Compositio Math. (Page 1 of 6)
doi:10.1112/S0010437X16007569

Rational points on Erdős–Selfridge superelliptic curves

Michael A. Bennett and Samir Siksek

Abstract

Given $k \geqslant 2$, we show that there are at most finitely many rational numbers x and $y \neq 0$ and integers $\ell \geqslant 2$ (with $(k, \ell) \neq (2,2)$) for which

$$x(x+1)\cdots(x+k-1) = y^{\ell}.$$

In particular, if we assume that ℓ is prime, then all such triples (x, y, ℓ) satisfy either $y = 0$ or $\ell < \exp(3^k)$.

1. Introduction

In a remarkable paper of 1975, Erdős and Selfridge [ES75] proved that the product of at least two consecutive positive integers can never be a perfect power. In other words, the Diophantine equation

$$x(x+1)\cdots(x+k-1) = y^{\ell} \tag{1}$$

has no solutions in positive integers x, y, k and ℓ with $k, \ell \geqslant 2$. Their proof, the culmination of more than 40 years of work by Erdős, relied on an ingenious combination of elementary arguments and a lemma on bipartite graphs.

For a fixed pair of positive integers (k, ℓ), equation (1) defines a *superelliptic curve* of genus at least $(\ell-1)(k-2)/2$. In particular, if $\ell + k > 6$, the genus exceeds 1, and by Faltings' theorem [Fal83], the number of rational points (x, y) is finite. Actually quantifying this result, for any given curve, can be an extremely challenging problem.

In the case of *integer* points on superelliptic curves, one can typically prove much stronger statements. In fact, given a polynomial $f(x)$ with integer coefficients having at least two distinct roots, a famous theorem of Schinzel and Tijdeman [ST76] asserts that the integer solutions to the equation $f(x) = y^{\ell}$ satisfy either $y \in \{0, \pm 1\}$ or $\ell \leqslant \ell_0$ for some (effectively computable) constant $\ell_0 = \ell_0(f)$. Analogous absolute bounds upon exponents ℓ for which there exist non-trivial rational points on superelliptic curves are very hard to come by (though conjectured to exist). Indeed, such results for the curves defined by (1), for small fixed values of k, are among the very few in the literature (other results are restricted to polynomials of the shape $f(x) = g(h(x))$, where $g(x) = x^2 + 1$ or $x^3 + 1$ (see Darmon and Merel [DM97]) and to certain families of g of small degree, treated in [BD13]). These curves corresponding to (1) admit a number of obvious rational points, including 'trivial' ones with $y = 0$, and two infinite families:

$$(x, y, k, \ell) = \left(\frac{a^2}{b^2 - a^2}, \frac{ab}{b^2 - a^2}, 2, 2\right), \quad a \neq \pm b, \tag{2}$$

Received 19 October 2015, accepted in final form 7 March 2016.
2010 Mathematics Subject Classification 11D61 (primary), 11D41, 11F80, 11F41 (secondary).
Keywords: superelliptic curves, Galois representations, Frey curve, modularity, level lowering.
The first author is supported by NSERC, while the second author is supported by the EPSRC *LMF: L-Functions and Modular Forms* Programme Grant EP/K034383/1.

and

$$(x, y, k, \ell) = \left(\frac{(1-2j)}{2}, \frac{\pm 1}{2^j} \prod_{i=1}^{j} (2i-1), 2j, 2 \right), \tag{3}$$

where a, b and j are integers with j positive. Two further solutions are given by

$$(x, y, k, \ell) = (-4/3, 2/3, 3, 3) \quad \text{and} \quad (-2/3, -2/3, 3, 3). \tag{4}$$

It may be that there are no other such points and, in particular, none whatsoever with $\ell \geqslant 4$. This is the content of a conjecture of Sander [San99] (with requisite corrections noted in [BBGH06]).

Conjecture (Sander). If $k \geqslant 2$ and $\ell \geqslant 2$ are integers, then the only rational points on the superelliptic curve defined by (1) satisfy either $y = 0$, or are as in (2), (3) or (4), for suitable choices of the parameters a, b and j.

