JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Mark WATKINS

A note on integral points on elliptic curves

Tome 18, n° 3 (2006), p. 707-720.

<http://jtnb.cedram.org/item?id=JTNB_2006__18_3_707_0>

Journal de Théorie des Nombres
de Bordeaux **18** (2006), 707-720

A note on integral points on elliptic curves

par Mark WATKINS

Résumé. À la suite de Zagier et Elkies, nous recherchons de grands points entiers sur des courbes elliptiques. En écrivant une solution polynomiale générique et en égalisant des coefficients, nous obtenons quatre cas extrémaux susceptibles d'avoir des solutions non dégénérées. Chacun de ces cas conduit à un système d'équations polynomiales, le premier ayant été résolu par Elkies en 1988 en utilisant les résultants de Macsyma ; il admet une unique solution rationnelle non dégénérée. Pour le deuxième cas nous avons constaté que les résultants ou les bases de Gröbner sont peu efficaces. Suivant une suggestion d'Elkies, nous avons alors utilisé une itération de Newton p-adique multidimensionnelle et découvert une solution non dégénérée, quoique sur un corps de nombres quartique. En raison de notre méthodologie, nous avons peu d'espoir de montrer qu'il n'y a aucune autre solution. Pour le troisième cas nous avons trouvé une solution sur un corps de degré 9, mais n'avons pu traiter le quatrième cas. Nous concluons par quelques commentaires et une annexe d'Elkies concernant ses calculs et sa correspondance avec Zagier.

Abstract. We investigate a problem considered by Zagier and Elkies, of finding large integral points on elliptic curves. By writing down a generic polynomial solution and equating coefficients, we are led to suspect four extremal cases that still might have nondegenerate solutions. Each of these cases gives rise to a polynomial system of equations, the first being solved by Elkies in 1988 using the resultant methods of Macsyma, with there being a unique rational nondegenerate solution. For the second case we found that resultants and/or Gröbner bases were not very efficacious. Instead, at the suggestion of Elkies, we used multidimensional p-adic Newton iteration, and were able to find a nondegenerate solution, albeit over a quartic number field. Due to our methodology, we do not have much hope of proving that there are no other solutions. For the third case we found a solution in a nonic number field, but we were unable to make much progress with the fourth case. We make a few concluding comments and include an appendix from Elkies regarding his calculations and correspondence with Zagier.

Manuscrit reçu le 1er décembre 2005.

1. Introduction

Let E be an elliptic curve given by the model $y^2 = x^3 + Ax + B$, and suppose that (X, Y) is an integral point on this model. How large can X be in terms of $|A|$ and $|B|$? One measure of the impressiveness of the size of an integral point is given by the quotient $\rho = \log(X)/\log(\max(|A|^{1/2}, |B|^{1/3}))$, which, as Zagier [13] indicates, can be interpreted as saying that X is of the order of magnitude of the ρth power of the roots of the cubic polynomial $x^3 + Ax + B$.

Lang [9] makes the conjecture that ρ is bounded, and notes (see [13]) that he and Stark worked out that generically $\rho \leq 10 + o(1)$ via probablistic heuristics, though a construction of Stark indicated that in similar situations there might be finitely many exceptional parametric families with larger ρ. Vojta [12] has related this conjecture to his more general Diophantine theory, where again these exceptional families cannot be eliminated. In 1987, Zagier [13] gave a construction that gives infinitely many curves with $\rho \geq 9 - o(1)$, and listed some impressive examples from numerical calculations of Odlyzko.

In a letter to Zagier in 1988, Elkies constructed infinitely many examples that satisfy $\rho \geq 12 - o(1)$. His construction is polynomial-based, and reduces to solving a system of polynomial equations formed from equating coefficients. There are exactly four choices of parameters that both yield $\rho = 12 - o(1)$ and for which there is a reasonable hope that a solution might exist. The first of these was the case worked out by Elkies. This already led to a system of 4 polynomial equations in 4 variables, which Elkies notes took a longish session of MACSYMA [10] to solve. The second choice of parameters immediately (via linear substitution) leads to a system of 6 equations and unknowns; even though computers have gained much in speed over the last 15 years, the resulting system is still too difficult to solve via Gröbner bases or resultants. We eliminated one variable from the system via another linear substitution (though this creates denominators), and then another via a resultant step. This gives us a rather complicated system of four equations and unknowns; the degrees of the polynomials were sufficiently large that, again, Gröbner bases and resultants were not of much use. We then proceeded to try to find solutions via a multidimensional p-adic iterative Newton method. We found one such solution over a quartic number field; it is an inherent problem with this method that we have little hope of proving that we have found all the solutions. With the third choice

of parameters, we found a solution in a nonic number field, and with the fourth case we made little progress.

As an appendix, we include some calculations of Elkies regarding the first case, and his 1988 letter to Zagier.

