C. R. Math. Rep. Acad. Sci. Canada Vol. **27**, (4), 2005 pp. 105–110

ON k-TH POWER NUMERICAL CENTRES

PATRICK INGRAM

Presented by David Boyd, FRSC

RÉSUMÉ. On dit qu'un entier N est un centre numérique de puissance k pour n si

$$1^k + 2^k + \cdots + N^k = N^k + (N+1)^k + \cdots + n^k.$$

En utilisant des minorations explicites de formes linéaires de logarithmes elliptiques, on démontre qu'il n'y a aucun centre numérique non trivial de puissance 5, et on montre qu'il y a qu'un nombre fini des paires (N, n) qui satisfont l'équation précèdente pour $k > 1$. Le problème de trouver des centres de puissance k pour $k = 1, 2, 3$ est traité dans [7].

We will call an integer N a k-th power numerical centre for n if

$$1^k + 2^k + \cdots + N^k = N^k + (N+1)^k + \cdots + n^k. \tag{1}$$

This equation is trivial in the case $k = 0$, while the solutions to the problem in the case $k = 1$ correspond to the solutions of the Pell equation $X^2 - 2Y^2 = 1$, with $X = 2n + 1$, $Y = 2N$. In [5] and [9] the cases with $k = 2, 3$ were treated, and it was shown that the only solutions to (1) were the trivial ones, *i.e.*, those with $(N, n) \in \{(0, 0), (1, 1)\}$. We will prove the following:

PROPOSITION. *For fixed $k > 1$, equation* (1) *has only finitely many solutions. In particular, for $k = 5$ there are only the trivial solutions.*

Equation (1) is, of course, equivalent to

$$S_k(N) + S_k(N-1) = S_k(n),$$

where

$$S_k(x) = 1^k + 2^k + \cdots + x^k.$$

For k even the above curves are smooth and so have genus $\frac{1}{2}k(k-1)$ by a straightforward application of a theorem of Hurwitz (see [7, p. 41]). When k is odd, the above admits the change of variables $x = (2n+1)^2$, $y = (2N)^2$ and the resulting curves are smooth in x and y of degree $\frac{k+1}{2}$, and so have genus $\frac{1}{8}(k-1)(k-3)$. The general claim, then, follows from the celebrated result

Received by the editors on July 8, 2005; revised September 15, 2005.

Many thanks are due to the author's thesis supervisor, Michael A. Bennett. Thanks are also due to Nils Bruin for his help with the hyperelliptic case and to the referee for several useful suggestions.

AMS subject classification: 11D25, 11J89.

Keywords: numerical centres, house problem, linear forms in elliptic logarithms.

of Faltings [4]. For a more direct proof we apply results of Bilu and Tichy [1] on the number of solutions to the Diophantine equation $f(x) = g(y)$. More specifically, we apply a refinement of this by Rakaczki [6] which applies just in case $f(x) = S_k(x)$.

For the result in the case $k = 5$, we apply the results of David [3], as presented in [11] (see also [10] and [12]). The problem of finding all integral points on the curve (1) in the case $k = 5$ reduces to that of locating all integral points on a certain non-Weierstrass model of an elliptic curve. As it turns out, integer points with sufficiently large naïve height on this model correspond to rational points on a Weierstrass model abnormally close to a particular K-rational point, for some cubic extension $K/\mathbb{Q}$. Using David's explicit lower bounds on linear forms in elliptic logarithms one may thence obtain a bound on the heights of these points.

We also note how one might go about finding all solutions to (1) in the case $k = 4$, although the required computations are daunting.

Proof of the general claim. If $g_k(x) := S_k(x) + S_k(x-1) = S_k(y)$ has infinitely many solutions then g_k takes one of the forms presented in [6], and we will preserve the case numbering found in that paper. We note that Cases VI and VII in this list require $k = 3$, which is a case dealt with by [9]. We note also that Case V is a special case of Case II. As noted in [6], if k is odd then $S_k(x) = \psi_k\big((x+1/2)^2\big)$, for some polynomial ψ_k, clearly of degree $\frac{k+1}{2}$.

