Large integral points on elliptic curves

Don Zagier

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3
Federal Republic of Germany

and

Department of Mathematics
University of Maryland
College Park, MD 20742
USA

MPI 86-23

Large integral points on elliptic curves

Don Zagier

In this note we will discuss two questions:
i) given an elliptic curve E over $\mathbb{Q}$, say in Weierstrass form $y^2=x^3+ax+b$ ($a, b \in \mathbb{Z}$), how to search efficiently for large integral solutions (x,y), and ii) how to construct elliptic curves which possess a large integral point.

Problem i) is usually handled by Skolem's p-adic method, or, in the case $a=0$, by factoring y^2-b in $\mathbb{Q}(\sqrt{b})$ and applying results on linear forms in logarithms [6,9]. We will describe three other methods. The first, which is certainly not new, works if the curve E has all its 2-torsion points defined over $\mathbb{Q}$ (i.e., if the cubic polynomial x^3+ax+b factors completely over $\mathbb{Q}$). The second needs only one 2-torsion point to be rational (i.e., $x^3+ax+b=0$ should have at least one rational root) but requires knowing generators of the Mordell-Weil group $E(\mathbb{Q})$. The third method makes no assumptions about the 2-torsion but again requires knowing a basis of $E(\mathbb{Q})$. This method is known in principle and has been used for theoretical purposes, but not, apparently, as an algorithm for actually finding integral points. All three methods depend eventually on the fact that approximate solutions of the equations

$$(1) \qquad \alpha r - \beta s \approx 0 \qquad \text{or} \qquad \alpha r - \beta s \approx \gamma \qquad (r, s \in \mathbb{Z})$$

(α, β, γ given real numbers) can be found rapidly by continued-fraction or related algorithms, and all three require a search time of the order of $\log \log B$ to find solutions with $|x|, |y| \leq B$.

For question ii) there seems to be no general procedure. We will describe some rather ad hoc methods and give a list of equations $y^2=x^3+ax+b$ having fairly

large integral solutions relative to the size of the coefficients a and b.

§1. Searching for large integral points

Method 1: Multiple Pell's equations

If an elliptic curve over $\mathbb{Q}$ has all its 2-torsion rational, it can be defined by an equation $y^2=(x-a_1)(x-a_2)(x-a_3)$ with $a_i \in \mathbb{Z}$, and Fermat descent leads to a finite list of triples (c_1,c_2,c_3) such that any integral solution has the form $x-a_i = c_i n_i^2$ $(i=1,2,3)$ for some $n_i \in \mathbb{Z}$. Combining any two of these equations gives a Pell-type equation $c_i n_i^2 - c_j n_j^2 = a_j - a_i$ whose solutions belong to finitely many sequences of exponential growth, and this means that $\log x$ is exponentially close to a member of an arithmetic sequence $\{\alpha r+\beta \mid r\in\mathbb{N}\}$ with $\alpha, \beta \in \mathbb{R}$. Combining any two of these formulas for $\log x$ gives an equation $\alpha r + \beta = \alpha' r' + \beta' + O(e^{-cr})$ $(c > 0)$ of the form (1), and this can be solved in time roughly $O(\log r) = O(\log \log x)$.

As an example we take the old chestnut: when is the sum of the first n squares a perfect square? This problem, often known as the "cannonball problem" because it appears in puzzle books (e.g. [5], #138) in terms of stacking cannon-balls into a square pyramid, has been solved long ago; the unique non-trivial solution $1^2+2^2+\ldots+24^2 = 70^2$ is connected with the construction of the Leech lattice [4] and hence has a certain importance in modern physics. The equation $1^2+\ldots+n^2 = m^2$ can be written $6m^2 = n(n+1)(2n+1)$, and an easy consideration shows that any solution has the form

$$n = a^2, \quad n+1 = 2b^2, \quad 2n+1 = 3c^2$$

or

$$(2) \qquad n = 6a^2, \quad n+1 = b^2, \quad 2n+1 = c^2,$$

the two being exemplified by $n=1$ and $n=24$, respectively. We consider only (2). It leads to three Pell equations

$$c^2 - 12a^2 = 1, \quad c^2 - 2b^2 = -1, \quad b^2 - 6a^2 = 1 \qquad (a,b,c>0)$$

with solutions given by

$$c + a\sqrt{12} = (7+2\sqrt{12})^r, \quad c + b\sqrt{2} = (1+\sqrt{2})^s, \quad b + a\sqrt{6} = (5+2\sqrt{6})^t \qquad (r,s,t > 0, \quad s \text{ odd}).$$

Hence

$$n = \frac{(7+\sqrt{48})^{2r}-2+(7-\sqrt{48})^{2r}}{8} = \frac{(1+\sqrt{2})^{2s}-6+(1-\sqrt{2})^{2s}}{8} = \frac{(5+\sqrt{24})^{2t}-2+(5+\sqrt{24})^{2t}}{4}$$

and

$$\begin{aligned} \log n &= 2r \log(7+\sqrt{48}) - \log 8 + O(\tfrac{1}{n}) \\ &= 2s \log(1+\sqrt{2}) - \log 8 + O(\tfrac{1}{n}) \\ &= 2t \log(5+\sqrt{24}) - \log 4 + O(\tfrac{1}{n}) \end{aligned} \tag{3}$$

with explicit $O(\ )$-constants. Combining any two of these leads to an approximate equation of the form (1). The most convenient two are the first two, since the terms $\log 8$ drop out and we are left with the homogeneous equation