2. Families of Pell type

First we review the construction of Elkies. Consider the equation

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

where $A, B, Q, X, Y \in \bar{\mathbf{Q}}(t)$ are polynomials in some number field K and we have $\deg Q = 2$. Given a polynomial solution to (1), via scaling we can make all the polynomials K-integral. The theory of the Pell equation implies that if the quadratic polynomial $Q(t)$ is a square for one integral t-value, then it is square for infinitely many integral t, and thus we get infinitely many curves $y^2 = x^3 + A(t)x + B(t)$ with K-integral points $(X(t), Y(t)\sqrt{Q(t)})$.

Let a, b, q, x, y be the degrees of these polynomials respectively. We wish for $\rho = x/\max(a/2, b/3)$ to be as large as possible. If we do a parameter count, we get that there are $(a + b + q + x + y) + 5$ coefficients of our polynomials. The total degree of our equation is $3x = q + 2y$, so we get $3x + 1$ equations. When $3x + 1 \le a + b + q + x + y + 5$, we might expect there to be a solution. However, we first need to remove the effect of the action of the group $\mathrm{PGL}_2(\bar{\mathbf{Q}})$ on our choice of coefficients.

Letting $l(P)$ be the leading coefficient of a polynomial P, we first scale t by $l(X)/l(Y)$ and then multiply through $l(Y)^x/l(X)^y$, so as to make X, Y, Q all monic. Then we translate so as to eliminate the t^{y-1} term in Y. Then we effect $t \to 1/t$ and multiply (X, Y, Q, A, B) by $(t^x, t^y, t^2, t^{2x}, t^{3x})$, and then scale so as to make[1] the t-coefficient of X be equal to 1. Finally we undo the $t \to 1/t$ transformation in the same manner. So we are left with $(a + 1) + (b + 1) + q + (x - 1) + (y - 1)$ coefficients, while we also lose one condition, namely that the leading coefficients match. Thus we want to have $a+b+q+x+y \ge 3x$ with $\rho = x/\max(a/2, b/3)$ as large as possible, and this turns out to be 12. We get 4 different possibilities, namely $(a, b, q, x, y) = (0, 1, 2, 4, 5), (1, 1, 2, 6, 8), (1, 2, 2, 8, 11), (2, 3, 2, 12, 17)$. For instance, for the first case we have the polynomials

$$X(t) = t^4 + t^3 + x_2t^2 + x_1t + x_0, \quad Y(t) = t^5 + y_3t^3 + y_2t^2 + y_1t + y_0,$$
$$Q(t) = t^2 + q_1t + q_0, \quad A(t) = a_0, \quad B(t) = b_1t + b_0,$$

and equating the t^0-t^{11} coefficients gives us 12 equations in these 12 unknowns. Fortunately, simple linear substitutions easily reduce this to 4

[1] We could alternatively equate two coefficients, or set the linear coefficient of Q equal to 1; we found that fixing the linear coefficient of X to be 1 was best amongst the various choices. In this scaling, we assume the coefficient is nonzero; the alternative case can be handled separately.

equations and unknowns; we give one such reduced set, in order to indicate the complexity of the equations.

$$12x_0x_2-12x_0q_0+60x_0+6x_1^2-24x_1x_2+48x_1q_0-156x_1-x_2^3-3x_2^2q_0+27x_2^2+9x_2q_0^2-174x_2q_0+$$
$$+417x_2-5q_0^3+171q_0^2-939q_0+1339=0,$$

$$4x_0x_1+4x_0x_2+4x_0q_0+8x_0+2x_1^2-x_1x_2^2-2x_1x_2q_0-6x_1x_2+3x_1q_0^2-10x_1q_0-17x_1+2x_2^2q_0+5x_2^2-$$
$$-12x_2q_0^2+26x_2q_0+38x_2+10q_0^3-71q_0^2+80q_0+83=0,$$

$$120x_0x_1x_2-72x_0x_1q_0+312x_0x_1-60x_0x_2^2+216x_0x_2q_0-576x_0x_2-60x_0q_0^2+336x_0q_0-516x_0+$$
$$+32x_1^3-168x_1^2x_2+288x_1^2q_0-936x_1^2-18x_1x_2^3-54x_1x_2^2q_0+342x_1x_2^2+114x_1x_2q_0^2-1836x_1x_2q_0+$$
$$+4146x_1x_2-42x_1q_0^3+1302x_1q_0^2-6870x_1q_0+9642x_1+9x_2^4+72x_2^3q_0-234x_2^3-342x_2^2q_0^2+2658x_2^2q_0-$$
$$-4488x_2^2+336x_2q_0^3-4518x_2q_0^2+17004x_2q_0-19446x_2-75q_0^4+1486q_0^3-9036q_0^2+22098q_0=19041,$$

