 \leq i \leq L} H(b_i).$$

The right hand side of the above inequality is called the height of f. All the results mentioned in this paper are effective and all the constants appearing in this paper are effectively computable. Now we are ready to state our conjecture.

Conjecture 1.1. *Let $m \geq 2$, and let x and y with $|y| > 1$ be integers satisfying*

$$f(x) = y^m. \tag{1.3}$$

There exists a number C depending only on L and H such that either

$$m \leq C$$

or

$$y^m - f(x) = y^m - b_1 x^{n_1} - \cdots - b_{L-1} x^{n_{L-1}} - b_L$$

has a proper subsum which vanishes.

The assumptions that f has at least two distinct roots and $f(0) \neq 0$ are necessary in Conjecture 1.1. For observing this, we take

$$f(X) = X^m, \qquad f(2) = 2^m \quad \text{for } m = 2, 3, \ldots$$

and

$$f(X) = 4X^{m+1} - 19X^m, \ f(5) = 5^m \quad \text{for } m = 2, 3, \ldots$$

If we consider

$$f(X) = X^m + X - 3, \qquad f(3) = 3^m \quad \text{for } m = 2, 3, \ldots$$

we see that the possibility of the proper subsum vanishing in Conjecture 1.1 is not ruled out. For positive integers μ, ν with $\mu > \nu$ and $\lambda = (\mu^m - \nu^m)^2$, $x = \mu^m + \nu^m$, the polynomial $f(X) = (X^2 - \lambda)/4$ satisfies $f(x) = (\mu\nu)^m$ for $m \geq 2$. Thus the dependence of C on H in the Conjecture is necessary. For an integer $x > 1$, we consider

$$f(X) = (x-1)(X^{m-1} + \cdots + X) + x, \ f(x) = x^m \quad \text{for } m = 3, 4, \ldots$$

in order to observe that the dependence of C on L in the Conjecture is also necessary.

2. Consequences of Conjecture 1.1

Pillai's Conjecture has been confirmed (see [16, Chapter 12]) if at least one of the four variables in (1.1) is fixed. This is also the case if $m = n$ in (1.1). We show

Corollary 2.1. *Conjecture 1.1 implies Pillai's Conjecture.*

Proof. Suppose that (1.1) is satisfied and Conjecture 1.1 is valid. There is no loss of generality in assuming that $\gcd(a, b, k) = 1$. We rewrite (1.1) as

$$y^n = \frac{a}{b}x^m - \frac{k}{b}.$$

Thus we take

$$f(X) = \frac{a}{b}X^m - \frac{k}{b}$$

in Conjecture 1.1. We observe that $f(0) \neq 0$ since k is non-zero and $f(X)$ has at least two distinct roots since $m \geq 2$. Further

$$L = 2, \qquad H = \max(|a|, |b|, |k|)$$

and

$$f(x) = y^n.$$

It is clear that

$$0 = y^n - f(x) = y^n - \frac{a}{b}x^m + \frac{k}{b}$$

has no proper subsum which vanishes. Hence we conclude from Conjecture 1.1 that n is bounded by a number depending only on a, b and k. Similarly, we derive that m is bounded by a number depending only on a, b and k. Now we apply a theorem of BAKER [1] on integral solutions of hyperelliptic equations to (1.1) and we conclude Pillai's Conjecture since $mn \geq 6$. □

As stated in Section 1, SCHINZEL and TIJDEMAN [12] proved

Theorem 2.2. *Let $f(X)$ be a polynomial with rational coefficients and at least two distinct roots. If m, x and y with $m \geq 2$ and $|y| > 1$ are integers satisfying* (1.3)*, then m is bounded by a number depending only on f.*

Corollary 2.3. *Conjecture 1.1 implies Theorem 2.2 unless $f(0) = 0$ and f has at most two distinct roots.*

In fact, we show that Conjecture 1.1 implies that if m, x and y with $m \geq 2$ and $|y| > 1$ are integers satisfying (1.3), then m is bounded by a number depending only on the height of f and the number of non-zero coefficients of f.