$$r \log(7+\sqrt{48}) - s \log(1+\sqrt{2}) = O((7+\sqrt{48})^{-2r}) . \tag{4}$$

Any solution of this would correspond to a very good rational approximation $\frac{s}{r}$ (with s odd) of the real number

$$\lambda = \frac{\log(7+\sqrt{48})}{\log(1+\sqrt{2})} = 2.98842151913866080048061748394973719231535212135 22...$$

and could be recognized by a very large partial quotient in the continued fraction expansion of λ. This expansion begins $[2,1,85,2,1,2,1,1,1,...]$. The large partial quotient 85 at the beginning corresponds to the rational approximation $\frac{3}{1}$ of λ and the the solution $n = 24$ of our original problem. Computing the expansion further to as many terms as justified by the above 50 digits of λ, we find no further large partial quotients, and this shows that (4) has no solution under about 10^{25} and consequently (2) no further solution under about $10^{10^{25}}$. This bound would be even larger if we had used a more accurate value of λ, e.g. $10^{10^{100}}$ if we had 200 rather than 50 digits; the time needed for the computation (of the decimal and then of the continued fraction expansion of λ) is negligible on even a modest computer. If we had taken a different pair of the equations (3) or were looking at a different example, then we would have had to look at an equation like (4) but with an extra additive constant, i.e., an equation like the second one in (1). A modification of the continued fraction algorithm permits

one to solve such equations almost as fast as their homogeneous counterparts.

Method 2: Pell's equation and canonical height

Now suppose that our elliptic curve has only one rational 2-torsion point, but that its Mordell-Weil group is known. As an example we take the curve

$$(5) \qquad E: \quad y^2 = x^3 - 30x + 133 = (x+7)(x^2-7x+19)\,,$$

which by inspection has the small integral solutions

$$T = (-7,0), \quad \pm P = (6,\pm 13), \quad \pm P + T = (2,\mp 9), \quad \pm 2P = (-3,\pm 14)$$

with $2T = 0$. By descent one shows easily that $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with generators P and T (a 2-descent over $\mathbb{Q}$ can be carried out for any elliptic curve having at least one rational 2-torsion point; see [8], pp. 301-304). If (x,y) is an integer solution of (5), then $x+7$ is positive and the g.c.d. of $x+7$ and $x^2-7x+19$ is a divisor of $117=3^2\cdot 13$, so $x+7=da^2$, $x^2-7x+19=db^2$ for $d \in \{1,3,13,39\}$. The values $d=3$ and $d=39$ lead to a contradiction (if $x^2-7x+19 = (x+1)^2-9(x+1)+27$ is divisible by an odd power of 3 then $x+1 \equiv 0 \bmod 9$ and $(x+7)/3$ cannot be a square or 13 times a square) and the value $d=1$ to the factorizable equation $(2b)^2-(2x-7)^2=27$ whose only solutions with $x+7$ a square are $x=-3$, $x=2$. We are left with

$$x + 7 = 13a^2\,, \qquad x^2 - 7x + 19 = 13b^2\,.$$

The second of these equations can be written $(2x-7)^2-52b^2=-27$ and has the general solution

$$2x-7+b\sqrt{52} = (\pm 5+\sqrt{52})(649+90\sqrt{52})^{\ell} \quad \text{or} \quad (\pm 21+3\sqrt{52})(649+90\sqrt{52})^{\ell}$$

The solutions with $-5+\sqrt{52}$ and $+21+3\sqrt{52}$ lead to x congruent to 1 or 5 (mod 9), incompatible with $x+7=13a^2$. Also, from $x \equiv -7 \pmod{13}$ we find that ℓ must be even, so in fact

$$(6) \qquad 2x-7+b\sqrt{52} = (5+\sqrt{52})(842401+116820\sqrt{52})^{r} \quad \text{or} \quad (-21+3\sqrt{52})(842401+116820\sqrt{52})^{r'}$$

for some $r,r' \geq 0$. The values $r=0$, $r'=0$ lead to the small solutions $x=6$ and $x=-7$, while $r=1$ leads to the "large" solution

(7) $$(x,y) = (5143326\ ,\ \pm 11664498677) \quad (= \pm 5P)\ .$$

But now we seem to have reached an impasse, for simply searching through small values of r and r' looking for x in (6) with $(x+7)/13$ a perfect square would first of all require huge accuracy (since x grows very rapidly and one cannot use an approximate value of an integer to test whether it is a square) and also would be only exponentially rather than doubly exponentially fast (i.e., would require computing time of the order of $\log x$ rather than $\log\log x$). So we need a second condition on x to replace the second Pell's equation of Method 1.

This second condition is provided by the canonical height function. We do not review the theory of the height (see, for instance, Chapter VIII of [8]), but only recall that it is a positive definite quadratic form

$$h\colon E(\mathbb{Q})/(\text{torsion}) \longrightarrow \mathbb{R}_+$$

which is effectively and rapidly computable (cf. [3] for an example of a high accuracy computation). Suppose we have a large solution (x,y) of (5) and write it as mP or $mP+T$ with $m \in \mathbb{Z}$. Then on the one hand

$$h((x,y)) = m^2\, h(P)$$

since h is quadratic, and on the other hand by the definition of the height

$$h((x,y)) = \log x + c + O(\tfrac{1}{x})$$

with c and the $O(\ )$-constant effectively computable. (Again we refer to the above sources; observe that for an integral point on an elliptic curve one would in general have $h((x,y)) = \log x + c_i + O(x^{-1})$ for one of a finite collection of constants c_i, depending on congruence conditions on x modulo the various primes of bad reduction of the curve.) Combining these two formulas and our Pell-type equation (6) gives the pair of equations

