Integral points on punctured abelian surfaces

Andrew Kresch and Yuri Tschinkel

[1] Department of Mathematics,
University of Pennsylvania,
Philadelphia, PA 19104,
kresch@math.upenn.edu
[2] Department of Mathematics,
Princeton University,
Princeton, NJ 08544,
ytschink@math.princeton.edu

Abstract. We study the density of integral points on punctured abelian surfaces. Linear growth rates are observed experimentally.

1 Introduction

Let V be a smooth projective algebraic variety over a number field K. We now ask whether there exists a finite extension K' of K such that K'-rational points are Zariski dense. This property is called potential density of rational points, and is known to hold, e.g., for abelian varieties, certain classes of Fano varieties, and certain K3 surfaces (see [6], [1] and the references therein). Potential density is conjecturally related to global geometric invariants of V, such as the Kodaira dimension [10].

An analogous question can be asked about integral points. Let (V, Z) be a projective variety and a proper subvariety, both defined over K. Choose models $(\mathcal{V}, \mathcal{Z})$ over the ring of integers $\mathfrak{o}_K$. Let S be a finite set of non-archimedean places of K. A rational point Q on V determines a section s_Q of the structure map from $\mathcal{V}$ to $\mathrm{Spec}(\mathfrak{o}_K)$. We say that the point Q is S-integral (with respect to $\mathcal{Z}$) if the section s_Q does not meet $\mathcal{Z}$ outside S. We say that integral points are potentially dense for the pair (V, Z) if there exists a finite extension K' of K, a finite set S' of non-archimedean places of K', and models $(\mathcal{V}', \mathcal{Z}')$ over $\mathrm{Spec}(\mathfrak{o}_{K'})$ of the base-changed (V', Z') such that S'-integral points on $(\mathcal{V}', \mathcal{Z}')$ are Zariski dense in V'. Concretely, this means that after a finite extension of the base field, and allowing for a finite set of bad places, a given system of integral equations for V has a Zariski dense set of integral solutions such that their reductions, outside the fixed bad places, are away from the reduction of Z (given also by integral equations).

Conjecture 1 ([7]). Let V be a smooth algebraic variety whose rational points are potentially dense. Then integral points are potentially dense with respect to any codimension ≥ 2 subvariety $Z \subset V$.

This conjecture holds, e.g., for toric varieties and Del Pezzo surfaces [7]. Conversely, knowing potential density of integral points for certain varieties, we may deduce potential density of rational points in many new cases. For instance, Conjecture 1 implies potential density for rational points on general K3 surfaces (see [7]). An important test of the above conjecture is the case of punctured abelian varieties (that is, pairs (J, Z), where J is an abelian variety and $Z \subset J$ a codimension ≥ 2 subvariety).

For punctured abelian surfaces potential density is only known when the abelian surface is special (e.g., isogenous to products of elliptic curves, or admitting extra endomorphisms, see [7]). Here we study the case of simple abelian surfaces J over $\mathbb{Q}$, punctured at one rational point (which we may as well take to be the identity) and having a point $Q \in J(\mathbb{Q})$ of infinite order. We carry out a simple numerical experiment which strongly suggests that integral points on punctured abelian surfaces are not only Zariski dense, but moreover constitute a positive proportion of the multiples of Q. It would be interesting to have a conceptual interpretation of the proportionality constant.

Acknowledgments. The authors would like to thank Fedor Bogomolov, Bredan Hassett, Barry Mazur and Joe Shalika for inspiring discussions. We especially thank Michael Stoll for a careful reading of the paper and for many useful suggestions. We have used the packages `magma` and `maple`. The first author was supported in part by a National Science Foundation Postdoctoral Research Fellowship, and the second author was supported in part by the Clay Foundation and the National Science Foundation.

2 Divison polynomials in genus 2

Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $2g + 1$ with no multiple factors and C the hyperelliptic curve (over $\mathbb{Z}$), defined by the equation

$$Y^2 = f(X).$$

Let (x, y) be a $\mathbb{Q}$-rational point on C, with $y \neq 0$, and let $Q := [(x, y) - \infty]$ be the corresponding point on the Jacobian $J = J(C)$. Denote by $\Theta = \Theta(J)$ the Θ-divisor. Cantor [2] has described a convenient algorithm for generating division polynomials $\psi_r(x)$ which vanish if and only if $r \cdot Q \in \Theta$. Moreover, $r \cdot Q = 0$ in J if and only if $\psi_{r'}(x) = 0$ for all r' with $|r' - r| \leq g - 1$. These polynomials give an efficient means of testing at which primes a given multiple of Q reduces to the identity in (the reduction modulo some prime of) the Jacobian.