PROOF. We assume Conjecture 1.1. First we consider the case that $f(0) \neq 0$. Let m, x and y with $m \geq 2$ and $|y| > 1$ be integers satisfying (1.3). We observe that H depends only on f and $L \leq n = \deg f$. Therefore we see that the constant C appearing in Conjecture 1.1 depends only on f. Further we apply Conjecture 1.1 to suppose that $y^m - f(x)$ has a proper subsum which vanishes. Then we see from (1.3) that its complement is a proper subsum which also vanishes. Thus

$$a_{m_1}x^{m_1} + \cdots + a_{m_t}x^{m_t} = 0,$$

where $m_1 > m_2 > \cdots > m_t$; $a_{m_1}, \ldots, a_{m_t}$ are coefficients of f and $a_{m_1} \cdots a_{m_t} \neq 0$. Then

$$a_{m_1}x^{m_1} = -a_{m_2}x^{m_2} - a_{m_3}x^{m_3} - \cdots - a_{m_t}x^{m_t}.$$

Dividing both the sides by x^{m_1-1}, we have

$$a_{m_1}x = -a_{m_2}x^{-(m_1-m_2)+1} - a_{m_3}x^{-(m_1-m_3)+1} - \cdots$$

Thus we see from (1.2) that

$$|a_{m_1}x| \leq H(1 + \frac{1}{|x|} + \frac{1}{|x|^2} + \cdots) \leq 2H \quad \text{if } |x| > 1.$$

On the other hand, we observe from (1.2) that

$$|a_{m_1}x| \geq H^{-1}|x|.$$

Hence $|x| \leq 2H^2$. Consequently, we see from (1.3) that $|y|^m$ is bounded by a number depending only on f and this is also the case with m since $|y| > 1$.

Next, we turn to the case $f(0) = 0$. Then we may suppose that f has at least two distinct non-zero roots. We write $f(X) = X^r g(X)$ where $g(0) \neq 0$ and g has at least two distinct non-zero roots. Then we see from (1.3) that there exists a polynomial $g_1(X)$ with at least two distinct non-zero roots and with rational coefficients whose heights are bounded by a number depending only on the height of f, such that $g_1(x)$ is an m-th power of a positive integer greater than 1. Now we apply the previous case to complete the proof of Corollary 2.3. □

3. Generalised *a b c* Conjecture and Conjecture 1.1

We state the Generalised a b c Conjecture from Darmon and Granville [4, p. 533].

Generalised *a b c* Conjecture. *Let $N \geq 3$ and $x_1, \ldots, x_N$ be non-zero integers satisfying*

$$x_1 + \cdots + x_N = 0, \quad \gcd(x_1, \ldots, x_N) = 1$$

and let no proper subsum of $x_1 + \cdots + x_N$ vanishes. Then there exist numbers C_1 and C_2 depending only on N such that

$$\max_{1\leq i\leq N} |x_i| \leq C_1 \left(\prod_{p \mid (x_1 \cdots x_N)} p \right)^{C_2}.$$

Corollary 3.1. *The Generalised a b c Conjecture implies Conjecture 1.1.*

Proof. The proof of Corollary 3.1 depends on Theorem 2.2. We denote by $C_3, \ldots, C_7$ numbers depending only on L and H. We suppose (1.3). By Theorem 2.2, we may assume that $n = \deg f \geq C_3$ with C_3 sufficiently large. Further we may suppose that no proper subsum of

$$y^m - f(x) = y^m - b_1 x^{n_1} - \cdots - b_{L-1} x^{n_{L-1}} - b_L = 0$$

vanishes. Now we clear out the denominators of the rational numbers b_i in the above relation and then we divide both sides by the greatest common divisor of the terms. We observe that the greatest common divisor is bounded since a_0 is non-zero. Now we apply the Generalised a b c Conjecture to conclude that

$$|y|^m \leq C_4 \ (|yx|)^{C_5}.$$

Further we see from (1.3) that

$$|x|^n \leq C_6 |y|^m.$$

By taking $C_3 > 2C_5$, we get

$$|x|^{2C_5} \leq |x|^n \leq C_6 |y|^m.$$

Consequently

$$|y|^{m/2} < C_4 C_6^{1/2} |y|^{C_5}$$

which implies that $m \leq C_7$ since $|y| > 1$. This completes the proof of Corollary 3.1. □

