The Diophantine equation $x(x+1)\cdots(x+(m-1))+r=y^n$

Yu.F. Bilu & M. Kulkarni (Talence) and B. Sury (Bangalore)

1 Introduction

Erdős and Selfridge [7] proved that a product of consecutive integers can never be a perfect power. That is, the equation $x(x+1)\cdots(x+(m-1))=y^n$ has no solutions in positive integers x,y,m,n with $m,n>1$. A natural problem is to study the equation

$$x(x+1)(x+2)...(x+(m-1))+r=y^n \tag{1}$$

with a *nonzero* integral (or rational) parameter r. M.J. Cohen [6] proved that (1) has finitely many solutions with $m=n$, and Yuan Ping-zhi [13] used the classical theorems of Baker and Schinzel-Tijdeman to show that, with some obvious exceptions, there are at most finitely many solutions with a fixed m. (See Theorem 1.2 below). Some special cases were completely solved by Abe [1] and Alemu [2].

In this paper we use prove that (1) has finitely many solutions (x,y,m,n) when r is not a perfect power.

Theorem 1.1 *Let r be a non-zero rational number which is not a perfect power in $\mathbb{Q}$. Then (1) has at most finitely many solutions (x,y,m,n) satisfying*

$$x,m,n\in\mathbb{Z},\quad y\in\mathbb{Q},\quad m,n>1. \tag{2}$$

Moreover, all the solutions can be explicitly determined.

We deduce Theorem 1.1 from three more particular results, one of which is the above-mentioned result of Yuan. First of all, let us display two infinite series of solutions which occur for two special values of r. For $r=1/4$ we have the solutions

$$x\in\mathbb{Z},\quad y=\pm(x+1/2),\quad m=n=2. \tag{3}$$

For $r=1$ we have infinitely many solutions

$$x\in\mathbb{Z},\quad y=\pm(x^2+3x+1),\quad m=4,\quad n=2. \tag{4}$$

In the following theorem m is fixed, and we solve (1) in x,y,n.

Theorem 1.2 (Yuan) *Let r be a non-zero rational number and $m>1$ an integer.*

1. *Assume that $(m,r)\notin\{(2,1/4),(4,1)\}$. Then (1) has at most finitely many solutions (x,y,n) satisfying*
$$x,n\in\mathbb{Z},\quad y\in\mathbb{Q},\quad n>1, \tag{5}$$
and all the solutions can be explicitly determined.

2. *Assume that $(m,r)=(2,1/4)$ or $(m,r)=(4,1)$. Then, besides the solutions from (3), respectively (4), equation (1) has at most finitely many solutions (x,y,n) satisfying (5), and all these solutions can be explicitly determined.*

Yuan formulates his result in a slightly different (and non-equivalent) form, and his proof is about three pages long. For the convenience of the reader, we give in Section 2 a concise proof of Theorem 1.2, following Yuan's argument with some changes.

Theorem 1.2 implies that n is bounded in terms of m and r. It turns out that, when $r \neq \pm 1$, it is bounded in terms of r only.

Theorem 1.3 *Let r be a rational number distinct from 0 and ± 1. Then there exists an effective constant $C(r)$ with the following property. If (x, y, m, n) is a solution of (1) satisfying (2) then $n \leq C(r)$.*

Now change the roles: n is fixed, m is variable.

Theorem 1.4 *Let r be a non-zero rational number and $n > 1$ an integer. Assume that r is not an n-th power in $\mathbb{Q}$. Then (1) has at most finitely many solutions (x, y, m) satisfying*

$$x, m \in \mathbb{Z}, \quad y \in \mathbb{Q}, \quad m > 1, \tag{6}$$

and all the solutions can be explicitly determined.

In [8] this theorem is extended (non-effectively) to the equation $x(x+1)\cdots(x+(m-1)) = g(y)$, where $g(y)$ is an arbitrary irreducible polynomial.