$$48x_0^2x_2-48x_0^2q_0+240x_0^2+64x_0x_1^2-128x_0x_1x_2+288x_0x_1q_0-768x_0x_1-40x_0x_2^3+24x_0x_2^2q_0-$$
$$-72x_0x_2^2+40x_0x_2q_0^2-816x_0x_2q_0+1864x_0x_2-24x_0q_0^3+792x_0q_0^2-4232x_0q_0+5928x_0-28x_1^2x_2^2-$$
$$-24x_1^2x_2q_0+24x_1^2x_2+36x_1^2q_0^2-312x_1^2q_0+420x_1^2+84x_1x_2^3-84x_1x_2^2q_0+388x_1x_2^2-244x_1x_2q_0^2+$$
$$+1480x_1x_2q_0-1876x_1x_2+180x_1q_0^3-2028x_1q_0^2+6428x_1q_0-6180x_1+3x_2^5+9x_2^4q_0-84x_2^4-26x_2^3q_0^2+$$
$$+480x_2^3q_0-1186x_2^3+10x_2^2q_0^3-224x_2^2q_0^2+1310x_2^2q_0-2140x_2^2+7x_2q_0^4-464x_2q_0^3+4210x_2q_0^2-$$
$$-12472x_2q_0+11807x_2-3q_0^5+228q_0^4-2942q_0^3+14284q_0^2-29791q_0+22560=0.$$

If we are willing to accept variables in denominators, we can go one step more and eliminate x_0 from one of the first three equations. A system like this was solved by Elkies in 1988 using MACSYMA which uses resultants; solving it is almost instantaneous[2] with MAGMA today, using either Gröbner bases or resultants. We get an isolated solution and also two (extraneous) positive-dimensional solution varieties (which correspond to points on the singular plane cubic curve):

$$(x_0,x_1,x_2,q_0) =(\tfrac{1}{192}[16u^2-200u-239],\tfrac{1}{8}[4u-1],u,\tfrac{9}{4}),$$
$$(u,-2v+3,v-5,v),(\tfrac{311}{64},\tfrac{61}{8},\tfrac{9}{2},\tfrac{11}{4}).$$

From the isolated point, via back-substitution we get

$$(y_0,y_1,y_2,y_3,q_1,a_0,b_0,b_1)=(\tfrac{715}{64},\tfrac{165}{16},\tfrac{77}{16},\tfrac{55}{8},3,\tfrac{216513}{4096},-\tfrac{3720087}{131072},\tfrac{531441}{8192}).$$

To derive the solution in the form given by Elkies, we first want to eliminate denominators, and we also wish to minimise the value of A that occurs at the end (that is, get rid of spurious powers of 2 and 3). This can

[2]That is, provided one deals with the multivariate polynomial rings properly and works over the rationals/integers at the desired times.

be done by replacing t by $1-9t/2$ and then multiplying (X,Y,Q,A,B) by $(s,-4s/3,9s/16,s^2,s^3)$ where $s=128/81$. This gives us

$$\begin{aligned}
X(t) &= 6(108t^4-120t^3+72t^2-28t+5),\\
Y(t) &= 72(54t^5-60t^4+45t^3-21t^2+6t-1),\\
Q(t) &= 2(9t^2-10t+3),\ A(t)=132,\ B(t)=-144(8t-1).
\end{aligned}$$

Note that $Q(1)=2^2$, so that there are infinitely many integral values of t for which $Q(t)$ is square. As noted by Elkies, we have that $X(t)\sim B(t)^4/2^{25}3^4$, so that small values of t do not give very impressive values of ρ.

2.1. The second case. We next consider the second case $\mathrm{EPZ}_{\mathrm{II}}$ of the Elkies-Pell-Zagier equation (1), where $(a,b,q,x,y)=(1,1,2,6,8)$. After making rational transformations, we are left with 18 equations in 18 unknowns, which reduce to 6 upon making linear substitutions. We can reduce to 5 via allowing denominators,[3] and then eliminate one more variable via resultants, but at this point, we are left with equations with too large of degrees for resultants or Gröbner bases to be of much use. Parts of two of the four equations appear below (the whole input file is about 500 kilobytes)

$$2101324894157987694q_0^{14}+10712927385148776768 0x_2^2x_3^2x_4^2q_0^5+\cdots=0,$$

$$\begin{aligned}
&3297090088072371384445122582 3q_0^{22}-\\
&\quad -3432844129581767991329518803 1488x_2^2x_3^2x_4^7q_0^6+\cdots=0.
\end{aligned}$$

We denote this reduced system of equations by R_{II}.

It was suggested to us by Elkies that it might be possible to find a solution via multidimensional p-adic Newton iteration.[4] In general, this method is most useful when we are searching for zero-dimensional solution varieties in a small number of variables. Writing $\vec{f}$ as our system of equations, we take a p-adic approximate solution $\vec{s}$ and replace it by $\vec{s}-J(\vec{s})^{-1}\vec{f}(\vec{s})$, where $J(\vec{s})$ is the Jacobian matrix of partial derivatives for our system evaluated at $\vec{s}$. Since the convergence is quadratic, it is not difficult to get p-adic solutions to high precision. From each liftable local solution mod p we thus obtain a solution modulo a large power of p, and then use standard lattice reduction techniques [4, §2.7.2] to try to recognise it as a rational or algebraic number.