$$\begin{aligned} \log x &= r\alpha + \beta + O(\tfrac{1}{x}) \quad \text{or} \quad r'\alpha + \beta' + O(\tfrac{1}{x}) \\ &= m^2 h(P) - c + O(\tfrac{1}{x}) \end{aligned}$$

with $\alpha = \log(842401+116820\sqrt{52})$, $\beta = \log\frac{5+\sqrt{52}}{2}$, $\beta' = \log\frac{-21+3\sqrt{52}}{2}$. If we

now simply forget that m^2 is a square and write s instead of m^2, we are left with a non-homogeneous approximate linear equation like the second one in (1) which again can be solved in roughly logarithmic time with respect to r or s and hence doubly logarithmic time with respect to x, with only moderate accuracy required. We omit the actual computational details since our third method will be superior anyway. Observe that the present method would also work, though not quite as well, if the rank of $E(\mathbb{Q})$ were larger than 1. If, for instance, $E(\mathbb{Q})$ had two (known) generators P_1 and P_2, then the fact that the height is a quadratic form would mean that the height of an unknown large integral point $(x,y) = m_1P_1 + m_2P_2$ would be a quadratic form $h_1m_1^2 + h_2m_1m_2 + h_3m_2^2$. If we then write s_1, s_2 and s_3 for the three unknown integers m_1^2, m_1m_2 and m_2^2 (thus forgetting that s_1 and s_3 are squares and $s_2^2 = s_1s_3$), we would have an equation of the form $r\alpha + h_1s_1 + h_2s_2 + h_3s_3 + \beta \approx 0$, i.e. like (1) but with more variables. This can be solved reasonably quickly by using the algorithm of [7] instead of continued fractions.

Method 3: Group law on $E(\mathbb{R})$

The third method is based on the fact that the Mordell-Weil group $E(\mathbb{Q})$ is a subgroup of $E(\mathbb{R})$, which is isomorphic to the circle group $\mathbb{R}/\mathbb{Z}$ or to two copies of the circle group. We need only consider the identity component $E(\mathbb{R})^0$

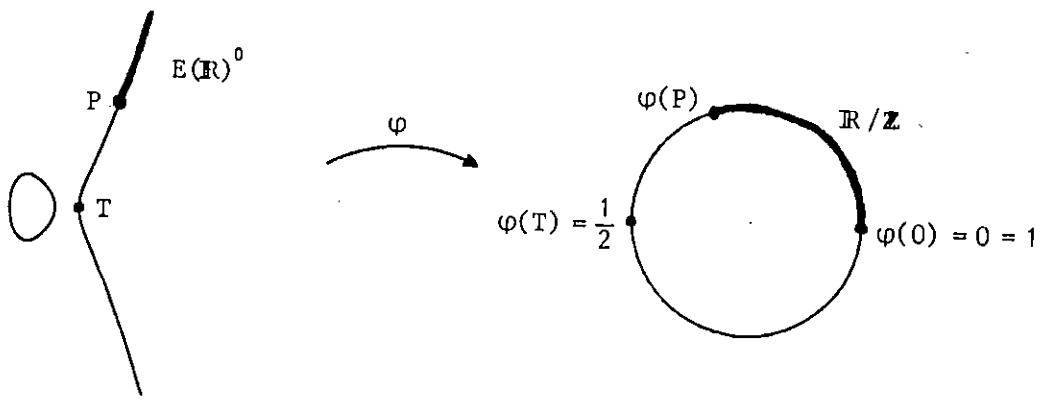

Figure 1

of $E(\mathbb{R})$ since in the Weierstrass model $y^2=x^3+ax+b$ the other component, if there is one, is compact and one can find all integral points on it by direct

search. The isomorphism $\varphi: E(\mathbb{R})^0 \longrightarrow \mathbb{R}/\mathbb{Z}$ is given explicitly by

$$(8) \qquad \varphi(P) \equiv \frac{1}{\Omega} \int_{\xi}^{\infty} \frac{dx}{\sqrt{x^3+ax+b}} \pmod 1$$

if $P = (\xi,\eta)$ with $\eta > 0$ and by $\varphi(-P) = -\varphi(P)$ if $\eta < 0$; here $\Omega = 2\int_{\gamma}^{\infty} \frac{dx}{\sqrt{x^3+ax+b}}$ (γ = largest real root of $x^3+ax+b=0$) is the real period of E.

As an example we again take the curve (5). Here $E(\mathbb{Q}) = \langle P,T \rangle$ with $2T=0$ and $P=(6,13)$ of infinite order. If $P' = (\xi,\eta)$ is a large integral solution of (5), then $\varphi(P') = O(\xi^{-\frac{1}{2}})$ by (8), the $O(\ )$-constant being known explicitly. On the other hand, $P' = rP$ or $rP+T$ for some $r \in \mathbb{Z}$, so $\varphi(P') \equiv r\varphi(P)$ or $r\varphi(P) + \frac{1}{2} \pmod 1$. Also, $\xi > e^{cr^2}$ for some $c > 0$ by the height considerations discussed under "Method 2," so $\varphi(P') = O(e^{-cr^2/2})$. We thus have an approximate equation of the form

$$(9) \qquad r \cdot 2\varphi(P) - s = O(e^{-cr^2/2}) \qquad (r, s \in \mathbb{Z}),$$