Case I. $g_k(x) = S_k\big(q(x)\big)$, where $q(x) \in \mathbb{Q}[x]$ is non-constant. Clearly in this case $\deg(q) = 1$, and so $q(x) = \mu x + \lambda$, $\mu, \lambda \in \mathbb{Q}$. As the leading coefficient of $S_k(x)$ is $\frac{1}{k+1}$, we have

$$S_k\big(q(x)\big) = \frac{\mu^{k+1}}{k+1}x^{k+1} + \cdots .$$

On the other hand, the leading coefficient of $g_k(x)$ is $\frac{2}{k+1}$, and so $\mu^{k+1} = 2$, implying $k = 0$.

Case II. k is odd and $g_k(x) = \psi_k\big(\delta(x)q(x)^2\big)$, with $\delta(x), q(x) \in \mathbb{Q}[x]$, δ linear. Here we see, by comparing degrees, that δ is constant and q linear. Again, the leading coefficient of ψ_k is $\frac{1}{k+1}$, and so the leading coefficient of $\psi\big(\delta q(x)^2\big)$ is $\frac{(\delta\mu^2)^{\frac{k+1}{2}}}{k+1}$, where $q(x) = \mu x + \lambda$, $\delta(x) = \delta$. We have then $(\delta\mu^2)^{\frac{k+1}{2}} = 2$, implying $k \leq 1$.

Case III. k is odd and $g_k(x) = \psi_k\big(c\delta(x)^t\big)$, where δ is linear, $c \in \mathbb{Q} \setminus \{0\}$, and $t \geq 3$ is an odd integer. This is impossible as then $\deg(g_k) = t(\frac{k+1}{2}) > k+1$.

Case VI. k is odd and $g_k(x) = \psi_k\big(\big(a\delta(x)^2 + b\big)q(x)^2\big)$ where $a, b \in \mathbb{Q} \setminus \{0\}$ and δ, q are as above. This case, once degrees are compared, reduces to our analysis of Case II.

Proof of the specific claim. It now remains to deal with the case where $k = 5$. This will be resolved using lower bounds on linear forms in elliptic logarithms, as per [3] and [11]. For the solution of the general cubic elliptic diophantine equation see also [10].

In the case $k = 5$, the change of variables $x = (2n+1)^2$, $y = (2N)^2$ yields the elliptic curve

$$x^3 - 5x^2 + 7x - 3 = 2y^3 + 20y^2 - 16y.$$

Note that we are passing from a curve with only finitely many rational points to one with (it turns out) infinitely many. This is, in fact, an improvement of the situation as there are much better tools for finding integer points on a curve like this than for finding the rational points on a genus eight curve. We will, however, find it more convenient to deal with the following model, obtained by a shift of one in the x-coordinate, which clearly preserves integrality of points:

$$f(t, v) = t^3 - 2t^2 - 2v^3 - 20v^2 + 16v = 0. \tag{2}$$

The transformation

$$X = \frac{-4t - 3v + 8}{v}$$
$$Y = -2\Big(\frac{4t^2 - 4t + 10v^2 - t^3 + 2v^3}{v^2}\Big)$$

yields a minimal Weierstrass model for (2), specifically

$$E : Y^2 = X^3 - X^2 - 41X + 441. \tag{3}$$

Our method of proof, following [11], will be to bound some linear form in elliptic logarithms from above, and then from below using the explicit bounds of [3]. We will identify points on the various models of the elliptic curve.

