TOWERS OF CURVES AND RATIONAL DISTANCE SETS

DINO LORENZINI

A rational (resp. integral) distance set is a subset S of the plane $\mathbb{R}^2$ such that for all $s, t \in S$, the distance between s and t is a rational number (resp. is an integer). Huff [4] considered rational distance sets S of the following form: given distinct $a, b \in \mathbb{Q}^*$, S contains the four points $(0, \pm a)$ and $(0, \pm b)$ on the y-axis, plus points $(x, 0)$ on the x-axis, for some $x \in \mathbb{Q}^*$. Such a point $(x, 0)$ must then satisfy the equations $x^2 + a^2 = u^2$ and $x^2+b^2 = v^2$ with $u, v \in \mathbb{Q}$. The system of associated homogeneous equations $x^2+a^2z^2 = u^2$ and $x^2 + b^2z^2 = v^2$ defines a curve $C(a^2, b^2)$ of genus 1 in $\mathbb{P}^3$. Huff, and later his student Peeples [12], provided examples where the elliptic curve $C(a^2, b^2)$ has positive rank over $\mathbb{Q}$, thus exhibiting examples of infinite rational distance sets that are not contained in a line or in a circle. These remain to this day the 'largest' known such examples.

The curves of higher genus whose rational points are related to rational distance sets with $2n + 1$ distinct points on the y-axis, $(0, \pm a_1), \ldots, (0, \pm a_n)$, and $(0, 0)$, plus points $(x, 0)$ on the x-axis, form an interesting class of curves with many rational points and an often computable Mordell-Weil rank over $\mathbb{Q}$. We make some remarks on these curves and on two open problems about rational distance sets.

For any field K with $\mathrm{char}(K) \neq 2$, and for $\alpha_1, \ldots, \alpha_n \in K^*$, pairwise distinct, let $C(\alpha_1, \ldots, \alpha_n)/K$ denote the curve in $\mathbb{P}^{n+1}$ defined by the system of equations

$$x^2 + \alpha_i z^2 = y_i^2, \text{for } i = 1, \ldots, n.$$

Since $\mathrm{char}(K) \neq 2$ and the coefficients $\alpha_1, \ldots, \alpha_n$ are distinct, the curve $C(\alpha_1, \ldots, \alpha_n)/K$ is smooth. This curve has the following 2^n obvious K-rational points

$$(x : y_1 : \ldots : y_n : z) = (1 : \pm 1 : \ldots : \pm 1 : 0),$$

plus the 2^n additional K-rational points $(0 : \pm a_1 : \ldots : \pm a_n : 1)$ when $\alpha_i = a_i^2$ for all $i = 1, \ldots, n$. The genus of $C_n = C(\alpha_1, \ldots, \alpha_n)/K$ is $2^{n-1}(n - 2) + 1$. This formula can be obtained with successive applications of the Riemann-Hurwitz formula on the tower of curves

$$C(\alpha_1, \ldots, \alpha_n) \longrightarrow C(\alpha_1, \ldots, \alpha_{n-1}) \longrightarrow \ldots \longrightarrow C(\alpha_1, \alpha_2).$$

The morphism $C_n \to C_{n-1}$ has degree 2 and is branched over 2^n points.

Let us call a point $(x : y_1 : \ldots : y_n : z)$ of $C_n(\mathbb{Q})$ non-obvious if $xz \neq 0$. We shall call two non-obvious points $(x : y_1 : \ldots : y_n : z)$ and $(x' : y'_1 : \ldots : y'_n : z')$ equivalent if $(x' : y'_1 : \ldots : y'_n : z')$ is of the form $(\pm x : \pm y_1 : \ldots : \pm y_n : z)$. It is natural to ask how many non-obvious (pairwise) non-equivalent points can a curve of type $C_n = C_n(a_1^2, \ldots, a_n^2)$ have. The current record is held by Lagrange and Leech [6], p. 758, who found a curve of type C_3 with 4 such points, and a curve of type C_4 with 3 such points. It is an unsolved problem stated in [3], D20, to find a curve of type C_4 with 4 non-obvious non-equivalent points.

Date: January 2, 2006.