and this is an equation of the (easier, homogeneous) form (1) which can be solved as usual by a continued fraction algorithm once we know $\varphi(P)$ accurately. Numerical integration on a pocket calculator gives $\varphi(P) \approx 0.200041344203$; this has the obvious rational approximation $\frac{1}{5}$, corresponding to the large integral point (7), and no other good approximations (in the sense of (9)) with numerator and denominator under around 10^6, showing that (5) has no further integral solution under about $10^{2.5\times10^{11}}$. To go further, we need a more accurate value of $\varphi(P)$. Numerical integration would work, but there are better ways. The denominator Ω in (8), a complete elliptic integral, can be calculated very rapidly by Gauss's arithmetic-geometric mean, and the method can be extended to cover also the incomplete elliptic integral in the numerator (Landen's transformation). This method is doubly exponential, i.e., in n steps one gets about 2^n digits of accuracy, but requires evaluating a transcendental function (see below). There is a simpler method which is only simply exponential but requires only elementary arithmetic operations. Namely, it is obvious from equation (8), or from Figure 1, that $\varphi(Q) \in (0,\frac{1}{2})$ for a point Q with positive y-coordinate and $\varphi(Q) \in (\frac{1}{2},1)$ if $y(Q) < 0$. Since $\varphi(2^iQ) \equiv 2^i\varphi(Q) \pmod 1$, we

immediately obtain the binary expansion

$$(10) \qquad \varphi(P) = \sum_{i=0}^{\infty} \frac{a_i}{2^i}, \qquad a_i = \begin{cases} 0 & \text{if } y(2^iP) > 0, \\ 1 & \text{if } y(2^iP) < 0. \end{cases}$$

Since doubling a point on $y^2 = x^3+ax+b$ is given by the simple formula

$$Q = (x,y) \Rightarrow 2Q = (\lambda^2 - 2x, \lambda(3x-\lambda^2) - y) \qquad \left(\lambda = \frac{3x^2+a}{2y}\right),$$

this gives an easy way to compute $\varphi(P)$ one binary digit at a time. Taking 167 terms of (10) gives the 50-digit value

$$\varphi(P) \approx 0.20004134420460575588311129477140424985602364831619,$$

and this is enough (since its continued fraction has no very large partial quotients after the initial $[4,1,966,1,\ldots]$) to show that (5) has no further integral solutions after (7) under about $10^{10^{50}}$. Again, we could push this bound up further in negligible computer time if we had more than 50 digits of accuracy available. If we used Landen's transformation mentioned above, then (10) would be replaced by a formula of the form

$$(11) \qquad \varphi(P) = \frac{a_1}{2} + \frac{a_2}{4} + \ldots + \frac{a_n}{2^n} + \frac{\arctan(b_n)}{2^n\pi} + \varepsilon_n \qquad (0 < \arctan(b_n) < \pi)$$

where b_n is a certain inductively computed algebraic number and $\varepsilon_{n+1} = O(\varepsilon_n^2)$. Then 10 terms (rather than 167) would suffice to give the above 50-digit value of $\varphi(P)$, and 12 (rather than 665) to give 200 digits. However, since the problem of computing $\varphi(P)$ is primarily one of accuracy, rather than time, anyway, this more complicated method is not worth applying and we omit the formulas for computing b_n in (11).

As in Method 2, we could deal with curves of rank >1 by using the algorithm of [7] rather than the continued fraction algorithm. Also, it is perhaps noting that the function φ is so easy to compute using (10) that it is actually the most convenient way to look for small linear dependences among rational or integral points on elliptic curves. For instance, the curve $y^2 = x^3+17$ of rank 2 has the integral points

$$P_1 = (-2,3),\ P_2 = (-1,4),\ P_3 = (2,5),\ P_4 = (4,9),\ P_5 = (8,23),$$
$$P_6 = (43,282),\ P_7 = (52,375),\ P_8 = (5234,378661)$$

(and their negatives). Using (10) we find

$$\varphi(P_1) = .432771019602809\ldots\,, \quad \varphi(P_2) = .379909003461601\ldots\,,$$
$$\varphi(P_3) = .245451042667221\ldots\,, \quad \varphi(P_4) = .187319976935588\ldots\,,$$
$$\varphi(P_5) = .134457960794380\ldots\,, \quad \varphi(P_6) = .058131065731633\ldots\,,$$
$$\varphi(P_7) = .052862016141208\ldots\,, \quad \varphi(P_8) = .005269049590425\ldots\,,$$

and looking for small linear dependencies (mod 1) by hand or by the algorithm of [7] we immediately find the representations of $P_3, \ldots, P_8$ as $2P_1+P_2$, $-P_1-P_2$, $-2P_1$, $3P_1+2P_2$, P_1-P_2 and $2P_1+3P_2$, respectively, the work involved being probably less than that needed to actually carry out the additions on the elliptic curve.

