

Dept. of Mathematics
Harvard University
Cambridge, MA 02138

May 24, 1988

Prof. Don Zagier
Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße
D-5300 Bonn 3
Federal Republic of Germany

Dear Prof. Zagier,

I have read with considerable pleasure your note on “Large integral points on elliptic curves”, which Prof. Gross showed me in response to a question. In the second part of that note you define a “measure of impressiveness”, ρ , of a large integral point (x, y) on the elliptic curve $x^3 + ax + b = y^2$ by

$$\rho = \log(x) / \log(\max(|a|^{\frac{1}{2}}, |b|^{\frac{1}{3}}))$$

and exhibit several infinite families of such points for which $\rho = 9 + O(\frac{1}{\log x})$. You conjectured, though, that ρ could be as large as 10, so I searched for an infinite family confirming this. What I found was an infinite family of Pell type for which $\rho = 12 - O(\frac{1}{\log x})$. The implied constant is quite large—bigger than 200—so ρ approaches 12 very slowly, remaining below $5\frac{1}{2}$ for x in the range $[1, 10^8]$ of Odlyzko’s computation, and first exceeding 10 and 11 for x of 51 and 107 digits respectively.

In your note you give a probabilistic heuristic suggesting that ρ should never significantly exceed 10. But a naïve counting of parameters and constraints for a Pell-type family

$$X^3(t) + A(t)X(t) + B(t) = Q(t)Y^2(t) \tag{1}$$

(in which A, B are polynomials of low degree, Q is a quadratic polynomial in t , and X, Y are polynomials of large degree) suggests that (1) should have several solutions with $\rho \rightarrow 12$, most simply with A constant, B linear, X quartic and Y quintic. Actually finding such a solution required a longish MACSYMA session to solve four nonlinear equations in four variables, which surprisingly have a unique nontrivial solution, (necessarily) defined over \mathbf{Q} : up to rescaling t and the polynomials A, B, Q, X, Y , the only solution to (1) is

$$\begin{aligned}
A &= 33, \quad B = -18(8t - 1), \quad Q = 9t^2 - 10t + 3, \\
X &= 324t^4 - 360t^3 + 216t^2 - 84t + 15, \\
Y &= 36(54t^5 - 60t^4 + 45t^3 - 21t^2 + 6t - 1).
\end{aligned} \tag{2}$$

As it stands, (2) seems of little use because Q is never a square for $t \in \mathbf{Z}$. However, we may rescale (2) by replacing (A, B, X) by $(4A = 132, 8B, 2X)$, which yields an integral point provided $2Q$ is a square. That Pell-type condition is satisfied by $t = 1$ and thus by infinitely many t , yielding an infinite family of solutions (b, x, y) to $x^3 + 132x + b = y^2$ with $x \sim 2^{-25}3^{-4}b^4$. The small factor $2^{-25}3^{-4} \doteq 3.68 \cdot 10^{-10}$ means that, although ρ eventually approaches 12, the first few admissible values of t yield only mediocre ρ : the second such value, $t = 15$, when $b = -17424$ and $x = 35334750$ (the largest such x to fall within the bounds of Odlyzko's search), produces only $\rho \doteq 5.34$ and was probably ignored; only the ninth value $t = 812111750209$ produces $\rho > 10$, and only the eighteenth, $t = -48926085100653611109021839$, reaches $\rho > 11$.

Some final remarks: Prof. Lang tells me that Vojta's conjectures imply the $\rho \leq 10 + \epsilon$ conjecture *except possibly for a finite number of exceptional families* such as those obtained by rescaling (2). Vojta proves this implication in a yet unpublished paper, but leaves open the existence of exceptional families. It's interesting to compare this situation with the similar conjecture of Hall concerning $|x^3 - y^2|$, where the best infinite families known come from the identity

$$(t^2 + 10t + 5)^3 - (t^2 + 22t + 125)(t^2 + 4t - 1)^2 = 1728t \tag{3}$$

(Exer. 9.10 in Silverman's *The Arithmetic of Elliptic Curves*, attributed to Danilov, *Math. Notes Acad. Sci. USSR* **32** (1982), 617–8), which yields Pell-type solutions with ρ tending this time to the “correct” value of 6. There is a natural reason (which Danilov does not mention in his article) for (3) to be defined over \mathbf{Q} : the fifth modular curve $(j(z), j(5z))$ is rationally parametrized by

$$j(z) = f(t) = \frac{(t^2 + 10t + 5)^3}{t}, \quad j(5z) = f\left(\frac{1}{t}\right),$$

and $f(t)$ is a sixth-degree rational function with a fifth-order pole at infinity (a cusp), two third-order zeros (CM by $\frac{1}{2}(1 + \sqrt{-3})$) and two second-order values of 1728 (CM by $\sqrt{-1} = i$; the appearance of $z = \frac{1}{5}(i \pm 2)$ when $j(z) = j(5z) = 1728$ splits the other two inverse images of 1728 under f)—hence (3). I have no similar rationale for (2), nor for why it gives “too large” a value of ρ .

Sincerely,

Noam D. Elkies