Claim 1. *On the curve in* (3),

$$-8.025 \leq \hat{h}(P) - h(P) \leq 7.072.$$

Proof. These are the height bounds presented in [8], although it is worth noting that we are using the definition of height found in [7], which differs from that found in [8] by a factor of two. ∎

Claim 2. *The Mordell–Weil group of $E/\mathbb{Q}$ is generated by the points $T = (-9, 0)$ and $P_0 = (1, 20)$, the former having order two, and the latter having infinite order.*

PROOF. Noting that 7 and 37 are primes of good reduction for E, and that $\#E(\mathbb{F}_7) = 8$ and $\#E(\mathbb{F}_{37}) = 46$, we see instantly that the order of torsion for $E/\mathbb{Q}$ divides two. A descent shows that the curve has rank at most one. The two points above demonstrate the sharpness of this, and all that remains is to establish that $(1, 20)$ is indivisible. Suppose that $(1, 20) = nR$ or $nR + T$ for some $R \in E(\mathbb{Q})$ and $n \geq 2$. Then one sees, through basic computation and height bounds, that $h(R) \leq 17.26$, and of course R must be an integer point. Thus $X(R)$ is an integer of modulus at most 3.13×10^7, and a search of all such points confirms our claim. ∎

The following claim is a simple computation, performed in PARI/GP.

CLAIM 3. *The only solutions to* (2) *with* $|t|, |v| \leq 10^4$ *are*

$$(t, v) \in \{(0, 0), (2, 0), (8, -8), (8, -6), (8, 4)\}.$$

CLAIM 4. *Let* $P = (t, v) = mP_0 + jT$ *be an integer point on* (2) *with* $|t|, |v| \geq 10^4$. *Then*

$$\frac{1}{|v|} \leq \exp(9.157 - 0.31m^2).$$

PROOF. Our first order of business is to bound $h\big(X(P)\big)$ in terms of $|v|$. By examining (2) we see that the condition that $|t|, |v|$ are large implies that P lies quite close to the asymptote $T = \alpha V + \beta$, where α is the real cube root of 2, and $\beta = \frac{10\alpha+2}{3}$. In particular, for $|v| \geq 10^4$, $|t - (\alpha v + \beta)| < 0.002$. As t and v are integers, we have

$$\begin{aligned} \hat{h}(P) - 7.072 \leq h\big(X(P)\big) &\leq \log \max\{|8 - 4t - 3v|, |v|\} \\ &\leq \log \max\{8 + (4\alpha + 3)v + 4\beta + 0.008, |v|\} \\ &\leq \log |(4\alpha + 3.003)v| \leq \log |v| + 2.085. \end{aligned}$$

From this we conclude that

$$-\log |v| \leq 9.157 - \hat{h}(P) \leq 9.157 - 0.31m^2.$$

∎

Let Q_0 be the limit point of points on (3) arising from the asymptote of (2), *i.e.*, $X(Q_0) = -4\alpha - 3$. We wish to translate the above into an upper bound on the difference between the elliptic logarithms of Q_0 and P. Note that as Q_0 is defined only over $K = \mathbb{Q}(\alpha)$, we must consider elliptic logs over a number field. First note that

$$\hat{h}(Q_0) \leq 10$$

and

$$\begin{aligned} |u(Q_0)| &= 1.52086\ldots, \\ |u(P_0)| &= 1.11199\ldots, \end{aligned}$$

where, as Section 4 of [11], u denotes the elliptic logarithm. We set

$$\mathcal{L} = u(P) - u(Q_0).$$

Claim 5.

$$|\mathcal{L}| \leq \frac{1}{4|v|}.$$

Proof. As in [11], we note that

$$|\mathcal{L}| = \left| \int_{v(P)}^{\infty} \frac{dv}{\partial f/\partial t} \right|.$$

One may verify that $|\partial f/\partial t| \geq 4v^2$ for $|v| \geq 10^4$, from which the above bound follows. ∎

Now we have

$$u(P) = mu(P_0) + ju(T) + m_0\omega,$$

where m_0 is chosen to specify the branch of the log and where $j \in \{0, 1\}$, so

$$|\mathcal{L}| = \left| mu(P) - u(Q_0) + (2m_0 + j)\frac{\omega}{2} \right| \leq \exp(7.771 - 0.31m^2).$$

Note that (see [11]) $m_0 \leq 2m + 1$, and so if M is the largest coefficient in the linear form, $M \leq 4m + 3$.