Theorem 1.1 is an immediate consequence of Theorems 1.3 and 1.4. Indeed, assume that r is not a perfect power. Theorem 1.3 implies that n is effectively bounded in terms of r. In particular, we have finitely many possible n. Theorem 1.4 implies that for each n there are at most finitely many possibilities of (x, y, m). This proves Theorem 1.1.

Remark 1.5 It is interesting to compare (1) with the classical equation of Catalan $x^m - y^n = 1$. This equation has been effectively solved by Tijdeman [12], and recently Mihăilescu [9] (see also [5]) solved it completely. However, much less is known about the equation $x^m - y^n = r$ for $r \neq \pm 1$. Just to the contrary, for equation (1) the case $r = \pm 1$ seems to be the most difficult.

2 Proof of Theorem 1.2

In this section $m > 1$ is an integer and $f_m(x) = x(x+1)\cdots(x+m-1)$.

Proposition 2.1 *Let λ be a complex number. Then the polynomial $f_m(x) - \lambda$ has at least 2 simple roots if $(m, \lambda) \notin \left\{(2, -1/4), \left(3, \frac{\pm 2}{3\sqrt{3}}\right), (4, -1)\right\}$. It has at least three simple roots if $m > 2$ and $(m, \lambda) \notin \left\{\left(3, \pm 4/3\sqrt{3}\right), (4, -1), (4, 9/16), \left(6, 16(10 \pm 7\sqrt{7})/27\right)\right\}$.*

Proof By the Theorem of Rolle, $f_m'(x)$ has $m-1$ distinct real roots. Hence $f_m(x) - \lambda$ may have roots of order at most 2. Beukers, Shorey and Tijdeman [4, Proposition 3.4] proved that for even m at most 2 double roots are possible, and for odd m only one double root may occur. It follows that for $m \notin \{2, 3, 4, 6\}$ the polynomial $f(x) - \lambda$ has at least 3 simple roots.

We are left with $m \in \{2, 3, 4, 6\}$. Since the polynomial $f(x) - \lambda$ has multiple roots if and only if λ is a stationary value of the polynomial $f(x)$ (that is, $\lambda = f(\alpha)$ where α is a root of $f'(x)$), it remains to determine the stationary values of each of the polynomials f_2, f_3, f_4 f_6 and count the simple roots of corresponding translates. The details are routine and we omit them. ■

Corollary 2.2 *Let r be a non-zero rational number. The polynomial $f_m(x) + r$ has at least 2 simple roots if $(m, r) \notin \{(2, 1/4), (4, 1)\}$. It has at least three simple roots if $m > 2$ and $(m, r) \notin \{(4, 1), (4, -9/16)\}$.* ■

We shall use the classical results of Baker [3] and of Schinzel-Tijdeman [10] on the superelliptic equation

$$f(x) = y^n. \tag{7}$$

In Baker's theorem $n \in \mathbb{Z}$ is fixed.

Theorem 2.3 (A. Baker) *Assume that $f(x) \in \mathbb{Q}[x]$ has at least 3 simple roots and $n > 1$, or $f(x)$ has at least 2 simple roots and $n > 2$. Then (7) has only finitely many solutions in $x \in \mathbb{Z}$ and $y \in \mathbb{Q}$, and the solutions can be effectively computed.*

(A non-effective version of this theorem goes back to Siegel [11].)

In the theorem of Schinzel and Tijdeman n becomes a variable.

Theorem 2.4 (Schinzel and Tijdeman) *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial having at least 2 distinct roots. Then there exists an effective constant $N(f)$ such that any solution of (7) in $x, n \in \mathbb{Z}$, $y \in \mathbb{Q}$ satisfies $n \le N(f)$.*

Corollary 2.5 *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial having at least 3 simple roots. Then (7) has at most finitely many solutions in $x, n \in \mathbb{Z}$, $y \in \mathbb{Q}$ satisfying $n > 1$. If $f(x)$ has 2 simple roots then (7) has only finitely many solutions with $n > 2$. In both cases the solutions can be explicitly determined.*

Proof of Theorem 1.2 Corollaries 2.2 and 2.5 imply that the theorem is true if $m > 2$ and $(m, r) \notin \{(4, 1), (4, -9/16)\}$. It remains to consider the cases $m = 2$ and $(m, r) \in \{(4, 1), (4, -9/16)\}$.