Sander [San99] proved this conjecture for $2 \leqslant k \leqslant 4$ and, together with Lakhal [LS03], treated the case $k = 5$. The conjecture was subsequently established for $2 \leqslant k \leqslant 11$ by the first author *et al.* [BBGH06] (see also [GHS04]) and for $2 \leqslant k \leqslant 34$ by Győry *et al.* [GHP09].

In this short note, we will treat the case of arbitrary k. While we are not able to prove the above conjecture in its entirety, we establish the following partial result.

Theorem 1. *Let $k \geqslant 2$ be a positive integer. Then (1) has at most finitely many solutions in rational numbers x and y, and integers $\ell \geqslant 2$, with $(k, \ell) \neq (2, 2)$ and $y \neq 0$. If we assume that ℓ is prime, all such solutions satisfy $\ell < \exp(3^k)$.*

The reader will note that solutions (3) and (4) do satisfy the bound $\ell < \exp(3^k)$. As far as the authors are aware, Theorem 1 is the first example of a rational analogue to the Schinzel–Tijdeman theorem to be proved for a superelliptic curve $f(x) = y^\ell$, where the polynomial f has arbitrarily high degree and does not arise via composition from a polynomial of small degree.

2. A ternary equation of signature (ℓ, ℓ, ℓ)

Lemma 2.1. *Let $k \geqslant 2$ be an integer and $\ell > k$ be prime. Suppose the superelliptic curve (1) has an (affine) rational point (x, y) with $y \neq 0$. Let $k/2 < p \leqslant k$ be prime. Then there are non-zero integers a, b, c, u, v, w satisfying*

$$au^\ell + bv^\ell + cw^\ell = 0 \tag{5}$$

such that:

(i) *the integers a, b and c are ℓth power free;*
(ii) *every prime divisor of abc is at most k;*
(iii) *$p \nmid abc$;*
(iv) *p divides precisely one of u, v, w.*

Proof. We write $x = n/s$ and $y = m/t$ where $m \neq 0$, the denominators s, t are positive integers and $\gcd(n, s) = \gcd(m, t) = 1$. From (1), we have

$$\frac{n(n+s)(n+2s)\cdots(n+(k-1)s)}{s^k} = \frac{m^\ell}{t^\ell}.$$

Our coprimality assumptions thus ensure that $s^k = t^\ell$. As ℓ and k are coprime, there is a positive integer d such that $s = d^\ell$ and $t = d^k$. We are thus led to consider the equation

$$n(n+d^\ell)(n+2d^\ell)\cdots(n+(k-1)d^\ell) = m^\ell, \tag{6}$$

where now all our variables are integers. We write, for each $i \in \{0, 1, \dots, k-1\}$,

$$n + id^\ell = a_i z_i^\ell, \tag{7}$$

where a_i is an ℓth power free integer. Since the greatest common divisor of $n + id^\ell$ and $n + jd^\ell$ divides $(i-j)$, each a_i thus has the property that its prime divisors are bounded above by k.

Our argument relies on the basic fact that, given k consecutive terms in arithmetic progression, each prime up to k necessarily divides either one of the terms or the modulus of the progression. Fix a prime p with $k/2 < p \leqslant k$.

Suppose first that $p \mid d$. Then $p \nmid m$ and thus $p \nmid a_i z_i$ for all i. From (7) we have

$$d^\ell + a_0 z_0^\ell - a_1 z_1^\ell = 0;$$

the proof of the lemma is complete in this case with $a = 1$, $b = a_0$, $c = -a_1$, $u = d$, $v = z_0$, $w = z_1$.

