Astérisque

JOSEPH H. SILVERMAN

Counting integer and rational points on varieties

Astérisque, tome 228 (1995), p. 223-236

<http://www.numdam.org/item?id=AST_1995__228__223_0>

Counting Integer and Rational Points on Varieties

Joseph H. Silverman*

Let

$$V/\mathbb{Q} \text{ be any variety.}$$

In other words, $V/\mathbb{Q}$ is a system of polynomial equations

$$P_i(X_1, \ldots, X_n) = 0, \qquad 1 \le i \le r, \tag{$*$}$$

where the polynomials have coefficients in $\mathbb{Q}$. We will be interested in studying the set

$$\begin{aligned} V(\mathbb{Q}) &= (\text{set of rational points on V}) \\ &= (\text{set of simultaneous solutions to the system } (*) \text{ with } X_i \in \mathbb{Q}), \end{aligned}$$

and also in some cases the set

$$\begin{aligned} V(\mathbb{Z}) &= (\text{set of integer points on V}) \\ &= (\text{set of simultaneous solutions to the system } (*) \text{ with } X_i \in \mathbb{Z}). \end{aligned}$$

The problem of describing the sets $V(\mathbb{Q})$ and $V(\mathbb{Z})$ is the central problem in the study of **Diophantine Equations**.

There are lots of good questions one can ask about a Diophantine set

$$\mathcal{D} = V(\mathbb{Q}) \qquad \text{or} \qquad \mathcal{D} = V(\mathbb{Z}),$$

for example:

[1] Is $\mathcal{D}$ finite?

[2] Is $\mathcal{D}$ Zariski dense in V? Is $\mathcal{D}$ dense in $V(\mathbb{R})$ taken with the real topology?

[3] Assuming $\mathcal{D}$ is infinite, how "large" a set is it?

* This article is an expanded version of a talk given at Columbia University, Dec. 2, 1991.

AMS Classification — Primary: 11G35, Secondary: 14G25, 11D85.

Positive answers to question [1] are known for subvarieties of abelian varieties (Faltings), affine curves (Thue, Siegel), and certain higher dimensional affine varieties (Schmidt, Faltings). The first part of question [2] is answered by a powerful conjecture of Vojta, and in an earlier talk Mazur discussed possible answers to the second part. In this talk I would like to describe some of what is known and what is conjectured concerning question [3]. In other words, assuming that $V(\mathbb{Q})$ and/or $V(\mathbb{Z})$ is infinite, I want to measure how "large" it is in some quantitative way.

To illustrate what this means, we'll start with the simplest example imaginable, namely

$$V/\mathbb{Q} \text{ is the system of 0 equations in 1 variable.}$$

In other words, V is the affine line $\mathbb{A}^1$. Then

$$\mathbb{A}^1(\mathbb{Z}) = \{X \in \mathbb{Z} : X \text{ satisfies no relations}\} = \mathbb{Z}.$$

Clearly $\#\mathbb{A}^1(\mathbb{Z}) = \infty$, so a reasonable way to describe the "size" of $\mathbb{A}^1(\mathbb{Z})$ is to use the counting function

$$N\bigl(\mathbb{A}^1(\mathbb{Z}), B\bigr) \overset{\text{def}}{=} \#\bigl\{X \in \mathbb{Z} : |X| \le B\bigr\}.$$

Clearly we have

$$N\bigl(\mathbb{A}^1(\mathbb{Z}), B\bigr) = 2[B] + 1 = 2B + O(1),$$

and the fact that $N\bigl(\mathbb{A}^1(\mathbb{Z}), B\bigr)$ grows like $2B$ gives a reasonable measure of the size of $\mathbb{A}^1(\mathbb{Z})$.