Proposition 1. *There exist infinite towers of curves $C_n(a_1^2,\ldots,a_n^2)$, each curve with two non-obvious and non-equivalent points, and such that*

$$\frac{|C_n(\mathbb{Q})|}{g(C_n)-1} \geq \frac{12}{n-2}.$$

Proof. Consider any elliptic curve $C(a^2,b^2)/\mathbb{Q}$ with positive rank. Let $P=(a_1:b_1:c_1:1)$ be a point of infinite order in $C(a^2,b^2)(\mathbb{Q})$, and let $mP := (a(mP):b(mP):c(mP):1)$. Note that $b(iP)c(iP)\neq 0$ for all i. Since the value $a(mP)$ can appear as the first coefficient of a point in $C(a^2,b^2)/\mathbb{Q}$ at most 8 times, we can find a subsequence, say $\{P_n=(a_n:b_n:c_n:1)\}_{n=1}^{\infty}$, of the sequence $\{mP\}$ such that the a_i^2s are all distinct. Consider the curve $C_n := C(a_1^2,\ldots,a_n^2)$. It contains the following $2\cdot 2^{n+1}$ distinct points:

$$(\pm a:\pm b_1:\ldots:\pm b_n:1) \text{ and } (\pm b:\pm c_1:\ldots:\pm c_n:1).$$

It follows that $|C_n(\mathbb{Q})|\geq 3(2^{n+1})$, as desired. ☐

Remark 2 In the tower $\{C_n\}_{n=3}^{\infty}$ presented in the proposition, there are many $\mathbb{Q}$-points at each level n such that all their preimages in any curve C_m with $m\geq n$ are all also $\mathbb{Q}$-rational. We shall say that such a point rationally splits in the tower. Clearly, if we can find a tower of curves $\{C_n\}_{n=1}^{\infty}$ with unramified morphisms $C_n\to C_{n-1}$ and a rational point which rationally splits completely, then we would have a tower with the ratio $|C_n(\mathbb{Q})|/(g(C_n)-1)$ bounded below by a constant. This problem is discussed in [2], where such towers are exhibited over certain small number fields, but not over $\mathbb{Q}$.

The asymptotic behaviour of $\mathrm{rank}(\mathrm{Jac}(C_n)(\mathbb{Q}))/g(C_n)$ is not understood, and it would be of interest to know whether $\limsup_{n\to\infty}\mathrm{rank}(\mathrm{Jac}(C_n)(\mathbb{Q}))/g(C_n)<1$.

Remark 3 Solymosi notes in [13] that it is not known whether it is possible to find, for each pair of integers n and m, an integral distance set with $m+n$ points such that a line contains exactly m of them. In fact, it would follow from a conjecture of Lang that when $n\geq 5$ and m is large enough, such a distance set cannot exist. Indeed, assume that we have such a distance set S. By translation and rotation, we can assume that the line containing the m points is the x-axis, and that one of the point of our distance set is the origin. Let $(x_i,0)$, $i=1,\ldots,m$ denote the points of S on the x-axis, with $x_m=0$. Note that $x_i\in\mathbb{Q}$. Since $n\geq 5$, we can find (a_1,b_1), (a_2,b_2), and (a_3,b_3) in S that are not on the x-axis and such that the equations $(x-a_iz)^2+b_i^2z^2=y_i^2$, $i=1,2,3$, are pairwise distinct (three distinct non-zero b_i^2). This system of equations defines a smooth curve C of genus 5 in $\mathbb{P}^3$. Since the coefficients of the points in S need not be in $\mathbb{Q}$ (see the construction in [13] after Cor. 1 for an example) we note that $(x_j-a_i)^2+b_i^2\in\mathbb{Q}$ for $j=1,2$ imply that $\mathbb{Q}(a_i,b_i^2)=\mathbb{Q}$. Thus, our curve C is defined over $\mathbb{Q}$, and $|C(\mathbb{Q})|\geq m$. It is shown in [1] that a conjecture of Lang implies that the set $\{|D(\mathbb{Q})|\}$ is bounded as $D/\mathbb{Q}$ runs over all smooth curves of a fixed genus $g\geq 2$. It would then follow that the set $|C(\mathbb{Q})|$ is bounded by a constant N independent of the equations of the curve C of genus 5, so that m is bounded.