We may thus suppose $p \nmid d$. This fact, combined with the inequality $p \leqslant k$, therefore forces p to divide $n + id^\ell$ for some $0 \leqslant i \leqslant k-1$. Suppose first that p does not divide any other factor on the left-hand side of (6). Thus $p \nmid a_j z_j$ for $j \neq i$. Moreover, $\mathrm{ord}_p(a_i z_i^\ell) = \mathrm{ord}_p(n + id^\ell) = \mathrm{ord}_p(m^\ell)$ and so $p \nmid a_i$ and $p \mid z_i$ (as a_i is ℓth power free). By (7) we have

$$\begin{aligned} a_i z_i^\ell - a_{i+1} z_{i+1}^\ell + d^\ell &= 0 \quad \text{if } i < k-1, \\ a_i z_i^\ell - a_{i-1} z_{i-1}^\ell - d^\ell &= 0 \quad \text{if } i = k-1, \end{aligned}$$

completing the proof in this case.

It remains to consider the case where p divides at least two factors of the left-hand side of (6). In fact, as $p > k/2$ and $p \nmid d$, precisely two factors are divisible by p and these have the form $n + id^\ell$ and $n + (i+p)d^\ell$. Thus $\mathrm{ord}_p((n+id^\ell)(n+(i+p)d^\ell)) = \mathrm{ord}_p(m^\ell)$. We shall make use of the identity

$$(n+(i+p)d^\ell)(n+id^\ell) - (n+(i+p-1)d^\ell)(n+(i+1)d^\ell) + (p-1)d^{2\ell} = 0.$$

Substituting from (7) completes the proof. □

3. Proof of Theorem 1

We now turn to the proof of Theorem 1. By previous work outlined in the introduction, we may suppose that $k \geqslant 35$. We shall suppose that $\ell > k$ is prime. Fix a prime $k/2 < p \leqslant k$ and suppose that (1) has a rational solution (x, y) with $y \neq 0$. By Lemma 2.1, there are non-zero integers a, b, c, u, v, w satisfying (5) and conditions (i)–(iv). By removing the greatest common factor, we may suppose that the three terms in (5) are coprime without affecting conditions (i)–(iv). After permuting the three terms and changing signs if necessary, we may suppose further that

$$au^\ell \equiv -1 \pmod 4, \quad bv^\ell \equiv 0 \pmod 2.$$

Let E be the Frey elliptic curve

$$E \;:\; Y^2 = X(X - au^\ell)(X + bv^\ell).$$

Write $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The action of $G_{\mathbb{Q}}$ on the ℓ-torsion of E gives rise to a representation

$$\overline{\rho}_{E,\ell} \,:\, G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell).$$

As $\ell > k \geqslant 35$ and E has full 2-torsion, we know by Mazur [Maz78] that $\overline{\rho}_{E,\ell}$ is irreducible. By the work of Kraus [Kra97] (which appeals to modularity [BCDT01] and Ribet's level lowering [Rib90]) the representation $\overline{\rho}_{E,\ell}$ arises from a newform f of weight 2 and level N', where

$$N' = 2^r \,\mathrm{Rad}_2(abc);$$

here $r \leqslant 5$ and $\mathrm{Rad}_2(n)$ denotes the product of the distinct odd primes dividing n. By (ii) and (iii) of Lemma 2.1 we find that

$$N' \mid 2^4 \cdot \prod_{q \leqslant k, q \neq p} q, \tag{8}$$

where the product is over prime q. We appeal to the following standard result (see, for example, [Sik12, Proposition 5.1]).

Lemma 3.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and $f = q + \sum_{i \geqslant 2} c_i q^i$ be a newform of weight 2 and level $N' \mid N$. Write $K = \mathbb{Q}(c_1, c_2, \dots)$ for the totally real number field generated by the Fourier coefficients of f. If $\overline{\rho}_{E,\ell}$ arises from f then there is some prime ideal $\lambda \mid \ell$ of K such that for all primes q,*

- *if $q \nmid \ell N N'$ then $a_q(E) \equiv c_q \pmod{\lambda}$;*
- *if $q \nmid \ell N'$ and $q \parallel N$ then $q + 1 \equiv \pm c_q \pmod{\lambda}$.*