Of course, we don't have to stick with $\mathbb{Q}$ and $\mathbb{Z}$, although I will for much of this talk. But for example if we look at the same variety and count points in the Gaussian integers $\mathbb{Z}[i]$, we have

$$\begin{aligned} N\bigl(\mathbb{A}^1(\mathbb{Z}[i]), B\bigr) &\overset{\text{def}}{=} \#\bigl\{X \in \mathbb{Z}[i] : |X| \le B\bigr\} \\ &= \#\bigl\{(x,y) \in \mathbb{Z}^2 : x^2 + y^2 \le B^2\bigr\} \\ &= \pi B^2 + O(B). \end{aligned}$$

(Better error estimates are available, but we won't concern ourselves with such matters.)

Now suppose we are interested in rational points? It clearly makes no sense to try to count $\mathbb{A}^1(\mathbb{Q}) = \mathbb{Q}$ by counting

$$\#\bigl\{X \in \mathbb{Q} : |X| \le B\bigr\},$$

since there are infinitely many rational points with absolute value less than B. So we want a better way to measure how large a rational number is, which leads to the notion of height. The *height of a rational number* z is

$$H(z) = H\left(\frac{a}{b}\right) \overset{\text{def}}{=} \max\{|a|,|b|\} \qquad \text{for } z = \frac{a}{b} \in \mathbb{Q} \text{ with } \gcd(a,b) = 1.$$

Then it is a nice exercise to show that the counting function for $\mathbb{A}^1(\mathbb{Q})$ is

$$N(\mathbb{A}^1(\mathbb{Q}),B) \overset{\text{def}}{=} \#\{X \in \mathbb{Q} : H(X) \le B\} \sim \frac{12}{\pi^2}B^2 \qquad \text{as } B \to \infty.$$

More generally, we can think of our variety V as a subset of projective space $\mathbb{P}^n$, so in order to define the height of a point in $V(\mathbb{Q})$, we just need to define the height of points in $\mathbb{P}^n(\mathbb{Q})$. This is easy. The *height of a point* $P \in \mathbb{P}^n(\mathbb{Q})$ is

$$H(P) = H([x_0,\dots,x_n]) \overset{\text{def}}{=} \max\{|x_0|,\dots,|x_n|\} \qquad \text{for } P = [x_0,\dots,x_n] \text{ with } x_i \in \mathbb{Z},\ \gcd(x_i) = 1.$$

We can now define the *counting function of the variety* $V \subset \mathbb{P}^n$ to be

$$N(V(R),B) \overset{\text{def}}{=} \#\{P \in V(R) : H(P) \le B\}.$$

Here R could be $\mathbb{Q}$ or $\mathbb{Z}$, or more generally it could be a number field K or ring of S-integers in K. Of course, to do this I need to define the height of a point in $\mathbb{P}^n(K)$. The definition is as follows, but if you haven't seen it before, you should ignore it and just stick with the case $R = \mathbb{Q}$ or $\mathbb{Z}$:

$$H(P) = H([x_0,\dots,x_n]) \overset{\text{def}}{=} \prod_{v \in M_K} \max_i\{|x_i|\}^{[K_v:\mathbb{Q}_v]} \qquad \text{for } P = [x_0,\dots,x_n] \in \mathbb{P}^n(K).$$

GOAL: Describe the asymptotic behavior of the counting function $N(V(R),B)$ as $B \to \infty$ in terms of elementary geometric invariants of the variety V and elementary arithmetic invariants of the ring R.

The counting function for $\mathbb{P}^n(K)$ was described by Schanuel in 1979:

Theorem. (Schanuel [**10**])

$$N\bigl(\mathbb{P}^n(K), B\bigr) \sim \frac{hR/w}{\zeta_K(n+1)} \left(\frac{2^{r_1}(2\pi^{r_2}}{d_K^{1/2}}\right)^{n+1} (n+1)^{r_1+r_2-1} B^{n+1}.$$

Here $h, R, w, r_1, r_2, d_K, \zeta_K$ are the usual quantities (class number, regulator, number of roots of unity, number of real and complex embeddings, absolute discriminant, zeta function) associated to the number field K.