Case 1: $\underline{m = 2,\ r \neq 1/4}$ In this case $f_2(x) + r$ has two simple roots, and Corollary 2.5 implies that $f_2(x) + r = y^n$ has at most finitely many solutions with $n > 2$ (and these solutions can be explicitly determined). We are left with the equation $x(x + 1) + r = y^2$, which is equivalent to the equation $(x + 1/2 + y)(x + 1/2 - y) = 1/4 - r$, having finitely many solutions.

Case 2: $\underline{m = 2,\ r = 1/4}$ In this case we have the equation $(x + 1/2)^2 = y^n$. It has infinitely many solutions given by (3) and no other solutions. Indeed, if (x, y, n) is a solution with $n > 2$ then $x + 1/2$ is a perfect power, which is impossible because its denominator is 2.

Case 3: $\underline{m = 4,\ r = 1}$ In this case we have the equation $\left(x^2 + 3x + 1\right)^2 = y^n$. It has infinitely many solutions given by (4) and only finitely many other solutions, all of which can be explicitly determined.

Indeed, let (x, y, n) be a solution with $n > 2$. If n is odd, then y is a perfect square: $y = z^2$ and $x^2 + 3x + 1 = \pm z^n$. Since $x^2 + 3x + 1$ has two simple roots, the latter equation has, by Corollary 2.5, only finitely many solutions with $n \ge 3$.

If $n = 2n_1$ is even then $x^2 + 3x + 1 = \pm y^{n_1}$, which has finitely many solutions with $n_1 \ge 3$. We are left with $n = 4$, in which case $x^2 + 3x + 1 = \pm y^2$. Equation $x^2 + 3x + 1 = y^2$ is equivalent to $(2x + 3 + 2y)(2x + 3 - 2y) = 5$, which has finitely many solutions. Equation $x^2 + 3x + 1 = -y^2$ is equivalent to $(2x + 3)^2 + 4y^2 = 5$, which has finitely many solutions as well.

Case 4: $\underline{m = 4,\ r = -9/16}$ In this case we have the equation $(x + 3/2)^2(x^2 + 3x - 1/4) = y^n$. Since its left-hand side has 2 simple roots, this equation has, by Corollary 2.5, only finitely many solutions with $n > 2$. We are left with the equation $(x + 3/2)^2(x^2 + 3x - 1/4) = y^2$, which is equivalent to the equation $16(x^2 + 3x + 1 - y)(x^2 + 3x + 1 + y) = 25$, having only finitely many solutions.

Theorem 1.2 is proved. ■

3 Proof of Theorems 1.3 and 1.4

Let α be a non-zero rational number and p a prime number. Recall that $\mathrm{ord}_p(\alpha)$ is the integer t such that $p^{-t}\alpha$ is a p-adic unit. The proofs of both theorems rely on the following simple observation.

Proposition 3.1 *Let p be a prime number and $t = \mathrm{ord}_p(r)$. Then for any solution (x, y, m, n) of (1), satisfying (2), one has either $m < (t+1)p$ or $n|t$.*

Proof Assume that $m \geq (t+1)p$. Then $\mathrm{ord}_p\big(x(x+1)(x+2)...(x+(m-1))\big) \geq t+1$. Hence

$$\mathrm{ord}_p\big(x(x+1)(x+2)...(x+(m-1))+r\big) = t,$$

that is, $\mathrm{ord}_p(y^n) = t$, which implies that $n|t$. ■

Proof of Theorem 1.3 Since $r \neq \pm 1$, there exists a prime number p such that $t = \mathrm{ord}_p(r) \neq 0$. Theorem 1.2 implies that for every $m > 1$ there exists an effective constant $N(m)$ such that for any solution of (1) satisfying (2) we have $n \leq N(m)$. Put $C'(r) = \max\{N(m) : 2 \leq m < (t+1)p\}$ if $t > 0$ and $C'(r) = 0$ if $t < 0$. Then $n \leq C'(r)$ when $m < (t+1)p$, and $n \leq |t|$ by Proposition 3.1 when $m \geq (t+1)p$. Thus, in any case $n \leq C(r) := \max\{C'(r), t\}$. ■

Proof of Theorem 1.4 The proof splits into two cases.