[3] This linear substitution is probably most efficiently done via resultants, as else the denominators will cause problems for some computer algebra systems.

[4] This technique appears in [5], while J. Wetherell tells us that he has used it to find torsion points on abelian varieties. In [5], the lifting step was done via computing derivatives numerically, while we chose to compute them symbolically. Uses of this technique in situations close to those that occur here will be described in [6]. Wooley gives [7, Prop. 5.20] as a theoretical reference.

First we tried the primes $p = 2, 3$, but we found no useful mod p solutions; all the local solutions had a noninvertible Jacobian matrix.[5] Furthermore, since a solution to $\mathrm{R_{II}}$ might very well have coordinates whose denominators have powers of 2 and 3, not finding a solution was not too surprising. With $p = 5$ we again found some (probable) positive-dimensional families and three other solutions, of which two had an invertible Jacobian modulo 5. However, these solutions to $\mathrm{R_{II}}$ failed to survive the undoing of the resultant step, and thus do not actually correspond to a solution to $\mathrm{EPZ_{II}}$. We found the same occurrence for $p = 7, 11, 13$ — there were various $\mathbf{Q}_p$ solutions to our reduced system, but these did not lift back to the original system.

With $p = 17$ our luck was better, as here we found a solution in the dihedral quartic number field K defined[6] by $z^4 - 2z^3 - 4z^2 + 5z - 2$, whose discriminant is $-3^2 11^3$. Letting θ be a root of this polynomial, the raw form of our solution is

$$\begin{aligned} x_2 &= \tfrac{1}{2430000}(90699840\theta^3 + 66428384\theta^2 + 19934816\theta - 283298787),\\ x_3 &= \tfrac{1}{6750}(20240\theta^3 + 70576\theta^2 - 121616\theta - 441839),\\ x_4 &= \tfrac{1}{900}(-5808\theta^3 - 7568\theta^2 + 33968\theta + 23959),\\ q_0 &= \tfrac{1}{2700}(2576\theta^3 + 3760\theta^2 - 8720\theta + 10971). \end{aligned}$$

After undoing the resultant step the rest is but substitution and we readily get a solution to $\mathrm{EPZ_{II}}$, albeit, in a quartic number field. Note that 17 is the smallest[7] odd unramified prime which has a degree 1 factor in K.

We next introduce some notation before stating our result; we have infinitely many Pell equations from which to choose, and so only present the simplest one that we were able to obtain. Let

$$p_2 = \theta, \quad q_2 = \theta - 1, \quad r_2 = \theta^2 - \theta - 5, \quad \text{and} \quad p_3 = 2\theta^2 - 2\theta + 1$$

be the primes above 2 and the ramified prime above 3, and

$$\eta_1 = \theta^3 + \theta^2 - 2\theta + 1 \quad \text{and} \quad \eta_2 = \theta^3 - 3\theta + 1$$

be fundamental units, so that we have $p_2 q_2 r_2 = 2$ and $p_3^2 = 3\eta_1^2\eta_2^{-1}$. Let $\beta = 2\theta^3 + 2\theta^2 - 6\theta - 3$ (this is of norm 3271), and with

$$Q(t) = c_2 t^2 + c_1 t + c_0 = 3p_2^7 q_2 \beta \eta_1^2 \eta_2^{-1} t^2 + 2q_2^3 \eta_1^2 \beta(\theta^3 - \theta^2 + 11)t + q_2^2 \beta^2 \eta_2^2$$

we have
$$\begin{aligned} A(t) = &-12q_2^4 r_2 p_3 \beta^2 \eta_1 \eta_2^{-3}(\theta^3 - \theta + 1)t - \\ &- q_2^2 p_3 \beta^2 \eta_1^{-1} \eta_2^{-2}(\theta^3 - \theta + 1)(9\theta^3 - 2\theta^2 + 5\theta + 9), \end{aligned}$$

[5]Many of them had a Jacobian equal to the zero matrix, and these we expect to come from positive-dimensional solution varieties.

[6]David Brown (Berkeley) indicated to us that this number field can also be obtained by evaluating the 11th modular polynomial at $(x, 0)$; that is $\Phi_{11}(x, 0) = f^3$ where f also defines K.