4. Problems on an equation of Nagell–Ljunggren

We consider the following equation:

$$\frac{x^m - 1}{x - 1} = y^q \quad \text{in integers } x > 1,\ y > 1,\ m > 2,\ q \geq 2. \tag{4.1}$$

By writing $y^q = (y^{q/p})^p$, there is no loss of generality in assuming that q is prime in (4.1). We observe that

$$\frac{3^5-1}{3-1} = 11^2, \quad \frac{7^4-1}{7-1} = 20^2, \quad \frac{18^3-1}{18-1} = 7^3. \tag{4.2}$$

The initial contributions on (4.1) are due to Nagell–Ljunggren and therefore, we call (4.1) the equation of Nagell–Ljunggren. Ljunggren [8] proved that (4.1) with $q = 2$ has no solution other than the ones given by (4.2). Therefore, we suppose from now on that $q > 2$ in (4.1). Further it follows from the results of Nagell [9] and Ljunggren [8] that (4.1) implies

$$m \equiv 5 \pmod 6 \text{ if } q = 3 \text{ and } 3 \nmid m, \quad 4 \nmid m$$

unless $(x, y, m, q) = (18, 7, 3, 3)$. For a survey on (4.1), we refer to Shorey and Tijdeman [16, Chapter 12] and Shorey [15, Section 4].

Let $\nu > 1$ be an integer. Let $P(\nu)$ denote the greatest prime factor of ν. We write $\omega(\nu)$ and $Q(\nu)$ for the number of distinct prime divisors of ν and the greatest square-free factor of ν, respectively. We recall that $\varphi(\nu)$ is the number of positive integers less than ν and coprime to ν. We start with the following factorisation on (4.1) given by Shorey [13].

Lemma 4.1. *Assume* (4.1). *Let D be a positive divisor of m such that*

$$\gcd(D, m/D) = \gcd(D, \varphi(Q(m/D))) = 1.$$

Then

$$\frac{(x^D)^{m/D}-1}{x^D-1} = y_1^q, \quad \frac{x^D-1}{x-1} = y_2^q$$

for positive integers y_1 and y_2.

Our final aim is to prove on (4.1) the following

Conjecture 4.2. *Equation* (4.1) *has no solution other than the ones given by* (4.2).

A weaker version of Conjecture 4.2 states

Conjecture 4.3. *Equation* (4.1) *has only finitely many solutions.*

Let $m = P_1^{A_1} \cdots P_s^{A_s}$ where $P_1 < \cdots < P_s$ are prime numbers and $A_1, \ldots, A_s$ are positive integers. We apply Lemma 4.1 successively with $D = P_s^{A_s}, \ldots, D = P_2^{A_2}$ to derive

Corollary 4.4. *It suffices to prove Conjecture 4.3 for* $\omega(m) = 1$.

Thus the case $\omega(m) = 1$ is the most difficult part of Conjecture 4.3. But we do not know an answer even to the following simpler question.

Conjecture 4.6. *Equation* (4.1) *with* $\omega(m) \geq 2$ *has only finitely many solutions.*

Another conjecture lying between Conjectures 4.3 and 4.6 states

Conjecture 4.5. *Equation* (4.1) *has only finitely many solutions whenever* x *is a perfect power.*

Conjecture 4.2 implies Conjecture 4.3 which gives Conjecture 4.5. Now we show

Corollary 4.7. *Conjecture 4.5 implies Conjecture 4.6.*

Proof. Assume (4.1) and Conjecture 4.5. Let $m = P_1^{A_1} \cdots P_s^{A_s}$ as above with $s \geq 2$. Then we apply Lemma 4.1 with $D = P_s^{A_s}$ to suppose that $m = 2D$ and

$$x^D + 1 = y_1^q.$$

This is Catalan's equation and Tijdeman [17] proved that it has only finitely many solutions. This completes the proof of Corollary 4.7. □