Before stating basic facts about division polynomials, let us recall how to represent a point on a Jacobian. From now on we specialize to the case $g = 2$. Every point on J is expressible in the form $D - 2 \cdot \infty$ for an effective degree 2 cycle D on C, and D is unique except in the case of the zero element of J. The

point $r \cdot Q$ can be put into this form by solving for polynomials $A(X)$ and $B(X)$ such that $A(X) - B(X)y$ vanishes to order r at Q, subject to degree bounds $\deg A \leq \lfloor (r+2)/2 \rfloor$ and $\deg B \leq \lfloor (r-3)/2 \rfloor$. Then $r \cdot Q \in \Theta$ is equivalent to the vanishing of the leading coefficient of A in the case r is even, or of B in the case r is odd. Cantor shows that one can produce universal polynomials A and B, whose coefficients are integer polynomials in the coefficients of f and in x (and y).

Concretely, let us continue to assume that f has coefficients in $\mathbb{Z}$. Cantor's algorithm generates polynomials $P_r(x)$ and $\psi_r(x)$ such that:

(i) $P_r(x) = 0$ if and only if $r \cdot Q \in \Theta$ (for all x in the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$), $\deg P_r = r^2 - 4$ when r is even, and $\deg P_r = r^2 - 9$ when r is odd (this specifies P_r uniquely, up to a scalar multiple).

(ii) Define $\psi_r(x)$ to be proportional to $P_r(x)$ when r is even and to $f(x)P_r(x)$ when r is odd, and to have leading coefficient $\binom{r+1}{3}$; then $\psi_r(x)$ is an integer-coefficient polynomial of degree $r^2 - 4$.

(iii) The ψ_r satisfy the following recurrence relation:

$$\psi_r \psi_s \psi_{s+r} \psi_{s-r} = \det \begin{pmatrix} \psi_{s-2}\psi_r & \psi_{s-1}\psi_{r+1} & \psi_s \psi_{r+2} \\ \psi_{s-1}\psi_{r-1} & \psi_s \psi_r & \psi_{s+1}\psi_{r+1} \\ \psi_s \psi_{r-2} & \psi_{s+1}\psi_{r-1} & \psi_{s+2}\psi_r \end{pmatrix} \tag{1}$$

for any $s \geq r$.

The recurrence (1) determines ψ_r for all $r \geq 8$, given $\psi_1 = 0$, $\psi_2 = 1$, ..., ψ_7. One can effectively determine the universal polynomials ψ_3, ..., ψ_7 by solving for the coefficients of the polynomials $A(X)$ and $B(X)$ mentioned previously, for each $r \leq 7$. This is achieved economically by introducing a new variable v given by $vf(x) = x - X$. Then $\sqrt{f(X)/f(x)}$ is a power series in v which is easily computed (for reason of convention, the branch $-1 + \cdots$ of the square root is chosen for $g = 2$). Then one is reduced to solving

$$v^r \mid a(v) - b(v)\sqrt{f(X)/f(x)} \tag{2}$$

for polynomials $a(v)$ and $b(v)$ satisfying the same degree bounds as above (a differs from A by the change of variable, and b differs from B by the change of variable and multiplication by y). In particular, $a(0)+b(0) = 0$. We have $a(0) = 0$ for given $x \in \overline{\mathbb{Q}}$ if and only if $P_{r-1}(x) = 0$, and we can take $-a(0) = b(0) = P_{r-1}$. This means that for $r \leq 6$, (2) reduces to solving at most one equation for one unknown coefficient, and this is easily solved. For instance, ψ_4 is displayed in Table 1. For $r = 7$, the two unknown coefficients of the quadratic polynomial $b(v)$ must be solved for.