Remark 4 Guy asks in [3], D20, conjecture (a), whether there exists an integer c such that any rational distance set of size $|S|$ is such that at least $|S|-c$ of its points lie on a line or on a circle. If this question has a positive answer, then it would follow from a conjecture of Lang that there exists an integer N such that if $|S|>N$, then $|S|-4$ points of S lie on a line or a circle. Indeed, let us first note that if a rational distance set S contains m points on a circle C, then we can find a second rational distance set S' such that $m-1$ points of S' lie on a line. To prove this fact, we choose a point P of S that lies on the given circle C, and use it as the origin for our plane. We pick as the x-axis the line passing through P and the center of C. Then every point $z:=(x,y)$ in the set S

is at a rational distance from $(0,0)$, that is, $|z| \in \mathbb{Q}$, where z is thought of as a complex number. We let $S' := \{1/z, z \in S\}$. Clearly, $|1/z - 1/w| = |z-w|/|z||w|$, so S' is also a rational distance set. Since the image of the circle C under the inversion $1/z$ is a vertical line, we find that S' contains $m-1$ points on a line (we lost one point since the inversion sends P to '∞').

Assume now that our set S contains $|S|-c$ points on a line. Suppose that $|S|-c > N$, where N is the maximal number of rational points that a curve of genus 5 can have (as explain in Remark 3, this number N exists if a conjecture of Lang holds). As in Remark 3, we conclude that $c \leq 4$, since otherwise we can construct a curve of genus 5 with more than N rational points.

Assuming that both conjecture (a) and Lang's conjecture are true, we can answer affirmatively another question raised by Guy in [3], D20. It is indeed true that $c = 4$ is the maximal possible value for c when the rational distance set is infinite.

Let K be any field with $\mathrm{char}(K) \neq 2$. The jacobian of the curve $C_n = C(\alpha_1, \ldots, \alpha_n)/K$ is isogenous to a product of hyperelliptic jacobians that we now describe explicitly. The function field $K(C_n)/K(x)$ is isomorphic to $K(x)(\sqrt{x^2+\alpha_i}, i = 1, \ldots, n)$. It contains the following quadratic subfields: for $2 \leq r \leq n$ and $1 \leq i_1 < \cdots < i_r \leq n$,

$$K(x)(\sqrt{(x^2+\alpha_{i_1}) \cdot \cdots \cdot (x^2+\alpha_{i_r})}).$$

Let $D_{(i_1,\ldots,i_r)}/K$ be the hyperelliptic curve given by the equation

$$Y^2 = (x^2+\alpha_{i_1}) \cdot \cdots \cdot (x^2+\alpha_{i_r}),$$

and consider the natural map

$$C_n \longrightarrow D_{(i_1,\ldots,i_r)},$$

where $(x : y_1 : \cdots : y_n : 1) \mapsto (x, y_{i_1} \cdots y_{i_r})$. Let G denote the group generated by the involutions $y_i \mapsto -y_i$ (the other variables remaining fixed), for $i = 1, \ldots, n$. The group G is also the Galois group of the extension $K(C_n)/K(x)$. Each quadratic extension corresponds to a maximal subgroup $H(i_1, \ldots, i_r)$ of G, so that the product of two such maximal subgroups is the whole group G. Clearly, C_n/G has genus 0.

Proposition 5. *The jacobian of C_n/K is isogenous over K to the product of the jacobians of the hyperelliptic curves $D_{(i_1,\ldots,i_r)}/K$.*

When $r > 2$, the jacobian of the hyperelliptic curve $D_{(i_1,\ldots,i_r)}/K$ is isogenous to the product of the jacobians of $Y^2 = (X+\alpha_{i_1}) \cdot \ldots \cdot (X+\alpha_{i_r})$, and of $Y^2 = X(X+\alpha_{i_1}) \cdot \ldots \cdot (X+\alpha_{i_r})$.

Proof. The first part of the proposition follows from Theorem C in [5], once we show that

$$g(C_n) = \sum_{r=2}^{n} \sum_{i_1<\cdots<i_r} \mathrm{genus}(D_{(i_1,\ldots,i_r)}).$$

It is clear that

$$\sum_{r=2}^{n} \sum_{i_1<\cdots<i_r} \mathrm{genus}(D_{(i_1,\ldots,i_r)}) = \binom{n}{2} + 2\binom{n}{3} + 3\binom{n}{4} + \cdots + (n-1)\binom{n}{n}.$$

This latter sum is also equal to $\binom{n}{n-2} + 2\binom{n}{n-3} + 3\binom{n}{n-4} + \cdots + (n-1)\binom{n}{0}$. Adding these two sums and dividing by 2 gives the value $2^{n-1}(n-2)+1$ for the sums, which is also the genus of C_n, as desired.