In particular, if we take $K = \mathbb{Q}$ then

$$h = 1,\ R = 1,\ w = 2,\ r_1 = 1,\ r_2 = 0,\ d_{\mathbb{Q}} = 1,$$

so

$$N\bigl(\mathbb{P}^n(\mathbb{Q}), B\bigr) \sim \frac{2^n}{\zeta(n)} B^{n+1};$$

and taking $n = 1$ we recover the exercise mentioned above,

$$N\bigl(\mathbb{A}^1(\mathbb{Q})\, B\bigr) = N\bigl(\mathbb{P}^1(\mathbb{Q})\, B\bigr) - 1 \sim \frac{2}{\zeta(2)} B^2 = \frac{12}{\pi^2} B^2.$$

Why is it true that $\mathbb{P}^n$ has a lot of rational points? In some sense, it is because there is a very large group acting on $\mathbb{P}^n(K)$, namely $\mathrm{Aut}_K(\mathbb{P}^n) = \mathrm{PGL}_{n+1}(K)$. A natural generalization of $\mathbb{P}^n$ is the Grassman variety

$$G(m, n) = (\text{collection of } m\text{-dimensional linear subspaces of } \mathbb{A}^n).$$

Thus for example $\mathbb{P}^n = G(1, n+1)$. There is a natural way to write $G(m, n)$ as a variety in $\mathbb{P}^{\binom{n}{m}-1}$ given by what are known as Plücker coordinates; in the following theorem we take $G(m, n)$ with this embedding into projective space.

Theorem. (Schmidt 1968 [**11**] for $K = \mathbb{Q}$, Thunder 1990 [**14**] for arbitrary K)

$$N\bigl(G(m, n)(K), B\bigr) \sim c_{m,n,K} B^n,$$

where $c_{m,n,K}$ is an explicitly given (quite complicated) constant.

The proofs of Schmidt and Thunder follow along the lines used by Schanuel, but are considerably more complicated. One can look more generally at homogeneous spaces, which will have large automorphism groups. Two recent results along these lines are the following.

Theorem.
(a) (Franke, Manin, Tschinkel 1989 [6]) *Let G be a semi-simple algebraic group over K, let P be a parabolic subgroup, and let $V = P\backslash G$ be the associated generalized flag manifold. Choose an embedding $V \subset \mathbb{P}^n$ with the property that the hyperplane section H is linearly equivalent to $-sK_V$ for some positive integer s. Then there is an integer $t \geq 0$ such that*

$$N\big(V(K), B\big)^s \sim c_V B(\log B)^t.$$

(b) (Duke, Rudnick, Sarnak 1991 [5]) *Let G be a linear semi-simple algebraic group over $\mathbb{Q}$, let $H \subset G$ be a reductive subgroup (with certain additional properties), and let $V = H\backslash G$. Then there are constants $a > 0$, $b \geq 0$, $c > 0$ such that*

$$N\big(V(\mathbb{Z}), B\big) \sim cB^a(\log B)^b.$$

Both of these results require fairly heavy machinery for their proofs. Notice that the variety $P\backslash G$ in (a) is projective, so one counts rational points, while the variety $H\backslash G$ in (b) is affine, so one counts integral points.

All of the varieties we've considered so far have had a lot of rational points, in the sense that $N\big(V(K), B\big)$ grows like a positive power of B. For such varieties it is natural to look at the quantity

$$\beta = \beta\big(V(K)\big) \stackrel{\text{def}}{=} \lim_{B\to\infty} \frac{\log N\big(V(K), B\big)}{\log B},$$

assuming that this quantity exists. Thus β measures how large $V(K)$ is in the sense that for every $\varepsilon > 0$ we have

$$B^{\beta-\varepsilon} \ll N\big(V(K), B\big) \ll B^{\beta+\varepsilon} \qquad \text{for } B \gg 1.$$

We also remark that if β exists and $V(K)$ is infinite, then β will be equal to the abscissa of convergence of Manin's height zeta function

$$\sum_{P\in V(K)} H(P)^{-s}.$$

Batyrev and Manin have recently [2] described some conjectures which relate β to a geometrically defined quantity $\alpha = \alpha(V)$. I'll describe α precisely in a moment, but if you are unfamiliar with the terminology, don't worry. The main thing to remember is that $\alpha(V)$ depends only on the geometry of the variety V over the complex numbers, or equivalently on geometric properties of the complex projective manifold $V(\mathbb{C})$. Also, it is frequently possible to compute $\alpha(V)$ directly from the equations for V.