Remarks on finding all integral points

We have described three methods, each of which is doubly exponential and in favorable circumstances permits one to find all integral points on an elliptic curve with coordinates up to a number of the order of $10^{10^{100}}$. The question naturally arises whether this, in combination with the known upper bounds on integral points given by Baker's results on linear forms in logarithms, suffices to ensure that all integral solutions of an equation $y^2 = x^3+ax+b$ have been found. Unfortunately, although the bound given by Baker's method is only singly exponential in a polynomial in $H = \max\{|a|,|b|\}$, the constants involved are so big that the bound is for all practical purposes actually triply exponential even for $H = 10$ the published result [1]

$$\max\{|x|,|y|\} \quad < \quad \exp((10^6 H)^{10^6})$$

gives the upper bound $|x| < 10^{10^{10^{6.8}}}$, far bigger than the above $10^{10^{100}}$. However, recently better estimates have been obtained by Masser and Wüstholz based on analogues of Baker's bounds for elliptic rather than ordinary logarithms (cf. [8], pp. 262-263); here "elliptic logarithm" refers to the function $\varphi: E(\mathbf{R})^0 \longrightarrow \mathbf{R}/\mathbf{Z}$ discussed under "Method 3" above. The best bound obtained (G. Wüstholz, not yet published) has the form

$$|\varphi(r_1P_1+\ldots+r_nP_n)| \;>\; e^{-c(\log r)^{n+1}\log\log r} \qquad \Big(r = \max_{1\le i\le n}|r_i|\Big)$$

where c is a computable constant depending on E and on $P_1,\ldots,P_n$ whose value

(not yet computed numerically) should be of the order of 10^{50} for n=1 and E, P_1 of reasonable size. Together with the upper bound $|\varphi| < e^{-c'r^2}$ discussed above, this should lead to a bound on r small enough to permit the determination of all integral points on E if the rank of $E(\mathbb{Q})$ is small and its generators are known.

§2. Curves with large integral points

We now turn to our second theme of finding examples of equations

$$y^2 = x^3 + ax + b \qquad (a, b \in \mathbb{Z}) \tag{12}$$

which have a large integral solution. We must first decide what we mean by "large." If x is any positive integer and we take for y the nearest integer to $x^{3/2}$, then $|y^2-x^3| < x^{3/2}+\frac{1}{4}$ and we obtain a solution of (12) with $|b| \le x/2$, $|a| \le x^{\frac{1}{2}}+1$. Since this works for all x, we want at least to require that a "large" solution have $a = O(x^\alpha)$, $b = O(x^\beta)$ with $\alpha < \frac{1}{2}$, $\beta < 1$. This forces us to choose $y = \langle x^{\frac{3}{2}} \rangle$ (nearest integer to $x^{\frac{3}{2}}$), b = smallest residue (in absolute value) of $y^2-x^3 \pmod x$, $a = (y^2-x^3-b)/x$ in (12), i.e., everything is determined by x. Since the a priori ranges of a and b are $O(x^{\frac{1}{2}})$ and $O(x)$, respectively, the probability that a given x leads to a solution with $a = O(x^\alpha)$, $b = O(x^\beta)$ is $O(x^{\alpha+\beta-\frac{3}{2}})$, and we will expect infinitely many such examples if the sum of this over all x diverges, i.e., if $\alpha+\beta \ge \frac{1}{2}$. In particular (specializing to $\alpha=0$, $\beta=0$, $\alpha=\beta$ and $3\alpha=2\beta$, respectively), we can expect that for any $\varepsilon > 0$ the four assertions

$$\begin{aligned}
y^2 = x^3 + b \quad (x, y, b \in \mathbb{Z}) &\Rightarrow x \le b^{2+\varepsilon} \quad \text{("Hall's conjecture")} \\
y^2 = x^3 + ax \quad (x, y, a \in \mathbb{Z}) &\Rightarrow x \le a^{2+\varepsilon} \\
y^2 = x^3 + ax + b \quad (x, y, a, b \in \mathbb{Z}) &\Rightarrow x \le \max\{|a|, |b|\}^{4+\varepsilon} \\
y^2 = x^3 + ax + b \quad (x, y, a, b \in \mathbb{Z}) &\Rightarrow x \le \max\{|a|^{\frac{1}{2}}, |b|^{\frac{1}{3}}\}^{10+\varepsilon}
\end{aligned}$$

hold with only finitely many exceptions but that each has infinitely many exceptions for $\varepsilon = 0$. A reasonable measure of the impressiveness of a large integral solution seems to be the number

$$\rho = \log(x)/\log(\max\{|a|^{\frac{1}{2}}, |b|^{\frac{1}{3}}\}) \tag{13}$$

(interpretation: x_i is of the order of the ρ-th power of the roots of $x^3+ax+b=0$); then asymptotically we would not expect to exceed $\rho = 10+\varepsilon$ and would regard any value of ρ near 10 as worth recording.

The above suggests an exhaustive way to find good solutions of (12): we simply try every value $x = 1,\dots,X$, set $y = \langle x^{\frac{3}{2}} \rangle$, $a = \langle y^2x^{-1} - x^2 \rangle$, $b = y^2-x^3-ax$ and record (a,b,x,y) if ρ is large enough. This method of coming up with examples is admittedly like the one Borho [2] once likened to that of draining a section of a river dry and picking up the fish from the river bed, earning the scorn of all real fishermen; nevertheless, it gives us a start. We can make two slight improvements. First of all, if we write $x = s^2+t$ with $-s < t \le s$ (every positive integer has a unique such representation), then by the binomial theorem $x^{\frac{3}{2}}$ equals $s^3 + \frac{3}{2}st + \frac{3}{8}s^{-1}t^2 + \varepsilon$ with $|\varepsilon| < .1$, so we can compute y as $\langle s^3 + \frac{3}{2}st + \frac{3}{8}s^{-1}t^2 \rangle$, thus avoiding the non-elementary square root operation. Also, if we write

$$(14) \qquad y = s^3 + \frac{3st+r}{2}, \qquad r = \left\langle \frac{3}{4}\frac{t^2}{s} \right\rangle$$