To produce the desired isogeny for the jacobian of $D_{(i_1,\ldots,i_r)}/K$, we consider the group H of automorphisms generated by the two involutions $x \mapsto -x$ and $Y \mapsto -Y$. There are 3 subgroups H_x (fixing x), H_y (fixing y), and H_{xy} (fixing xy) of order 2 in H. The quotient by H_x is the curve given by $Y^2 = (X+\alpha_{i_1})\cdot\ldots\cdot(X+\alpha_{i_r})$, and the quotient by H_{xy} is the curve given by $Y^2 = X(X+\alpha_{i_1})\cdot\ldots\cdot(X+\alpha_{i_r})$. The quotient by $H_x\cdot H_{xy}$ has genus 0. We find that $g(D_{(i_1,\ldots,i_r)}) = g(D_{(i_1,\ldots,i_r)}/H_x)+g(D_{(i_1,\ldots,i_r)}/H_y)+g(D_{(i_1,\ldots,i_r)}/H_{xy})$, so the isogeny we want is again a consequence of Theorem C of [5]. □

Example 6 When $n=4$, the curve C_4 has genus 17, with 15 elliptic curve quotients, and one quotient of genus 2,

$$Y^2 = X(X+\alpha_1)(X+\alpha_2)(X+\alpha_3)(X+\alpha_4).$$

The curve $y^2 = x(x+\alpha)(x+\alpha^{-1})(x+\beta)(x+\beta^{-1})$ has an additional automorphism[1] $(x,y)\mapsto(1/x, y/x^3)$. This automorphism has only two fixed points, with $x=1$, and the quotient is thus of genus 1, given by $v^2 = (u+2)(u+\alpha+\alpha^{-1})(u+\beta+\beta^{-1})$, with $(x,y)\mapsto(x+1/x, y(x+1)/x^2)$.

It follows that the curve $C(a^2,a^{-2},b^2,b^{-2})$ is a family of curves over $\mathbb{Q}$ of genus 17, with a jacobian isogenous over $\mathbb{Q}$ to a product of 17 elliptic curves. The same is true for the twist $C_4 = C(1,a^2,a^4,a^6)$, with additional[2] quotient $v^2=(u+2a^3)(u+a^2+a^4)(u+a^6+1)$, with $(x,y)\mapsto(x+a^6/x, y(x+a^3)/x^2)$. Note that some of the elliptic quotients in this example are isomorphic. Does this latter curve $C_4/\mathbb{Q}$ ever have a non-obvious $\mathbb{Q}$-rational point?

Remark 7 A different way to view the curve C_n when n is even is to consider the extension

$$K(x^2)(\sqrt{x^2(x^2+\alpha_1)\ldots(x^2+\alpha_n)}) \subseteq K(C_n).$$

This extension has degree 2^n, and defines an unramified morphism of curves $C_n\to D_n$ over K, where D_n is the hyperelliptic curve defined by the equation $Y^2 = X(X+\alpha_1)\ldots(X+\alpha_n)$. This morphism is Galois, with Galois group $(\mathbb{Z}/2\mathbb{Z})^n$. By abelian class field theory, the morphism $C_n\to D_n$ is obtained by pull-back from an isogeny $\mathrm{Jac}(D_n)\to\mathrm{Jac}(D_n)$. When n is even, $g(D_n)=n/2$, and the isogeny is the multiplication by 2 on $\mathrm{Jac}(D_n)$. When n is odd, the extension $K(x)(\sqrt{(x^2+\alpha_1)\ldots(x^2+\alpha_n)})\subseteq K(C_n)$ is still unramified of degree 2^{n-1}.