To define $\alpha(V)$, we recall that the variety V is assumed to be given as a subset of projective space $V \subset \mathbb{P}^n$. We let $H \in \operatorname{Div}(V)$ be the divisor corresponding to a hyperplane, and let $K_V \in \operatorname{Div}(V)$ be a canonical divisor. Further let $\operatorname{NS}(V)$ be the Néron-Severi group of V, which is the group of divisors modulo algebraic equivalence. Then

$$\alpha(V) \overset{\text{def}}{=} \inf\{r \in \mathbb{R} : rH + K_V \text{ is in the effective cone of } \operatorname{NS}(V) \otimes \mathbb{R}\}.$$

Notice that $\alpha(V)$ is reminiscent of the quantities that come up in Nevanlinna theory and in Vojta's conjectures.

Conjecture. (Batyrev, Manin 1990 [**2**])
(a) *For every $\varepsilon > 0$ there is a non-empty Zariski open subset $U \subset V$ such that*

$$\beta\big(U(K)\big) \leq \alpha(V) + \varepsilon.$$

(b) *Suppose that the canonical divisor K_V is not in the closure of the cone of effective divisors in $\operatorname{NS}(V) \otimes \mathbb{R}$. Then there exists a non-empty Zariski open subset $U \subset V$ and a finite extension K'/K such that*

$$\beta\big(U(K')\big) = \alpha(V).$$

For example, on $\mathbb{P}^n$ we have

$$K_{\mathbb{P}^n} = (-n-1)H, \quad \text{so } \alpha(\mathbb{P}^n) = n+1.$$

On the other hand, Schanuel's theorem says that

$$N\big(\mathbb{P}^n(K), B\big) \sim c_{n,K}B^{n+1}, \quad \text{so } \beta\big(\mathbb{P}^n(K)\big) = n+1.$$

Thus in this case we have $\alpha = \beta$, which verifies the Batyrev-Manin conjecture (without the necessity of taking a Zariski open subset or going to an extension field).

An interesting consequence of the Batyrev-Manin conjecture arises if one considers the case that the canonical divisor K_V is trivial, so $\alpha(V) = 0$. One deduces that for every $\varepsilon > 0$ there is a non-empty Zariski open subset $U_\varepsilon \subset V$ such that

$$\beta\big(U(K)\big) \leq \varepsilon.$$

In other words, $V(K)$ has comparatively few points. For example we might look at K3 surfaces, of which the Kummer surfaces described in Mazur's talk are a particular kind. The conjecture says that if V/K is a K3 surface, then for every $\varepsilon > 0$ there is a finite union of curves $Z \subset V$ so that

$$N\big((V \setminus Z)(K), B\big) \le B^{\varepsilon} \qquad \text{for all } B \gg 1.$$

Now it may happen that a K3 surface will contain infinitely many rational curves $Z_1, Z_2, \ldots$ (that is curves $Z_i \cong \mathbb{P}^1$). Note that each Z_i will have a counting function

$$N\big(Z_i(K), B\big) \sim c_i B^{2/d_i},$$

where d_i is the degree of the curve Z_i in $Z_i \subset V \subset \mathbb{P}^n$. This shows that the Batyrev-Manin conjecture for such K3 surfaces cannot be improved, in the sense that one cannot replace the B^{ε} by a smaller function. (See **[15]** for some recent work concerning rational points on Kummer surfaces.)

One case where the Batyrev-Manin conjecture is known to be true is that of abelian varieties. In fact, Néron used his theory of canonical heights to prove the following much more precise result.