(rejecting the solution if $r \not\equiv st \pmod 2$), then

$$(15) \qquad y^2 - x^3 = \frac{1}{4}[s^2(4sr-t^2) + r^2 + 6str] - t^3,$$

which involves only numbers of the order of $x^{\frac{3}{2}}$ rather than x^3, so we can compute with modest accuracy. In this way we can fairly quickly find all solutions of (12) with a and b fairly small relative to x and x less than some chosen bound X. At my request, A. Odlyzko ran this algorithm on a Cray-1 up to $X = 10^8$ (running time: 4 minutes), printing out all solutions with $|a| \le x^{\frac{1}{4}}$, $|b| \le x^{\frac{1}{3}}$. He found 117 solutions in this range, of which 54 had the form $a = \pm1$ or ±2 and $b = \square$, corresponding to the parametric solutions

$$(16) \qquad \begin{aligned} (x,y) &= (64n^6 \pm 8n^2,\ 512n^9 \pm 96n^5 + 3n), & y^2 &= x^3 \pm x + n^2, \\ (x,y) &= (4n^6 \pm 4n^2,\ 8n^9 \pm 12n^5 + 3n), & y^2 &= x^3 \pm 2x + n^2 \end{aligned}$$

with $n \le 10$, $n \le 17$, respectively. Some of the best of the other 63 solutions are listed in Table 1, with the corresponding values of ρ (note that $\rho = 9 + O(\frac{1}{\log n})$ for the families (16)). The curve (ℓ) in this table is the curve (5) used as an example in §1. Most of the curves in Odlyzko's table had a relatively

	a	b	x	y	ρ
(a)	-2	5	1,318	47,849	13.39
(b)	4	-1	4,321	284,038	12.08
(c)	0	17	5,234	378,661	9.07
(d)	11	4	16,833	2,183,948	8.12
(e)	-13	37	60,721	14,962,645	8.59
(f)	-12	-10	80,327	22,766,293	9.09
(g)	-7	22	484,961	337,722,676	12.71
(h)	-9	28	764,396	668,309,460	12.20
(i)	-13	4	1,056,517	1,085,962,264	10.82
(j)	-19	-51	2,955,980	5,082,205,677	10.12
(k)	-24	124	4,435,710	9,342,104,422	9.53
(ℓ)	-30	133	5,143,326	11,664,498,677	9.09
(m)	-37	60	11,975,623	41,442,617,124	9.03
(n)	-23	-33	17,454,557	72,922,784,957	10.64
(o)	-16	49	19,103,002	83,493,454,805	12.09
(p)	27	-62	28,844,402	154,914,585,540	10.42
(q)	37	18	64,039,202	512,470,496,030	9.96
(r)	2	97	90,086,608	855,047,718,145	12.01

Table 1. Some large solutions of (12)

large number of small integral points; only 8 (including the curves (h), (ℓ), (m) and (p) of Table 1) had a rational 2-torsion point.

We now try to construct families of curves with big solutions. The first idea is to choose $x = s^2+t$ with $3t^2$ divisible by $4s$, since this will give the best approximation of r to $\frac{3t^2}{4s}$ in (14). If $4sr = 3t^2$ then (15) reduces to $y^2-x^3 = \frac{1}{8}t^3 + \frac{1}{4}r^2$, and this can be made near a multiple of $x = s^2+t$ by choosing $\frac{1}{8}t^3$ divisible by s^2. The conditions $4s \mid 3t^2$, $8s^2 \mid t^3$ lead to $s = \lambda n^3$, $t = 2\lambda u n^2$, $r = 3\lambda u^2 n$ and hence to

$$(17) \qquad (x,y) = (\lambda^2 n^6 + 2\lambda u n^2,\ \lambda^3 n^9 + 3\lambda^2 u n^5 + \tfrac{3}{2}\lambda u^2 n),\quad y^2 = x^3 + (\lambda u^3)x + (\tfrac{1}{4}\lambda^2 u^4 n^2)$$

with $\lambda, u, n \in \mathbf{Z}$ and (to ensure integrality) $2 \mid \lambda u n$. The best values are obtained with n large and λ and u small. In particular, the values $u = \pm 1$, $\lambda = 1, 2$ give the families (16), and any fixed values of λ and u lead to an infinite parametric family with $\rho = 9 + o(1)$. We can modify the family (17) by adding a

constant c to the formula $x = \lambda^2 n^6 + 2\lambda u n^2$; this leads after some calculation to

$$(18) \qquad \begin{aligned} x &= \lambda^2 n^6 + 2\lambda u n^2 + c \\ y &= \lambda^3 n^9 + 3\lambda^2 u n^5 + \tfrac{3}{2}\lambda(u^2+cn^2)\delta \\ a &= \lambda\delta u - 3c^2 \\ b &= \tfrac{1}{4}\lambda^2\delta^2 n^2 - c\lambda\delta u + 2c^3 \end{aligned}$$

with $\lambda, u, n, c \in \mathbb{Z}$, $\delta := u^2 - 3cn^2$, and $\lambda\delta n \equiv 0 \pmod 2$. For fixed values of c and δ the equation $u^2-3cn^2=\delta$ is a Pell's equation with (if any) infinitely many integral solutions and we again get infinite families of examples with $\rho = 9 + o(1)$. For instance, taking $\lambda = \delta = 1$ we find for $c=2$ and $(n,u) = (20,49)$ the curve (q) of Table 1, while taking $c = 4$, 10, 1 and 6 and the smallest integer solution of $u^2-3cn^2=1$ with $n > 20$ leads to the larger examples given in Table 2.