If the curve $C_n/\mathbb{Q}$ has a quotient $E/\mathbb{Q}$ of genus 1 with rank 0, then we obtain an explicit bound for $|C_n(\mathbb{Q})|$ since $|E(\mathbb{Q})|\le 16$ by the theorem of Mazur [9]. Note that such a quotient can exist even when C_n has a non-obvious point. Indeed, consider the curve $C_4 = C(a^2,a^{-2},b^2,b^{-2})$ as in Example 6, and choose a and b such that C_n has a non-obvious point $(x:y_1:\ldots:y_4:1)$ with $x=1$. Then the image of this point on the curve $C_2 = C(a^2,a^{-2})$ always has order 8, and to obtain the desired example, we choose a so that the rank of $C(a^2,a^{-2})$ is zero. This is achieved for instance with $a=3/4$ and $b=5/12$ (in this example, the Chabauty rank over $\mathbb{Q}$ is at most[3] $g(C_4)-2$).

If $C_n/\mathbb{Q}$ has 2 non-obvious non-equivalent $\mathbb{Q}$-rational points, then its quotients $C(a_{i_1}^2,a_{i_2}^2)$ have positive rank over $\mathbb{Q}$ since the non-obvious points produce more than 16 $\mathbb{Q}$-rational points on $C(a_{i_1}^2,a_{i_2}^2)$. It would be interesting to find examples of curves C_n with two non-obvious non-equivalent points and whose jacobians have a non-trivial quotient of rank less than its dimension. Proposition 10 shows that this cannot happen for $n\le 5$ if C_n has good reduction modulo a prime $p\le 4n+1$.

[1] So does the curve $C_{2m} = C(a_1^2,a_1^{-2},\ldots,a_m^2,a_m^{-2})$ with $(x:y_1:\ldots:y_{2m}:z)\longmapsto(z:y_2a_1:y_1/a_1:\ldots:y_{2m}a_m:y_{2m-1}/a_m:x)$.

[2] When $a=10$, all 15 natural elliptic quotients of C_4 have positive rank. This additional one has rank 0.

[3] Computations were done using the programs mwrank [10] and gp/pari [11]. The rank of the jacobian of dimension 2 can be computed using Stoll's program in Magma [8], and is found to be 0. Thanks to Steve Donnelly for his help with the Magma computations.

Proposition 8. *Let K be a field with a discrete valuation v, valuation ring $\mathcal{O}_K$, and maximal ideal (π). Let $k := \mathcal{O}_K/(\pi)$. Assume that $char(k) \neq 2$. Consider the curve $C_n = C(a_1^2, \dots, a_n^2)/K$. After a change of variables if necessary, we may assume that $a_i \in \mathcal{O}_K$ for all $i = 1, \dots, n$, and that at least one of the a_is is not divisible by π. Let $\Delta := \prod_i a_i \prod_{i \neq j}(a_i^2 - a_j^2)$. Then*

(1) *C_n/K has good reduction over $\mathcal{O}_K$ if and only if $\pi \nmid \Delta$.*
(2) *Assume that π divides only one of the factors in the product Δ. Then C_n/K has stable reduction over $\mathcal{O}_K$ consisting in the union of two curves of type C_{n-1} meeting in 2^{n-1} points.*
(3) *Assume in addition that π exactly divides $a_i^2 - a_j^2$. Then the special fiber $\mathcal{X}_k$ of the minimal regular model $\mathcal{X}/\mathcal{O}_K$ of the curve C_n/K consists in the union of two curves of type C_{n-1} meeting in 2^{n-1} points.*

Proof. (1) If C_n has good reduction, then all its elliptic quotients have good reduction, including $y^2 = x(x + a_i^2)(x + a_j^2)$, and we find that $\pi \nmid \prod a_i \prod(a_i^2 - a_j^2)$. Reciprocally, if $\pi \nmid \prod a_i \prod(a_i^2 - a_j^2)$, then the equations for C_n reduce modulo π to a set of equations that define a smooth space curve over k.