3 Results

We performed the following numerical experiment. Start with a curve C of genus 2 defined by $Y^2 = f(X)$, where $f(X)$ is a monic degree-5 polynomial with

$$
\begin{aligned}
f(X) &= X^5 + \alpha X^4 + \beta X^3 + \gamma X^2 + \delta X + \varepsilon,\\
\psi_4(x) &= 10x^{12} + 24\alpha x^{11} + (26\beta + 16\alpha^2)x^{10} + 20(2\alpha\beta + \gamma)x^9\\
&\quad + 10(4\alpha\gamma + 3\beta^2 - \delta)x^8 + 80(\beta\gamma - \varepsilon)x^7\\
&\quad + (-112\alpha\varepsilon + 68\beta\delta + 64\gamma^2 + 8\alpha\beta\gamma - 2\beta^3 - 16\alpha^2\delta)x^6\\
&\quad + (-4\beta^2\gamma - 8\beta\varepsilon - 64\alpha^2\varepsilon - 8\alpha\beta\delta + 16\alpha\gamma^2 + 152\gamma\delta)x^5\\
&\quad + 10(-8\alpha\beta\varepsilon + 4\alpha\gamma\delta + 11\delta^2 + 12\gamma\varepsilon - \beta^2\delta)x^4\\
&\quad + 40(\alpha\delta^2 - \beta^2\varepsilon + 6\delta\varepsilon)x^3 + 10(\beta\delta^2 + 16\varepsilon^2 - 4\beta\gamma\varepsilon + 8\alpha\delta\varepsilon)x^2\\
&\quad + (8\beta\delta\varepsilon - 16\gamma^2\varepsilon + 64\alpha\varepsilon^2 + 4\gamma\delta^2)x + 16\beta\varepsilon^2 - 8\delta\gamma\varepsilon + 2\delta^3.
\end{aligned}
$$

Table 1. The universal $\psi_4(x)$

integral coefficients. Assume that the Jacobian J is simple, has Mordell-Weil rank 1 (over $\mathbb{Q}$), and that there is an integral point (x, y) such that $Q = [(x, y) - \infty]$ has infinite order in J.

Let S be the set of prime divisors of $2\,y\,\mathrm{disc}(f)$. Now the curve reduces well modulo all primes not in S, and we have an integral model for J over $\mathrm{Spec}(\mathbb{Z})\smallsetminus S$, with an S-integral point Q disjoint from the zero section. We count positive integers r such that $r \cdot Q$ is as well disjoint from the zero section (again, over the complement of S); such r will be called *good*. For $r \cdot Q$ to be disjoint from zero outside S is equivalent to $\psi_{r-1}(x)$, $\psi_r(x)$, and $\psi_{r+1}(x)$ having no common prime factors outside S. A table is made of the density of the good integers r. Amazingly, we observe linear growth.

Remark 1. The significance of any sort of growth is that the set of good integers being infinite implies Zariski density of S-integral points on the punctured J (here we use the fact that J is simple).

We describe the procedure in detail for one curve, and then present tables giving the data from several curves.

The curve C_1 given by

$$y^2 = x^5 - 14x^4 + 65x^3 - 112x^2 + 60x$$

has rational point $(3, 6)$, and its Jacobian J_1 satisfies $J_1(\mathbb{Q}) = \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^4$ (see [4]). Here $S = \{2, 3, 5\}$. Then we have (at $x = 3$)

$$
\begin{aligned}
\psi_3 = 144, \qquad \psi_4 = -41472, \qquad \psi_5 = 585252864,\\
\psi_6 = -35588725014528, \qquad \psi_7 = 5004999490025816064.
\end{aligned}
$$

Notice that 7 is a common factor of ψ_5, ψ_6, and ψ_7, so that $6 \cdot Q$ is not S-integral on the punctured J_1. Hence 6 and all its multiples are not good. The

next integer, besides multiples of 6, which fails to be good is 22. The third is 38:

$$\gcd(\psi_{37}, \psi_{38}, \psi_{39}) = 2^{854} \cdot 3^{344} \cdot 17.$$

The first two columns of Table 2 show integer ranges (1–100, ..., 901–1000) and the density of good r in each range.

range of r	density(J_1)	density(J_2)	density(J_3)	density(J_4)
1– 100	0.77	0.62	0.74	0.67
101– 200	0.69	0.63	0.70	0.67
201– 300	0.71	0.61	0.74	0.66
301– 400	0.74	0.62	0.69	0.70
401– 500	0.72	0.62	0.69	0.68
501– 600	0.72	0.63	0.74	0.67
601– 700	0.73	0.60	0.70	0.64
701– 800	0.70	0.64	0.72	0.70
801– 900	0.72	0.59	0.73	0.68
901–1000	0.72	0.63	0.69	0.67