[7]Due to our method of division of labour we actually first found the solution mod 29. Since we do not know K ahead of time, we have little choice but to try all small primes.

$$X(t) = 2^4 3^4 p_2^5 q_2^7 \beta \eta_1^8 \eta_2^{-4} t^6 + 2^3 3^4 q_2^5 r_2 \beta \eta_1^9 \eta_2^{-4}(17\theta^3 + 2\theta^2 - 71\theta + 33)t^5 +$$
$$+ 2^2 3^3 q_2 \beta \eta_1^8 \eta_2^{-3}(1463\theta^3 - 2436\theta^2 - 2667\theta + 1903)t^4 +$$
$$+ 24 q_2 \beta \eta_1^6 \eta_2^{-2}(25901\theta^3 + 32060\theta^2 - 52457\theta + 15455)t^3 +$$
$$+ 12 q_2^2 p_3 \beta \eta_1^3 (40374\theta^3 + 47422\theta^2 - 61976\theta + 37707)t^2 +$$
$$+ 2 q_2^2 r_2^2 p_3 \beta \eta_1^3 \eta_2 (7081\theta^3 - 854\theta^2 + 90791\theta - 23035)t +$$
$$+ q_2 \beta \eta_1 \eta_2^2 (190035\theta^3 + 199008\theta^2 - 174189\theta + 50449),$$

and

$$B(t) = -6 q_2^7 r_2^2 \beta^3 \eta_1 \eta_2^{-4}(2\theta - 1)^4 t -$$
$$- q_2^4 r_2 \beta^3 \eta_1^{-1} \eta_2^{-3}(2\theta - 1)^4 (4\theta^3 + 18\theta^2 - 16\theta + 1).$$

With the above definition of $c_2 = 3 p_2^7 q_2 \beta \eta_1^2 \eta_2^{-1}$, we have that

$$f_1 = p_2^{-1} q_2 p_3^{-1} \eta_1^{-3} \eta_2 (\theta^3 + 2\theta^2 - \theta + 1)\sqrt{c_2} + r_2 \eta_1^{-1} \eta_2 (3\theta^3 - 19\theta^2 + 20\theta - 5),$$
$$f_2 = 2^2 p_2^4 p_3^{-1} \eta_1^{-1} \eta_2^{-1} \sqrt{c_2} + \eta_1 \eta_2^{-1}(19\theta^3 - 51\theta^2 + 38\theta - 5),$$

and

$$f_3 = p_2 q_2^2 \eta_1^{-4} \eta_2^3 (6\theta^2 - 2\theta + 1)\sqrt{c_2} + r_2 \eta_1 \eta_2 (19\theta^3 - 14\theta^2 - 71\theta - 41)$$

are units of relative norm 1 in $K(\sqrt{c_2})$. Again from the above definitions we have $\sqrt{c_0} = \pm q_2 \beta \eta_2 = \pm(49\theta^3 + 41\theta^2 - 77\theta + 33)$, and so we solve the Pell equation and obtain square values of $Q(t)$ by taking

$$t = 2\sqrt{c_0} uv + v^2 c_1 \quad \text{where} \quad f_1^i f_2^j f_3^k = u + v\sqrt{c_2}$$

for integers i, j, k. We can make t integral via various congruence restrictions on (i, j, k); however, note that p_2 divides all but the constant coefficients of our polynomials (including Y), and so we still get integral solutions to $\mathrm{EPZ_{II}}$ even when p_2 exactly divides the denominator of t. Similarly, the only nonconstant coefficient that p_3 fails to divide is the linear coefficient of Q; since p_3^3 divides $Y(t)$, this nuisance evaporates when we consider solutions to $\mathrm{EPZ_{II}}$. As $t \to \infty$ the norm of the ratio $X(t)/A(t)^6$ tends to $1/2^{56}3^{20}17^6 3271^{11}$; we do not know if this is as large as possible.

We are fairly certain that there are no more nondegenerate algebraic solutions to $\mathrm{EPZ_{II}}$, but have no proof of this. For the small primes,[8] we can identify every local solution to $\mathrm{R_{II}}$ that has invertible Jacobian as algebraic. In addition to the above quartic solution, there are five such solutions[9] having degrees 13, 17, 19, 22, and 22, each with maximal Galois group.

[8] It takes about 1 minute to find local solutions mod 17, and thus $p = 97$ takes about a day.

[9] Since the local images of these solutions to $\mathrm{R_{II}}$ failed to survive the undoing of the resultant step modulo p, this determination of their algebraicity is unnecessary as evidence toward our claim that $\mathrm{EPZ_{II}}$ has no more solutions, but might be interesting in that it shows the splitting of a large-dimensional algebra into many smaller fields.

2.2. The third case. We next discuss whether we expect to be able to find a solution for the third set of parameters $(a,b,q,x,y) = (1,2,2,8,11)$. Analogous to before, via linear substitutions and a resultant step, we should be able to get down to about 6 equations and unknowns, and we call the resulting system $\mathrm{R}_{\mathrm{III}}$. This already is not the most pleasant computational task, but only needs be done once (it takes about 15 minutes). It takes time proportional to p^6 to check all the local solutions, so we can't take p too much above 20. The size of the minimal polynomial of a prospective solution does not matter much due to the quadratic convergence of the Newton method, but the degree of the field of the solution has a reasonable impact. We cannot expect to check fields of degree more than 30 or so. We need p to have a degree 1 factor, but by the Chebotarev density theorem we can predict that this should happen often enough (even for a high degree field) so that some prime less than 20 should work.