Theorem. (Néron 1965 **[9]**) *Let $A \subset \mathbb{P}^n$ be an abelian variety defined over a number field K, and let $r = r(A, K)$ be the rank of the group of rational points $A(K)$. Then there is a constant $c = c(A, K) > 0$ such that*

$$N\big(A(K), B\big) \sim c(\log B)^{r/2} \qquad \textit{as } B \to \infty.$$

Thus not only is $\beta\big(A(K)\big) = 0$, but in fact $N\big(A(K), B\big)$ only grows like a power of $\log B$. There are other sorts of Diophantine equations which exhibit this kind of $\log B$ growth. The simplest example is Pell's equation

$$V : x^2 - Dy^2 = 1,$$

where D is a positive square-free integer. As is well-known, every integer solution in $V(\mathbb{Z})$ is obtained from a single primitive solution, and it is easy to verify that

$$N\big(V(\mathbb{Z}), B\big) \sim c \log B.$$

More generally, if the rational or integral points on a variety form a finitely generated abelian group, then they satisfy estimates similar to the estimate given in Néron's theorem.

So far we have seen varieties whose counting functions grow like a power of B and varieties whose counting functions grow like a power of $\log B$. And of course, there are varieties whose counting functions are bounded (i.e. varieties with finitely many rational points). I would like to ask if these three cases give the only sort of behavior possible. To make this precise, I need to explain what I mean when I say that "a function $f(B)$ grows like a power of B". A reasonable interpretation is that

$$\lim_{B\to\infty} \frac{\log\log f(B)}{\log\log B} = 1.$$

In any case, if $f(B) \sim cB^a(\log B)^b$ with $a > 0$, then $f(B)$ will satisfy this condition. Similarly, if $f(B)$ grows like a power of $\log B$, then it will satisfy

$$\lim_{B\to\infty} \frac{\log\log f(B)}{\log\log\log B} = 1.$$

This leads me to ask the following question (which is certainly not a conjecture, since I have virtually no evidence. Some, however, might for that reason consider it to be a provocation rather than a question!):

Question. *Let $V/\mathbb{Q}$ be a variety. Is it true that V satisfies one of the following three properties?*

(i) $$N\bigl(V(\mathbb{Q}),B\bigr) = O(1) \quad \textit{as } B \to \infty \textit{ (i.e. } V(\mathbb{Q}) \textit{ is finite).}$$

(ii) $$\lim_{B\to\infty} \frac{\log\log N\bigl(V(\mathbb{Q}),B\bigr)}{\log\log B} = 1.$$

(iii) $$\lim_{B\to\infty} \frac{\log\log N\bigl(V(\mathbb{Q}),B\bigr)}{\log\log\log B} = 1.$$

*More generally, is this true with $V(\mathbb{Q})$ replaced by $V(R)$, where V/K is any (quasi-projective) variety defined over a number field K and R is any subring of K. (For more details and a more precise version of this question, see [**12**].)*

I would like to conclude by discussing a very classical family of Diophantine equations whose solutions in integers can be completely described, but whose counting functions are still quite mysterious. We consider first the *Markoff equation*

$$V_3 : X^2 + Y^2 + Z^2 = 3XYZ.$$

(The subscript on V refers to the number of variables.) This equation has the obvious solution $(1, 1, 1)$; and given any solution (x, y, z) there are trivial ways to produce new solutions such as permuting the coordinates or changing the signs of two of the coordinates. But there is another, less obvious, way to produce a new integer solution from a given one. Here's how. Given an integer solution (x, y, z), if we substitute $X = x$ and $Y = y$ into the equation