(s)	$y^2 = x^3 + 49x - 64$,	$x =$	482,042,404	$y =$	10,583,464,697,386
(t)	$y^2 = x^3 - 59x + 74$,	$x =$	7,257,247,018	$y =$	618,241,079,050,562
(u)	$y^2 = x^3 + 94x + 689$,	$x =$	30,841,587,841	$y =$	5,416,329,712,145,492
(v)	$y^2 = x^3 + 469x + 1594$,	$x =$	6,327,540,232,326	$y =$	15,916,675,888,150,694,092

Table 2. Curves given by (18) with $\lambda=1$, $\delta=1$

Next, we analyze some of the large solutions in Table 1 to see if they have a special form which can be generalized. The solutions in (b), (d), (i), (m) and (q) are of the form $3P$ for some P with small integral coordinates, those in (k) and (ℓ) have the form $5P$, and those of (h) and (r) have the form $2P + T$ where $2T = 0$ (in fact, the solution in (h) has the form $4P + T$ with $P = (-1,6)$ or $(9,-26)$ and $T = (-4,0)$). This suggests looking for parametric families of curves with integral points of one of these forms. We first need a small integral (or, in the case of 2P+T, half-integral) point P on our curve. It is convenient to abandon the standard Weierstrass form and instead shift x by $x(P)$ so that $P = (0,n)$ for some $n \in \mathbb{Z}$, i.e., we take our curve in the form

$$(19) \qquad E: \; y^2 = x^3 + \ell x^2 + mx + n^2, \qquad P = (0,n) \qquad (\ell, m, n \in \mathbb{Z}).$$

Then by direct calculation we have

$$x(2P) = \frac{m^2}{4n^2} - \ell, \quad x(3P) = \frac{n^6}{k^2} + \frac{mn^2}{k},$$

$$x(5P) = \left(\frac{n^3}{k} + \frac{m}{2n} + \frac{2k^2(n^4+mk)}{n(n^8+mkn^4-2k^3)}\right)^2 - \left(\frac{n^3}{k} + \frac{m}{2n}\right)^2 ,$$

where $k = \frac{1}{8}(m^2-4\ell n^2)$. Making 2P integral consists simply in requiring that $m = 2nh$ in (19) for some integer h, but the corresponding value $x(2P) = h^2-\ell$ is not particularly big, corresponding to the fact that there are no cases of a point 2P in Table 1. Making $x(3P)$ integral and large can be done most easily by taking $k = \pm 1$ or, since only $8k$ need be integral, $k = \pm\frac{1}{2}$, $\pm\frac{1}{4}$ or $\pm\frac{1}{8}$, i.e. $m^2-4\ell n^2 = \pm 1$, ± 2, ± 4 or ± 8. This has trivial solutions with $\ell = 0$, $m = \pm 1$ or ± 2, leading to the families (16), and Pell-type solutions with $\ell \neq 0$ fixed and small, leading to the families (18). Thus we get nothing new with this Ansatz. Of course, we may have $k\,n$ (and hence 3P integral) for other values of k than ± 1, $\pm\frac{1}{2}$, $\pm\frac{1}{4}$ or $\pm\frac{1}{8}$ (as mentioned, several of the large solutions found have the form 3P without belonging to the parametric family (18)), but it is not clear how to obtain infinite families of curves satisfying this.

We next try to make 5P integral as in the curves (k), (ℓ) of Table 1. The above formula for $x(5P)$ is integral at k and n, so need solutions of

$$(20) \qquad n^8 + mkn^4 - 2k^3 \mid 2k^2(n^4 + mk)$$

in integers $n, 8k, m$ with $8k-m^2$ divisible by n^2. It is not clear how to solve this parametrically in general. However, our test curves (k) and (ℓ) have not only P and 5P, but also 2P integral, i.e. $2n \mid m$. Write $m = 2nh$ and set $p = \ell-h^2$; then our curve becomes $y^2 = x^3 + (h^2+p)x^2 + (2nh)x + n^2$ and (20) reduces to

$$(2n - ph)^2 + p^2(p - h^2) \mid n^3p^3(n - ph) .$$

This is still hard to solve in full generality, but we can get two classes of solutions by choosing either

$$2n - ph = 0 , \qquad p = h^2 + h^i \quad (0 \leq i \leq 14)$$

or

$$p - h^2 = 0 , \qquad 2n - ph = \pm 1 .$$

The first does not lead to particularly large $x(5P)$, but the second gives

$$p = h^2, \quad n = \frac{h^3 \pm 1}{2}, \quad \ell = 2h^2, \quad m = h^4 \pm h, \quad x = h^{14} \mp 2h^{11} + h^8 \pm 2h^5 - 2h^2$$

with x fairly large. To get n integral we take h odd; we also choose $3|h$ so that $\ell \equiv 0 \pmod 3$ and the equation (19) can be put into standard Weierstrass form without introducing denominators. This gives the two families

$$(21) \qquad \begin{aligned} x &= h^{14} \mp 2h^{11} + h^8 \pm 2h^5 - \tfrac{4}{3}h^2, \quad y = h^{21} \mp 3h^{18} + 3h^{15} \pm 2h^{12} - 5h^9 \pm 2h^6 + \tfrac{3}{2}h^3 \mp \tfrac{1}{2}, \\ y^2 &= x^3 + (-\frac{h^4}{3} \pm h)\, x + \frac{19h^6 \mp 18h^3 + 27}{108} \qquad (h \equiv 3 \pmod 6) \end{aligned}$$

with $\rho = 7 + o(1)$. For $h=3$ they give the curves (k) and (ℓ).