With these considerations in mind, we checked the $\mathrm{R}_{\mathrm{III}}$ system for local solutions for all primes $p < 20$ and with $p = 19$ we found[10] a local solution that lifted to a global $\mathrm{EPZ}_{\mathrm{III}}$ solution in the nonic number field given[11] by $z^9 - 2z^8 - 6z^7 + 8z^6 - 7z^5 + 18z^4 + 44z^3 + 32z^2 + 24z + 24$, which has discriminant $-2^{10}3^7 5^5 11^4$. For reasons of space, we do not record the solution here.[12] For $\mathrm{EPZ}_{\mathrm{IV}}$ we were unable to use resultants to reduce beyond 13 variables and did not attempt to find local solutions, even with $p = 5$. If the system had reduced down to 10 variables (as would be hoped from analogy with the above), we could probably check $p = 5$ and maybe $p = 7$.

3. Concluding comments

Note that the above four choices of (a,b,q,x,y) are members of infinite families for which each member has a reasonable possibility of having infinitely many solutions with $\rho > 10$. Indeed, by taking

$$(a,b,q,x,y) = (2m, 3m, 2, 10m+2, 15m+2) \qquad \rho = 10 + 2/m$$

$$(a,b,q,x,y) = (2m, 3m+1, 2, 10m+4, 15m+5) \qquad \rho = \frac{10m+4}{m+1/3}$$

$$(a,b,q,x,y) = (2m+1, 3m+1, 2, 10m+6, 15m+8) \qquad \rho = \frac{10m+6}{m+1/2}$$

$$(a,b,q,x,y) = (2m+1, 3m+2, 2, 10m+8, 15m+11) \qquad \rho = \frac{10m+8}{m+2/3}$$

[10] For $p = 13, 17$ the reduction of the global solution intersected a degenerate solution variety.

[11] This model was obtained with `polredabs` of PARI/GP using partial reduction (possibly using a suborder of the maximal order); `OptimisedRepresentation` in MAGMA was too slow.

[12] One model is given modulo 19 by $X(t) = t^8+t^7+6t^6+16t^5+8t^3+4t^2+12$, $Q(t) = t^2+3t+13$, $A(t) = 16t+15$, $B(t) = 17t^2+6t+14$, and the reader can verify this lifts to a $\mathbf{Q}_{19}$-solution with coefficients $x_8, x_7, q_2 = 1$ and $y_{10} = 0$, with precision $19^{2^{10}}$ sufficient to identify it algebraically.

in each case we have, since $a + b + q + x + y = 3x$, the same number of equations and unknowns, with the value of $\rho = x/\max(a/2, b/3)$ as indicated. However, we might also suspect that the fields of definition of these putative solutions become quite large; thus there is no contradiction with Lang's conjecture, which is only stated for a fixed ground field.

We can also note that with $(a, b, q, x, y) = (2, 3, 2, 10, 14)$ we can expect there to be a nondegenerate 1-dimensional solution variety V with $\rho = 10$. This presumably could be found by a variant of the above methodology, perhaps by taking specialisations to 0-dimensional varieties and finding points on these, and then using this information to reconstruct V. We have not been able to make this work in practise; although the specialised system can be reduced to 7 equations and unknowns and we can find a liftable solution mod 5, it appears that the process of specialisation increases the degree of the field of the solution beyond our computational threshold.

3.1. Performance of computer algebra systems. For our computations we used both PARI/GP [11] and MAGMA [1]. In the end, we were able to do all the relevant computations[13] using only MAGMA (V2.12-9), but this was not apparent at the beginning. The main difficulty with MAGMA was dealing with multivariate polynomial rings, especially as we eliminated variables — if we did not also decrease the dimension of the ambient ring, we could experience slowdown. We also found it to be important to work over the integers rather than rationals as much as possible,[14] as else the continual gcd-computations to eliminate denominators could swamp the calculation. The availability of multivariate gcd's in MAGMA frequently allowed us to reduce the resulting systems by eliminating a common factor. We found MAGMA much superior than PARI/GP in searching for local solutions.[15] MAGMA did quite well in obtaining algebraic numbers from p-adic approximations; after discussions with the maintainer of PARI/GP, we were able to get `algdep` to work sufficiently well to obtain the above solutions. The lifting step[16] was noticeably slower in MAGMA than in PARI/GP, but as we noted above, the time to do this is not the bottleneck.

3.2. Acknowledgements. Thanks are due to Karim Belabas, Nils Bruin, Noam Elkies, and Allan Steel for comments regarding this work. The author was partially funded by an NSF VIGRE Postdoctoral Fellowship at

[13]Our MAGMA input files are available from `www.maths.bris.ac.uk/~mamjw`

[14]Except in the (simple) cases where we were able to use the Gröbner basis machinery; there we want to be working over the rationals rather than the integers.