Note that $\ell > k \geqslant p$ and so $\ell \neq p$. Moreover, from (8) we have $p \nmid N'$. Conclusion (iv) in Lemma 2.1 ensures that E has multiplicative reduction at p and so $p \parallel N$. We apply Lemma 3.1 with $q = p$. Thus ℓ divides $\mathrm{Norm}_{K/\mathbb{Q}}(p + 1 \pm c_p)$. As c_p (in any of the real embeddings of K) is bounded by $2\sqrt{p}$, this quantity is non-zero and hence provides an upper bound upon ℓ:

$$\ell \leqslant (p + 1 + 2\sqrt{p})^{[K:\mathbb{Q}]} = (\sqrt{p} + 1)^{2[K:\mathbb{Q}]}.$$

It remains to establish that $\log \ell < 3^k$. The degree $[K : \mathbb{Q}]$ is bounded by $g_0^+(N')$ which denotes the dimension of the space of cuspidal newforms of weight 2 and level N'. From Martin [Mar05], we have

$$g_0^+(N') \leqslant \frac{N'+1}{12}.$$

Thus

$$\log \ell \leqslant \frac{N'+1}{6} \log\left(\sqrt{p} + 1\right).$$

By Schoenfeld [Sch76],

$$\sum_{\substack{q \leqslant k \\ q \text{ prime}}} \log q < 1.000\,081 k.$$

Finally, a routine computation making use of (8) and our assumption $17 < k/2 \leqslant p \leqslant k$ allows us to conclude that $\log \ell < 3^k$.

4. Concluding remark

It is worth observing that our arguments employed to prove Theorem 1 actually enable us to reach a like conclusion for curves of the shape

$$x(x+1)\cdots(x+k-1) = by^{\ell},$$

where b is any integer with the property that its prime factors do not exceed $k/2$.

References

BBGH06 M. A. Bennett, N. B. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, Proc. Lond. Math. Soc. (3) **92** (2006), 273–306.

BD13 M. A. Bennett and S. Dahmen, *Klein forms and the generalized superelliptic equation*, Ann. of Math. (2) **177** (2013), 171–239.

BCDT01 C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

DM97 H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

ES75 P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292–301.

Fal83 G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpen*, Invent. Math. **73** (1983), 349–366.

GHP09 K. Győry, L. Hajdu and Á. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression*, Compositio Math. **145** (2009), 845–864.

GHS04 K. Győry, L. Hajdu and N. Saradha, *On the diophantine equation $n(n+d)\cdots n+(k-1d) = by^l$*, Canad. Math. Bull. **47** (2004), 373–388.

Kra97 A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), 1139–1161.

LS03 M. Lakhal and J. W. Sander, *Rational points on the superelliptic Erdős–Selfridge curve of fifth degree*, Mathematika **50** (2003), 113–124.

Mar05 G. Martin, *Dimensions of the spaces of cuspforms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$*, J. Number Theory **112** (2005), 298–331.

Maz78 B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

Rib90 K. Ribet, *On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Invent. Math. **100** (1990), 431–476.

San99 J. W. Sander, *Rational points on a class of superelliptic curves*, J. Lond. Math. Soc. (2) **59** (1999), 422–434.

ST76 A. Schinzel and R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. **XXXI** (1976), 199–204.

Sch76 L. Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$ II*, Math. Comp. **30** (1976), 337–360.

Sik12 S. Siksek, *The modular approach to Diophantine equations*, in *Explicit Methods in Number Theory: Rational Points and Diophantine Equations*, Panoramas et Syntheses, vol. 36, eds K. Belabas, F. Beukers, P. Gaudry, W. McCallum, B. Poonen, S. Siksek, M. Stoll and M. Watkins (Société Mathématique de France, Paris, 2012), 151–179.

Michael A. Bennett bennett@math.ubc.ca
Department of Mathematics, University of British Columbia,
Vancouver, BC, Canada V6T 1Z2

Samir Siksek S.Siksek@warwick.ac.uk
Mathematics Institute, University of Warwick,
Coventry CV4 7AL, UK