It remains to determine a lower bound on $|\mathcal{L}|$. In the notation of [3] we have $D = 3$, $\beta_0 = 0$, $\beta_1 = m$, $\beta_2 = -1$, $\beta_3 = 2m_0 + j$. We will be considering $u_1 = u(P_0)$, $u_2 = u(Q_0)$, $u_3 = u(T)$. So $\gamma_1 = P_0$, $\gamma_2 = Q_0$, $\gamma_3 = T$. The conditions on $B, \hat{E}, V_1, \ldots, V_3$ become (note, our $\hat{E}$ is David's E)

$$3\log(B) \geq \log(V_1) \geq \log(V_2) \geq \log(V_3)$$

$$\log(B) \geq \max\{37.425, 4m + 3\}$$

$$\log(V_1) \geq \max\{13.76769, 5.7114\}$$

$$\log(V_2) \geq \max\{13.76769, 10.6837\}$$

$$\log(V_3) \geq 13.76769$$

$$e \leq \hat{E} \leq 5.344$$

which is obtained by making sharp the inequalities for the V_i, $\hat{E} = 5.344$, $B = 4m + 3$ (at least for $m \geq 9$). This yields

$$\log|\mathcal{L}| \geq 2.891 \times 10^{75}\big(\log(B) + 2.7747\big)\big(\log\log(B) + 16.5424\big)^4.$$

Combining we obtain the absolute bound

$$|m| \leq 10^{42}.$$

Applying the LLL algorithm in a fashion similar to that in Section 5 of [11] we may reduce this bound to 27 at which point the result is easily verified using PARI. One notes that the only integer points on the original curve corresponding to points $nP+jT$ with $|n| \leq 27$ are the points $\mathcal{O}, T, P+T, 2P, -P$, corresponding to the points in Claim 3. The only integer points on the original curve arising from these are $(0,0)$ and $(1,1)$.

REMARK 1. In the case $k = 4$, one may, by performing the change of variables

$$x = \frac{2n+1}{N}$$

$$y = \frac{48n^5 + 120n^4 + 100n^3 + 30n^2 - 1 - 96N^5 - 80N^3}{N^3},$$

reduce the problem of finding rational points on the (in this case genus six) curve defined by (1) to that of finding rational points on the hyperelliptic curve

$$y^2 = x^6 - 24x^5 + 400x^3 + 336x + 7936.$$

Unfortunately, this curve is not ideal for treating with the methods of Chabauty; the sextic above has Galois group S_6, and the method consequently requires computing the Mordell–Weil groups of elliptic curves over number fields of degree 45.

REFERENCES

1. Yu. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*. Acta Arith. **95** (2000), 261–288.
2. N. Bruin, *Chabauty methods using elliptic curves.* J. Reine Angew. Math. **562** (2003), 27–49.
3. S. David, *Minorations de formes linéaires de logarithmes elliptiques.* Mém. Soc. Math. France (N.S.) **62**, 1995.
4. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), 349–366.
5. R. Finkelstein, *The house problem.* Amer. Math. Monthly **72** (1965), 1082–1088.
6. Cs. Rakaczki, *On the diophantine equation $S_m(x) = g(y)$*. Publ. Math. Debrecen **65** (2004), 439–460.
7. J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Math. **106**, Springer–Verlag, New York, 1986.
8. ———, *The difference between the Weil height and the canonical height on elliptic curves.* Math. Comp. **55** (1990), 723–743.
9. R. Steiner, *On k-th-power numerical centers.* Fibonacci Quart. **16** (1978), 470–471.
10. R. J. Stroeker and B. M. M. de Weger, *Solving elliptic Diophantine equations: the general cubic case.* Acta Arith. **87** (1999), 339–365.
11. R. J. Stroeker and N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms.* Acta Arith. **67** (1994), 177–196.
12. ———, *Computing all integer solutions of a genus 1 equation.* Math. Comp. **72** (2003), 1917–1933.

Department of Mathematics
University of British Columbia
Vancouver, British Columbia
V6T 1Z4
email: pingram@math.ubc.ca