[15]For R_{II}, MAGMA took about 5 minutes to find all solutions mod 23, and with R_{III} it took 19 hours to find all solutions mod 19 — the bulk of the time is actually in computing the determinant of the Jacobian matrix to see if the solution lifts; we could ameliorate this partially by (say) not computing the whole Jacobian matrix when the first row is zero.

[16]We did not attempt to use secant-based methods (e.g., Broyden [3]) or those of Brent [2].

The Pennsylvania State University, the MAGMA Computer Algebra Group at the University of Sydney, and EPSRC grant GR/T00658/01 during the time in which this work was done.

References

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language.* In *Computational algebra and number theory* Proceedings of the 1st MAGMA Conference held at Queen Mary and Westfield College, London, August 23–27, 1993. Edited by J. Cannon and D. Holt, Elsevier Science B.V., Amsterdam (1997), 235–265. Cross-referenced as J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Online at `http://magma.maths.usyd.edu.au`

[2] R. P. Brent, *Algorithms for Minimization Without Derivatives.* Prentice-Hall, Englewood Cliffs, NJ, 1973.

[3] C. G. Broyden, *A Class of Methods for Solving Nonlinear Simultaneous Equations.* Math. Comp. **19** (1965), 577–593.

[4] H. Cohen, *A course in computational algebraic number theory.* Graduate Texts in Mathematics, 138. Springer-Verlag, New York, 1993.

[5] N. D. Elkies, *Shimura curves for level-3 subgroups of the (2,3,7) triangle group, and some other examples.* To appear in ANTS-VII proceedings, online at `http://arxiv.org/math.NT/0409020`

[6] N. D. Elkies, M. Watkins, *Polynomial and Fermat-Pell families that attain the Davenport-Mason bound.* In progress.

[7] M. J. Greenberg *Lectures on forms in many variables.* W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[8] M. Hall Jr., *The Diophantine equation* $x^3 - y^2 = k$. In *Computers in number theory*, Proceedings of the Science Research Council Atlas Symposium No. 2 held at Oxford, from 18–23 August 1969. Edited by A. O. L. Atkin and B. J. Birch. Academic Press, London-New York (1971), 173–198.

[9] S. Lang, *Conjectured Diophantine estimates on elliptic curves.* In *Arithmetic and geometry. Vol. I.,* edited by M. Artin and J. Tate, Progr. Math., **35**, Birkhäuser Boston, Boston, MA (1983), 155–171.

[10] Macsyma, a sophisticated computer algebra system. See `http://maxima.sourceforge.net` for history and current version of its descendants.

[11] PARI/GP, CVS development version `2.2.11`, Université Bordeaux I, Bordeaux, France, June 2005. Online at `http://pari.math.u-bordeaux.fr`

[12] P. Vojta, *Diophantine approximations and value distribution theory.* Lecture Notes in Mathematics, 1239. Springer-Verlag, Berlin, 1987. x+132 pp.

[13] D. Zagier, *Large Integral Points on Elliptic Curves,* and addendum. Math. Comp. **48** (1987), no. 177, 425–436, **51** (1988), no. 183, 375.

Appendix by Noam D. Elkies (Harvard University)

I. Calculations for the First Case

We compute polynomials $X, A, B, Q, Y \in \mathbf{C}(t)$ of degrees $4, 0, 1, 2, 5$, satisfying

$$X^3 + AX + B = QY^2. \tag{2}$$

Without loss of generality, we take $X, A, B, Q, Y \in \bar{\mathbf{Q}}(t)$. We may normalize X, Y to be monic, and translate t so $Q = t^2 - c$. Since (2) has degenerate solutions with $(X, A, B, Y) = (Q(t + b_1)^2, 0, 0, Q(t + b_1)^3)$, we write

$$X = Q((t + b_1)^2 + 2b_2) + 2b_3 t + 2b_4 \tag{3}$$

for some scalars b_1, b_2, b_3, b_4. Because $AX + B = O(t^5)$ at $t = \infty$, we have $Y = (X^3/Q)^{1/2} + O(t^{-2})$, which determines Y and imposes two conditions on b_1, b_2, b_3, b_4, c. Considered as equations in b_4, c, these conditions are simultaneous linear equations, which we solve to obtain

$$b_4 = \frac{b_2^2}{6b_3}(3b_3 - 2b_1b_2), \quad c = \frac{(b_3 - b_1b_2)(3b_3^2 - 3b_1b_2b_3 + 2b_2^3)}{3b_2^2b_3}. \tag{4}$$

Then A is the t^4 coefficient of $QY^2 - X^3$; we compute

$$A = \frac{3b_3^2}{b_2^2}(b_3 - b_1b_2)^2 + \frac{b_2^2}{3b_3^2}(6b_1b_3^3 + 2b_2^2b_3^2 - 6b_1^2b_2b_3^2 - 2b_1b_2^3b_3 + b_1^2b_2^4). \tag{5}$$