There has been progress on Conjecture 4.5 recently. Saradha and Shorey [11] confirmed the conjecture when x is a square. In fact they proved that (4.1) has no solution whenever $x = z^2$ with $z \geq 32$ and $z \in \{2, 3, 4, 8, 9, 16, 25, 27\}$. Further Bennett [2] and Bugeaud, Mignotte, Roy and Shorey [3], independently, covered the remaining cases. Thus (4.1) has no solution if x is a square. Further Hirata-Kohno and Shorey [6] confirmed the conjecture when $x = z^\mu$ where μ is a fixed odd prime and $q > 2(\mu - 1)(2\mu - 3)$. By taking $\mu = 3$ in the preceding result, we see that (4.1) with $x = z^3$ and $q \notin \{5, 7, 11\}$ has only finitely many solutions. For a survey of results on Conjecture 4.5, we refer to Shorey [15, Section 4].

5. Results on Conjecture 4.6

A weaker version of Conjecture 4.6, namely that (4.1) with $\omega(m) > q - 2$ has only finitely many solutions, has been given by Shorey [13], [14]. The proof depends on the results of Shorey [13, [14] that (4.1) has only finitely many solutions if either $m \equiv 1 \pmod{q}$ or x is a q-th power. These results have been improved as follows:

Lemma 5.1. *Equation* (4.1) *has no solution whenever* x *is a* q*-th power.*

Lemma 5.2. *Equation* (4.1) *with* $m \equiv 1 \pmod{q}$ *has no solution.*

Lemma 5.1 is due to Le [7] and Lemma 5.2 is an immediate consequence of a theorem of Bennett [2] saying that for a positive integer a, the equation

$$(a+1)x^n - ay^n = 1 \text{ has no solution in integers } x > 1,\ y > 1,\ n \geq 3.$$

We use the above lemmas in the proof of Shorey's result saying that (4.1) with $\omega(m) > q-2$ has only finitely many solutions, to show

Theorem 5.3. *Equation (4.1) with* $\omega(m) > q-2$ *has no solution.*

Proof. Suppose that (4.1) is satisfied. We write

$$m = q^e p_1^{a_1} \cdots p_r^{a_r}$$

where $e \geq 0$, $a_1 > 0, \ldots, a_r > 0$ and $p_1 < p_2 < \cdots < p_r$ are prime numbers different from q. For $1 \leq \mu \leq \nu \leq r$, we put

$$m_{\mu,\nu} = p_\mu^{a_\mu} \cdots p_\nu^{a_\nu}.$$

By repeated application of Lemmas 4.1 and 5.2, we derive that none of $p_1, \ldots, p_r$ is congruent to $1 \pmod{q}$. Then we apply Lemma 4.1 with $D = q^e$ and Lemma 5.1 to conclude that $e = 0$. For $1 \leq \mu \leq \nu \leq r$, we write $D_1 = m_{1,\mu-1}$, $D_2 = m_{\mu,\nu}$ and $D_3 = m_{\nu+1,r}$. We apply Lemma 4.1 with $D = D_3$ and $D = D_2$ to derive that $\frac{X^{D_2}-1}{X-1}$ with $X = x^{D_3}$ is a q-th power. Then we conclude from Lemma 5.2 that none of $m_{\mu,\nu}$ with $1 \leq \mu \leq \nu \leq r$ is congruent to $1 \pmod{q}$. Finally, we consider

$$m_{1,1} = p_1^{a_1},\ m_{1,2} = p_1^{a_1} p_2^{a_2},\ \ldots,\ m_{1,r} = p_1^{a_1} \cdots p_r^{a_r}.$$