Case 1: there is a prime p such that n does not divide $t = \mathrm{ord}_p(r)$ In this case Proposition 3.1 implies that $m \leq (t+1)p$. Also, $(n, r) \notin \{(2, 1/4), (4, 1)\}$, because in both these cases r is an n-th power. Now Theorem 1.2 implies that we may have only finitely many solutions.

Case 2: n is even and $r = -r_1^n$, where $r_1 \in \mathbb{Q}$ Write $z = (y/r_1)^{n/2}$. Let p be prime number congruent to $3 \bmod 4$ and such that $\mathrm{ord}_p(r) = 0$. If $m \geq p$ then

$$\mathrm{ord}_p\left(1+z^2\right) = \mathrm{ord}_p\left(r^{-1}x(x+1)\cdots(x+m-1)\right) > 0,$$

which implies that -1 is a quadratic residue $\bmod\, p$, a contradiction. Thus, $m < p$ and Theorem 1.2 again implies that we may have only finitely many solutions. ■

Acknowledgements We thank Yuan Ping-zhi for informing us about his work. The second-named author thanks A2X, Université Bordeaux I, for its hospitality, and, especially, Prof. Philippe Cassou-Nogues for all his help and encouragement which enabled her to work in the university.

References

[1] N. Abe, On the Diophantine Equation $x(x+1)\cdots(x+n)+1 = y^2$, *Proc. Japan Acad. Ser. A Math. Sci.* **76** (2000), 16–17.

[2] Y. Alemu, On the Diophantine equation $x(x+1)\cdots(x+n) = y^2-1$, *SINET* **18** (1995), 1–22.

[3] A. Baker, Bounds for solutions of hyperelliptic equations, *Proc. Cambridge Phil. Soc.* **65** (1969), 439–444.

[4] F. Beukers, T.N. Shorey, R. Tijdeman, Irreducibility of polynomials and arithmetic progressions with equal product of terms, in *Number Theory in Progress: Proc. Int. Conf. in Number Theory in Honor of A. Schinzel, Zakopane, 1997* (eds. K. Győry, H. Iwaniec, J. Urbanowicz), W. de Gruyter, 1999, pp. 11–26.

[5] Yu.F. Bilu, Catalan's conjecture (after Mihăilescu), Séminaire Bourbaki, Exposé 909, 55ème année (2002-2003); http://www.math.u-bordeaux.fr/~yuri/publ/preprs/catal.pdf .

[6] M. J. Cohen, The difference between the product of n consecutive integers and the nth power of an integer, *Computers and Mathematics with Applications* **39** (2000), no. 11, 139–157.

[7] P. Erdős, J.L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 292–301.

[8] M. Kulkarni, B. Sury, On the Diophantine equation $x(x+1)(x+2)\cdots(x+(m-1))=g(y)$, *Indag. Math.*, to appear.

[9] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, submitted.

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

[11] C.L. Siegel, The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$, *J. London Math. Soc.*, **1** (1926), 66–68; *Ges. Abh.*, Band 1, 207–208.

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

[13] Yuan Ping-zhi, On the special Diophantine equation $a\binom{x}{n} = by^r + c$, *Publ. Math. Debrecen* **44** (1994), 137–143.

Bilu & Kulkarni: A2X, Université Bordeaux 1, 351 cours de la Libération, 33405 Talence, France; e-mail yuri@math.u-bordeaux.fr, manisha@math.u-bordeaux.fr
Sury: Statistics & Mathematics Unit, Indian Statistical Institute, 8th Mile, Mysore Road, Bangalore - 560 059, India; email: sury@isibang.ac.in