Finally, we consider the case when $2P+T$ is integral for some P, where T is a rational 2-torsion point. This time we shift coordinates to make $T = (0,0)$, so our curve has an equation $y^2 = x^3 + \ell x^2 + mx$. We assume that P has the form $(\xi^2, \xi\eta)$ with ξ integral and $\eta^2 = \xi^4 + \ell\xi^2 + m$ (this is the case for our examples (h) and (r), except that ξ has a denominator 2 which can be removed by rescaling). Then $x(2P) = (\frac{\xi^4 - m}{2\xi\eta})^2$ and $x(2P+T) = m/x(2P)$. If we have $\xi^4 - m = \pm 1$, then $x(2P)$ is the reciprocal of a large integer and $x(2P+T)$ is integral and large. Both of our test curves are of this type with the + sign, so we choose $m = \xi^4 - 1$; then the condition on η becomes $\eta^2 = \xi^2(2\xi^2 + \ell) - 1$. This leads to

$$\ell = r - 2\xi^2, \quad m = \xi^4 - 1, \quad x(2P+T) = 4\xi^2\eta^2(\xi^4 - 1),$$

where (ξ, η) is a solution of the Pell's equation $\eta^2 - r\xi^2 = -1$. We look for r such that this equation has a solution with ξ of the order of $r^{\frac{1}{2}}$; then $\ell = O(r)$, $m = O(r^2)$, $x(2P+T) = O(r^5)$ and our curve has $\rho = 5 + o(1)$, the best that can be attained this way. We get some improvement by taking $r \equiv 2 \pmod 8$ (then ξ and η are odd and we can divide ℓ, m by 2^2 and 2^4) and $r \equiv 2 \pmod 3$ (then $3|\ell$ and we can put our curve into standard Weierstrass form without extra denominators). This gives

$$(22) \qquad \begin{aligned} y^2 &= x^3 - \tfrac{1}{48}(r^2 - 4r\xi^2 + \xi^4 + 3)\, x + \tfrac{1}{1728}(r - 2\xi^2)(2r^2 - 8r\xi^2 - \xi^4 + 9), \\ (x,y) &= (\xi^2\eta^2(\xi^4 - 1) + \tfrac{1}{12}(r - 2\xi^2),\ \tfrac{1}{4}\xi\eta(\xi^4 - 1)(4r\xi^6 - 4\xi^4 - 2r\xi^2 + 1)), \\ & r \equiv 2 \pmod{24}, \quad \eta^2 - r\xi^2 = -1. \end{aligned}$$

The values $r = 2$, $(\xi, \eta) = (5,7)$ and $r = 74$, $(\xi, \eta) = (5,43)$ give the curves (h)

and (p). The values $r = 338$, $(\xi,\eta) = (13,239)$ give the curve (x) in Table 3 below; this curve is especially interesting because it has $b = 0$, but this never happens again with (22), since $r = 2\xi^2$ leads to the equation $\eta^2 = 2\xi^4 - 1$ whose only non-trivial solution is (13,239). Larger values of r give less impressive solutions (since the family (22) has only $\rho = 5 + o(1)$), but sometimes the coefficients a and b have the form $\lambda\mu^2 a_1$, $\lambda^2\mu^3 b_1$ for some smaller integers λ, μ, a_1 and b_1, and then the curve can be put into the form $\mu y^2 = \lambda x^3 + a_1 x + b_1$ with smaller coefficients. In this way the values $r = 218$, 338, 5018 and 3170 (and (ξ,η) = smallest solution of $\eta^2 = r\xi^2 - 1$) give the curves with large integral points shown in Table 3.

(w)	$6y^2 = 5x^3+14x+19$,	$x =$	50689092575	$y =$	10417923210092732
(x)	$y^2 = x^3 + 1785x$,	$x =$	275702503440	$y =$	144764163249358380
(y)	$y^2 = 95x^3+93x-946$,	$x =$	185532736100114	$y =$	2463160018431117356384 4
(z)	$3y^2 = 143x^3-9x+9116$,	$x =$	147235975797220556	$y =$	39005720082463093451787342 0

Table 3. Curves coming from equation (22)

Bibliography

[1] A. Baker, Transcendental Number Theory, Cambridge University Press, 1975.

[2] W. Borho, Befreundet Zahlen, Ein zweitausend Jahre altes Thema der elementaren Zahlentheorie, Mathematische Miniaturen, Birkhäuser 1981, 5-38.

[3] J. Buhler, B. Gross, D. Zagier, On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3, Math. Comp. 44 (1985) 473-481.

[4] J.H. Conway, N.J.A. Sloane, Lorentzian forms for the Leech lattice, Bull. A.M.S. 6 (1982) 215-217.

[5] H.E. Dudeney, Amusements in Mathematics, Th. Nelson, London, 1917.

[6] W. Ellison, F. Ellison, J. Pesek, C. Stahl and D. Stall, The Diophantine equation $y^2+k=x^3$, J. Number Theory 4 (1972) 107-117.

[7] A.K. Lenstra, H.W. Lenstra jr., L. Lovász, Factoring polynomials with rational coefficients, Math. Annalen 261 (1982) 215-217.

[8] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Text 106, Springer, New York-Boston-Heidelberg-Tokyo, 1986.

[9] R. Steiner, On Mordell's equation $y^2-k=x^3$: a problem of Stolarsky, Math. Comp. 46 (1986) - .