Table 2. Densities of S-integral points on J_i

We performed a similar experiment with the following curves:

$$\begin{aligned} C_2 &: f(X) = X^5 + 9X^4 + 14X^3 - 18X^2 - 15X + 9, & (x, y) &= (0, 3), \\ C_3 &: f(X) = X^5 + 2X^4 - 3X^3 - 2X^2 + 2X, & (x, y) &= (2, 6), \\ C_4 &: f(X) = X^5 + 11X^4 + 7X^3 - 89X^2 + 2X + 88, & (x, y) &= (-7, 54). \end{aligned}$$

By a computation in [3], these are curves having Jacobians of Mordell-Weil rank 1 over $\mathbb{Q}$. It is easy to see that the Jacobians we are considering are simple over $\mathbb{Q}$ (e.g., by factoring the number of $\mathbb{F}_p$-points for suitable p). The corresponding columns of Table 2 indicate the experimentally observed densities for these Jacobians.

4 Heuristics

Let J be an abelian variety over $\mathbb{Q}$, and let Γ be the Mordell-Weil group $J(\mathbb{Q})$. Fix an integral model of J, and let S be the set of primes of bad reduction. Then, for p a prime not in S, let us denote by g_p the order of the subgroup of $J(\mathbb{F}_p)$ generated by Γ. The quantity

$$\rho(J) = \prod_{p \notin S} (1 - 1/g_p). \tag{3}$$

is a lower bound for the density of S-integral points on the punctured Jacobian. We do not know whether this product converges.

Conjecture 2. If J is simple of dimension ≥ 2 and has positive Mordell-Weil rank, then the product (3) converges.

Remark 2. Replacing Γ by a finite-index subgroup does not change the convergence of (3). Also, note that the conclusion of Conjecture 2 may fail if J is isogenous to a product of elliptic curves.

We computed the Euler products using the first 400 primes of good reduction, for the Jacobians J considered above. In our computation we used the subgroup generated by our point Q in place of the full Mordell-Weil group to obtain a quantity $\tilde{\rho}(J)$ for each Jacobian J. Numerically we observe convergence. The results are presented in Table 3.

	J_1	J_2	J_3	J_4
$\tilde{\rho}(J)$	0.576	0.404	0.538	0.516

Table 3. Values of Euler products for J_i

Remark 3. For J of dimension 2, a positive answer to Conjecture 2 would imply the density of integral points.

One can ask, for some abelian variety, how often the reduction of the cyclic group generated by a given point is the full group $J(\mathbb{F}_p)$; for elliptic curves, this question was raised by Lang and Trotter in [8]. Assuming the Generalized Riemann Hypothesis (GRH), Serre showed that for elliptic curves E, the number of primes $p \leq B$ such that $E(\mathbb{Z}/p\mathbb{Z})$ is cyclic is $\sim cB/log(B)$ (as $B \to \infty$ and for some c). Again, under GRH, the density is

$$\sum_{n \geq 1} \mu(n)/[K_n : Q],$$

where $\mu(n)$ is the Möbius function and K_n is the field generated by n-torsion points on E (see [9]). An unconditional lower bound $\gg B/log(B)^2$ (for elliptic curves with no rational 2-torsion points) has been proved by Gupta and Murty [5].

References

1. F. Bogomolov and Yu. Tschinkel, *Density of rational points on elliptic K3 surfaces*, Asian J. Math. **4** (2000), 351–368.
2. D. G. Cantor, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. **447** (1994), 91–145.
3. E. V. Flynn, *Descent via isogeny in dimension* 2, Acta Arith. **66** (1994), 23–43.
4. D. Gordon and D. Grant, *Computing the Mordell-Weil rank of Jacobians of curves of genus two*, Trans. Amer. Math. Soc. **337** (1993), 807–824.

5. R. Gupta and M. R. Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. **101** (1990), 225–235.
6. J. Harris and Yu. Tschinkel, *Rational points on quartics*, Duke Math. J. **104** (2000), 477–500.
7. B. Hassett and Yu. Tschinkel, *Density of integral points on algebraic varieties*, in: E. Peyre and Yu. Tschinkel, eds., Rational Points on Algebraic Varieties, *Progr. Math.* **199**, Birkhäuser (2001), 169–197.
8. S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), 289–292.
9. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
10. P. Vojta, Diophantine approximation and value distribution theory, Lecture Notes in Math. **1239**, Springer-Verlag, Berlin, 1987.