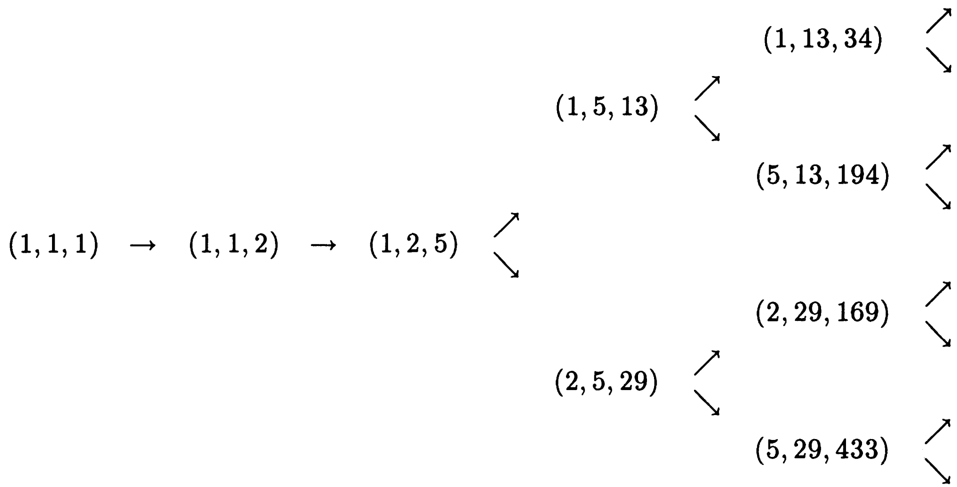

Figure 1

for V_3 we get a monic quadratic equation in Z one of whose roots is $Z = z$. The other root $Z = z'$ will also be an integer, and then (x, y, z') is our new point. Carrying out this procedure, we see that we get a map (in fact, an involution)

$$\phi : V_3(\mathbb{Z}) \longrightarrow V_3(\mathbb{Z}), \qquad (x, y, z) \longmapsto (x, y, 3xy - z).$$

Theorem. (Markoff 1880 [8]) *Every point in $V_3(\mathbb{Z})$ other than $(0,0,0)$ can be obtained from $(1,1,1)$ by applying permutations, sign changes, and the map ϕ.*

The proof of Markoff's theorem is quite easy. One shows that if $P = (x, y, z)$ satisfies $0 < x \le y < z$, then the Z-coordinate of $\phi(P)$ is strictly less than z. This allows one to descend to the case that $0 < x \le y = z$, and then the equation for V_3 shows that one has arrived at $(1,1,1)$.

In order to count the integer solutions to the Markoff equation, it suffices to count the solutions satisfying $0 < x < y < z$ (and then take into account the 6 permutations and 3 sign changes). These normalized solutions form the tree pictured in Figure 1. Cohn [4] gave $\gg\ll$ estimates for $N\bigl(V_3(\mathbb{Z}), B\bigr)$, and Zagier strengthened these to give the following asymptotic formula:

Theorem. (Zagier 1982 [16]) *There is a constant $c_3 \approx 3.253$ such that the counting function for the Markoff equation V_3 satisfies*

$$N\bigl(V_3(\mathbb{Z}), B\bigr) \sim c_3(\log B)^2 \qquad \textit{as } B \to \infty.$$

It was noted by Hurwitz in 1907 [7] that Markoff's technique allows one to find all integer solutions to the more general equation

$$V_n : X_1^2 + X_2^2 + \cdots + X_n^2 = nX_1X_2\cdots X_n.$$

In other words, all of $V_n(\mathbb{Z})$ can be obtained from the initial point $(1,1,\ldots,1)$ by applying permutations, sign changes, and the map

$$(x_1, x_2, \ldots, x_n) \longmapsto (x_1, x_2, \ldots, x_{n-1}, nx_1x_2\cdots x_{n-1} - x_n).$$

Based on Zagier's result, one might guess that the counting function for $V_n(\mathbb{Z})$ would grow like $(\log B)^{n-1}$, but in fact this is not the case, as was recently shown by Baragar.