The identity (2) then holds if the t^3 and t^2 coefficients of $X^3 + AX - QY^2$ vanish. Writing these coefficients in terms of b_1, b_2, b_3, we find that they share a factor $b_3 - b_1b_2$ that we already encountered in our formula (4) for c. Namely, the t^3 and t^2 coefficients are

$$(b_3 - b_1b_2)\frac{6b_3^3 - 6b_1b_2b_3^2 + 6b_2^3b_3 - 2b_1b_2^4}{3b_3}, \tag{6}$$

(7)

$$(b_3 - b_1b_2)\frac{18b_3^5 + (15b_2^3 - 18b_1^2b_2^2)b_3^3 + 15b_1b_2^4b_3^2 + (2b_2^6 - 6b_1^2b_2^5)b_3 - 2b_1b_2^7}{9b_2b_3^2}.$$

If $b_3 = b_1b_2$ then $c = 0$ and $b_4 = b_2^2/6$, and we calculate $A = -b_2^4/3$ and $B = 2b_6^2/27$. But this makes $X^3 + AX + B = (X + 2(b_2^2/3))(X - (b_2^2/3))^2$, so our elliptic curve degenerates to a rational curve with a node (or a cusp if b_2 vanishes too).

Therefore the numerators of the fractions in (6,7) must vanish. The first of these yields a linear equation in b_1, which we solve to obtain

$$b_1 = \frac{3b_3(b_3^2 + b_2^3)}{b_2(3b_3^2 + b_2^3)}. \tag{8}$$

Substituting this into (7) yields $2b_2^6b_3(3b_3^2 - 2b_2^3)/(3b_3^2 + b_2^3)$. We conclude that $3b_3^2 = 2b_2^3$.

All nonzero solutions of $3b_3^2 = 2b_2^3$ are equivalent under scaling. We choose $(b_2, b_3) = (6, 12)$ and work our way back. We find $b_1 = 10/3$, and then $c = -8/9$, $b_4 = -2$, and finally $A = 528$ and $B = 128(12t + 31)$. To optimize the constants in the resulting family of large integral points on elliptic curves, we replace t by $6t - (10/3)$ and renormalize to obtain at last

$$A = 33,\ B = -18(8t - 1),\ Q = 9t^2 - 10t + 3,$$

$$X = 3(108t^4 - 120t^3 + 72t^2 - 28t + 5)$$
$$Y = 36(54t^5 - 60t^4 + 45t^3 - 21t^2 + 6t - 1). \tag{9}$$

To complete the proof that there are no other solutions, we must also consider the possibility that the denominator of (4) vanishes, which is to say $b_2 = 0$ or $b_3 = 0$. If $b_2 = 0$ then the t^6 and t^5 coefficients of $X^3 - QY^2$ reduce to $3b_3^2$ and $6b_3(b_1b_3 + b_4)$. Thus we also have $b_3 = 0$, and then $A = -3b_4^2$ and $X^3 + AX - QY^2 = 2b_4^3$, so the condition on the t^3 and t^2 coefficients holds automatically for any choice of b_4 and c. But this makes $X^3 + AX + B = (X - 2b_4)(X + b_4)^2$, so again we have a degenerate elliptic curve. If $b_3 = 0$ but $b_2 \neq 0$ we obtain $b_1 = 0$ and $6b_4 = b_2(3c - b_2)$. Then $A = -b_2^2(9c_2 + 4b_2^2)/12$, and $X^3 + AX - QY^2$ has t^3 coefficient zero but t^2 coefficient $b_2^3c^2/2$. Since we assume $b_2 \neq 0$, we conclude $c = 0$, leaving $A = -b_2^4/3$ and $B = 2b_2^6/27$, for the same degenerate elliptic curve as above.

II. Letter from Noam D. Elkies to Don Zagier (1988)

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 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

$$X^3(t) + A(t)X(t) + B(t) = Q(t)Y^2(t) \tag{10}$$

(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 (10) should have several solutions with $\rho \to 12$, 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 (10) is

$$A = 33,\ B = -18(8t - 1),\ Q = 9t^2 - 10t + 3,$$

$$X = 324t^4 - 360t^3 + 216t^2 - 84t + 15, \tag{11}$$

$$Y = 36(54t^5 - 60t^4 + 45t^3 - 21t^2 + 6t - 1).$$

As it stands, (11) seems of little use because Q is never a square for $t \in \mathbf{Z}$. However, we may rescale (11) 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, $t = -4892608510065361110902l839$, 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 (11). 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

$$(t^2 + 10t + 5)^3 - (t^2 + 22t + 125)(t^2 + 4t - 1)^2 = 1728t \tag{12}$$

(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 (12) to be defined over $\mathbf{Q}$: the fifth modular curve $(j(z), j(5z))$ is rationally parametrized by

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

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 (12). I have no similar rationale for (11), nor for why it gives "too large" a value of ρ.

Sincerely,
(signed)
Noam D. Elkies

Mark Watkins
Department of Mathematics
University Walk
University of Bristol
Bristol, BS8 1TW
England
E-mail: watkins@maths.usyd.edu.au