We know that none of these is congruent to $0, 1 \pmod{q}$. Further, for $1 \leq \mu < \nu \leq r$ we observe that $m_{1,\mu}$ and $m_{1,\nu}$ are incongruent $\pmod{q}$, otherwise

$$\frac{m_{1,\nu}}{m_{1,\mu}} = m_{\mu+1,\nu} \equiv 1 \pmod{q}.$$

Hence $\omega(m) = r \leq q-2$. This completes the proof of Theorem 5.3. □

Now we consider (4.1) with the additional assumption

$$\gcd(m, \varphi(Q(m)) = 1. \tag{5.1}$$

Erdős [5] gave an asymptotic formula for the number of positive integers satisfying (5.1). Thus there are infinitely many positive integers m satisfying (5.1). The assumption $\omega(m) > q - 2$ in the above results can be relaxed in this case. Shorey [14] showed that (4.1) with (5.1) and

$$2^{\omega(m)} > q - 1 \tag{5.2}$$

has only finitely many solutions. In fact, we have

Theorem 5.4. *Equation* (4.1) *with* (5.1) *and* (5.2) *has no solution.*

The proof depends on Lemmas 4.1, 5.2 and a result of Le [7]. The derivation of Theorem 5.4 from these results is similar to that of Theorem 5.3 from Lemmas 4.1, 5.1, 5.2 and we refer to Shorey [14] for details.

Acknowledgements. I thank N. Saradha, M. Waldschmidt and the referee for comments on an earlier draft of this paper.

References

[1] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444.

[2] M. Bennett, Rational approximation to algebraic numbers of small height: The diophantine equation $|ax^n - by^n| = 1$, *J. reine angew. Math.* (*to appear*).

[3] Y. Bugeaud, M. Mignotte, Y. Roy and T. N. Shorey, The equation $\frac{x^n-1}{x-1} = y^q$ has no solution with x square, *Math. Proc. Camb. Philos. Soc.* **127** (1999), 353–372.

[4] H. Darmon and A. Granville, On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* **27** (1995), 513–543.

[5] P. Erdős, Some asymptotic formulas in Number Theory, *Jour. Indian Math. Soc.* **12** (1948), 75–78.

[6] Noriko Hirata-Kohno and T. N. Shorey, On the equation $(x^m-1)/(x-1) = y^q$ with x power, Analytic number theory (Y. Motohashi, ed.), *Cambridge University Press, Cambridge*; *London Math. Soc. Lecture Note Series* **247** (1997), 343–351.

[7] M. H. Le, A note on the diophantine equation $\frac{x^m-1}{x-1} = y^n$, *Math. Proc. Camb. Philos. Soc.* **116** (1994), 385–389.

[8] W. Ljunggren, Noen Setninger om ubestemte likninger av formen $(x^n - 1)/(x-1) = y^q$, *Norsk. Mat. Tidsskr. 1. Hefte* **25** (1943), 17–20.

[9] T. Nagell, Note sur l'équation indéterminée $(x^n - 1)/(x - 1) = y^q$, *Norsk. Mat. Tidsskr.* **2** (1920), 75–78.

[10] S. S. Pillai, On the equation $2^x - 3^y = 2^X + 3^Y$, *Bull. Calcutta Math. Soc.* **37** (1945), 15–20.

[11] N. Saradha and T. N. Shorey, The equation $\frac{x^n-1}{x-1} = y^q$ with x square, *Math. Proc. Camb. Philos. Soc.* **125** (1999), 1–19.

[12] A. Schinzel and R. Tijdeman, On the equation $y^m = P(x)$, *Acta Arith.* **31** (1976), 199–204.

[13] T. N. Shorey, Perfect powers in values of certain polynomials at integer points, *Math. Proc. Camb. Philos. Soc.* **99** (1986), 195–207.

[14] T. N. Shorey, On the equation $z^q = (x^n - 1)/(x - 1)$, *Indag. Math.* **48** (1986), 345–351.

[15] T. N. Shorey, Exponential diophantine equations involving products of consecutive integers and related equations, Number Theory (R. P. Bambah, V. C. Dumir and R. J. Hans-Grill, eds.), *Hindustan Book Agency*, 1999, 463–495.

[16] T. N. Shorey and R. Tijdeman, Exponential Diophantine equations, Cambridge Tracts in Mathematics **87**, *Cambridge University Press*, *Cambridge*, 1986.

[17] R. Tijdeman, On the equation of Catalan, *Acta Arith.* **29** (1976), 197–209.

T. N. SHOREY
SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
MUMBAI 400 005
INDIA

(Received January 8, 1999; revised June 25, 1999)