Theorem. (Baragar 1991 [1])
(a) *Suppose that the counting function for V_4 grows like*

$$N\bigl(V_4(\mathbb{Z}), B\bigr) \sim c_4(\log B)^\alpha$$

for some constants $c_4 > 0$ and $\alpha > 0$. Then

$$2.38 < \alpha < 2.8.$$

In particular, $N\bigl(V_4(\mathbb{Z}), B\bigr)$ does not grow like $(\log B)^3$.
(b) *More generally, suppose that the counting function for V_n grows like*

$$N\bigl(V_n(\mathbb{Z}), B\bigr) \sim c_n(\log B)^{\alpha(n)}$$

for some constants $c_n > 0$ and $\alpha(n) > 0$. Then

$$1.45\log n - 1 \le \alpha(n) \le 3.7\log n.$$

Numerical evidence compiled by Baragar suggests that $\alpha(4) \approx 2.44$. It is not at all clear what $\alpha(4)$ should be, so I will leave you with one final question:

Is it conceivable that

$$N\bigl(V_4(\mathbb{Z}), B\bigr) \sim c_4(\log B)^\alpha$$

for some *irrational* number α?

Addendum I: Counting Geometrically Generated Points

On certain varieties it is possible to describe the counting function for geometrically generated subsets of $V(K)$, even though the counting function for $V(K)$ itself remains intractable. We briefly describe two examples.

Suppose that V is an elliptic surface, which means that there is a morphism $\pi : V \to C$ to a smooth curve C such that almost every fiber of π is an elliptic curve. Then the group of sections $C \to V$ (defined over K) forms a finitely generated abelian group which we will denote by $V(C)$. If $\sigma : C \to V$ is any section to π, then we get rational points on V by applying σ to rational points on C,

$$\sigma\bigl(C(K)\bigr) \subset V(K).$$

Doing this for every section, we get a subset of $V(K)$ which we will denote by

$$V^{\mathrm{sect}}(K) \overset{\mathrm{def}}{=} \bigl\{\sigma(t) : \sigma \in V(C) \quad \text{and} \quad t \in C(K)\bigr\}.$$

If C has genus at least 2, then $C(K)$ is finite, so the subset $V^{\mathrm{sect}}(K)$ will not be very interesting. (In particular, it will not be Zariski dense.) On the other hand, if C has genus 0, then the image of every section has so many rational points that the counting function $V^{\mathrm{sect}}(K)$ looks like the counting function for $\mathbb{P}^1$. So the interesting case is when C has genus 1, which means that both $C(K)$ and $V(C)$ are finitely generated abelian groups. They then interact with each other in a non-trivial way as described in the following result of Greg Call.

Theorem. (Call 1984 [**3**]) *Let $V \to C$ be an elliptic surface defined over a number field K, let $V(C)$ be the group of sections defined over K, and let $V^{\mathrm{sect}}(K)$ be the subset of $V(K)$ consisting of those points which lie on a section. Assume further that C has genus 1, so its group of rational points $C(K)$ is a finitely generated group, and let*

$$r(V) = \operatorname{rank} V(C) \qquad \textit{and} \qquad r(C) = \operatorname{rank} C(K).$$

Then

$$N\bigl(V^{\mathrm{sect}}(K), B\bigr) \gg\ll \begin{cases} (\log B)^{\frac{1}{2}\max\{r(V),r(C)\}} & \textit{if } r(V) \neq r(C), \\ (\log B)^{\frac{1}{2}r(V)} \log\log B & \textit{if } r(V) = r(C). \end{cases}$$

For our second example of geometrically generated points, consider a surface V inside $\mathbb{P}^2 \times \mathbb{P}^2$ described by the intersection of a $(1,1)$-form and a $(2,2)$-form. Thus V is given by two homogeneous equations

$$V : \sum_{i,j=1}^{3} a_{ij} x_i y_j = \sum_{i,j,k,l=1}^{3} b_{ijkl} x_i x_j y_k y_l = 0.$$

This surface is another example of a K3 surface. The projections $\pi_1, \pi_2 : V \to \mathbb{P}^2$ are double covers, so there are associated involutions $\sigma_1, \sigma_2 : V \to V$. Let $\mathcal{A}$ be the subgroup of $\operatorname{Aut}(V)$ generated by σ_1 and σ_2. It is not hard to prove that $\mathcal{A}$ is isomorphic to the free product $(\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/2\mathbb{Z})$, so in particular it is infinite. One then checks that for most points $P \in V(K)$, the orbit

$$\mathcal{A}P \overset{\text{def}}{=} \{\phi P : \phi \in \mathcal{A}\}$$

is likewise infinite. The following result shows that the points in any such orbit are extremely sparse (although one expects that $V(K)$ will contain infinitely many distinct orbits).

Theorem. (Silverman 1991 [**13**]) *Let $P \in V(K)$ be a rational point on the K3 surface described above, and assume that the orbit $\mathcal{A}P$ is infinite. Further let*

$$f_P = \begin{cases} 2 & \textit{if no non-zero element of } \mathcal{A} \textit{ fixes } P, \\ 1 & \textit{if some non-zero element of } \mathcal{A} \textit{ fixes } P. \end{cases}$$

Then

$$N(\mathcal{A}P, B) = \frac{f_P}{\log(2+\sqrt{3})} \log\log B + O(1).$$

Addendum II: The Circle Method

As the referee has kindly pointed out, the circle method provides another powerful technique for counting integral points on varieties. For example, Birch (*Proc. Royal Academy* 1962) has shown that if $P_1, \dots, P_r$ are polynomials of degree d in $\mathbb{Z}[X_1, \dots, X_n]$, if the corresponding variety V is not too singular, and if n is very large compared to d and r, then the counting function for V has the form

$$N(V(\mathbb{Z}), B) \sim c_V B^{n-rd}.$$

There is a similar statement for projective varieties. Note that this formula is compatible with the conjecture of Batyrev and Manin, since the canonical divisor on V is $K_V \sim (n-rd)H$.

Acknowledgements

I would like to thank Greg Call, Barry Mazur, and the referee for their helpful suggestions which greatly improved the original draft of this article.

References

1. Baragar, A.: Asymptotic growth of Markoff-Hurwitz numbers. Compositio Math. to appear
2. Batyrev, V.V., Manin, Y.: Sur le nombre des points rationnels de hauteur borné des variétés algébriques. Math. Ann. **286**, 27–43 (1990)
3. Call, G.: Counting Geometric Points on Families of Abelian Varieties. Math. Nach. to appear
4. Cohn, H.: Growth types of Fibonacci and Markoff. Fibonacci Quart. **17**, 178–183 (1979)
5. Duke, W., Rudnick, Z., Sarnak, P.: Density of integer points on affine homogeneous varieties. to appear
6. Franke, J., Manin, Y., Tschinkel, Y.: Rational points of bounded height on Fano varieties. Invent. Math. **95**, 421–435 (1989)
7. Hurwitz, A.: Über eine Aufgabe der unbestimmten Analysis. Archiv. Math. Phys. **3**, 185–196 (1907)
8. Markoff, A.A.: Sur les formes binaires indéfinies. Math. Ann. **17**, 379–399 (1880)
9. Néron, A.: Quasi-fonctions et hauteurs sur les variétés abéliennes. Annals of Math. **82**, 249–331 (1965)
10. Schanuel, S.: Heights in number fields. Bull. Soc. Math. France **107**, 433–449 (1979)
11. Schmidt, W.: Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. Duke Math. J. **35**, 327–339 (1968)
12. Silverman, J.H.: Integral points on curves and surfaces. H.P. Schlickewei & E. Wirsing (Eds.), Number Theory, Ulm 1987, 202–241 Lecture Notes in Math.. New York: Springer-Verlag 1989
13. Silverman, J.H.: Rational points on K3 surfaces: A new canonical height. Invent. Math. **105**, 347–373 (1991)
14. Thunder, J.: An asymptotic estimate for heights of algebraic subspaces. Trans. AMS **331**, 395–424 (1992)
15. Todorov, A.: The number of rational points on some Kummer surfaces. to appear

16. Zagier, D.: On the number of Markoff numbers below a given bound. Math. Comp. **39**, 709–723 (1982)

Joseph H. Silverman
Mathematics Department
Brown University
Providence, RI 02912 USA
⟨jhs@gauss.math.brown.edu⟩