(2) Without loss of generality, we can assume that either $\pi \mid a_1$, or $\pi \mid a_1^2 - a_2^2$. Let $x^2 + \overline{a_i}^2 = y_i$, $i = 1, \dots, n$, denote the reduction of the equations for C_n modulo π. When $\pi \mid a_1$, the ideal $(x^2 + \overline{a_i}^2 = y_i^2, i = 1, \dots, n)$ is clearly contained in the intersection of the ideals $(x - y_1, x^2 + \overline{a_i}^2 = y_i^2, i = 2, \dots, n)$ and $(x + y_1, x^2 + \overline{a_i}^2 = y_i^2, i = 2, \dots, n)$. Similarly, when $\pi \mid a_1^2 - a_2^2$, the ideal $(x^2 + \overline{a_i}^2 = y_i^2, i = 1, \dots, n)$ is contained in the intersection of the ideals $(y_1 - y_2, x^2 + \overline{a_i}^2 = y_i^2, i = 2, \dots, n)$ and $(y_1 + y_2, x^2 + \overline{a_i}^2 = y_i^2, i = 2, \dots, n)$. Our assumptions implies that the four new ideals define smooth curves of type C_{n-1}/k, which each have genus $2^{n-2}(n-3) + 1$. The corresponding pairs of curves intersects in 2^{n-1} points, of the form, when $\pi \mid a_1^2 - a_2^2$, $(x = \pm\sqrt{-1}\overline{a_1} : y_1 = 0 : y_2 = 0 : y_3 : \dots : y_n : 1)$.

Such a configuration of two irreducible components meeting in 2^{n-1} points implies that the toric rank of the Néron model of the jacobian of $\mathrm{Jac}(C_n)/K$ is at least $2^{n-1} - 1$. The abelian contributions from the two irreducible components of genus $2^{n-2}(n-3) + 1$ and the toric rank $2^n - 1$ add up to $g(C_n) = 2(2^{n-2}(n-3) + 1) + 2^{n-1} - 1$. Thus, we have completely determined the stable model over $\mathcal{O}_K$.

(3) We keep the notation introduced in (3), and assume now that $\mathrm{ord}_\pi(a_1^2 - a_2^2) = 1$. To prove our statement, we only need to show that each intersection point in the special fiber is regular in the model. More precisely, consider the affine model $\mathcal{Y}/\mathcal{O}_K$ given by the spectrum of $\mathcal{O}_K[x, y_1, \dots, y_n]/(x^2 + a_i^2 = y_i^2, i = 1, \dots, n)$. The intersection points corresponds to maximal ideals M generated by π and $n+1$ other linear elements including y_1 and y_2 (we work here over K^{unr}, whose residue field is algebraically closed, so K^{unr} contains the square roots of any element coprime to π). We need to show that M/M^2 has dimension 2 over k. We use our additional hypothesis to obtain that $\pi \in (y_1^2 - y_2^2) \in M^2$ if $\mathrm{ord}_\pi(a_1^2 - a_2^2) = 1$. It follows that $M/M^2 = (y_1, y_2)$. □

Lemma 9. *Let p be an odd prime. Let $C_n := C(a_1^2, \dots, a_n^2)/\mathbb{F}_p$ be smooth.*

(1) *If $2n + 1 \leq p \leq 4n - 1$, then $C_n(\mathbb{F}_p)$ consists only in the 2^{n+1} obvious points.*
(2) *If $p = 4n + 1$, then $|C_n(\mathbb{F}_p)| = 2^{n+1}$ or $2^{n+1} + 2^n$.*

Proof. Since C_n is smooth, the a_i^2s are all distinct and non-zero, and thus $p \geq 2n+1$. The projective curve D given by the equation $X^2 + Y^2 = Z^2$ has exactly $p + 1$ $\mathbb{F}_p$-points. If $(x : y_1 : \dots : y_n : 1)$ is a non-obvious point of $C_n(\mathbb{F}_p)$, then $(\pm x : a_i : \pm y_i)$ are $4n$ distinct points on $D(\mathbb{F}_p)$, unless $y_i = 0$ for some (unique) i. In the latter case, $x = \sqrt{-1}a_i$ and we have only $4(n-1) + 2$ distinct solutions, including the trivial solutions $(1 : \pm\sqrt{-1} : 0)$.

Thus if there exists a non-obvious point and $p \equiv 3 \pmod 4$, $4n \le p-3$ implies $p \ge 4n+3$. Similarly, if $p \equiv 1 \pmod 4$, $4(n-1)+2 \le p-3$ implies $p \ge 4n+1$. When $p = 4n+1$, we could have $4(n-1)+2 = p-3$, in which case a non-obvious point with $y_i = 0$ for some i could exist. Such a point gives $2^n - 1$ other equivalent points. $\square$

Proposition 10. *Consider the curve $C_n := C(a_1^2, \dots, a_n^2)/\mathbb{Q}$, and let $J_n/\mathbb{Q}$ denote its jacobian. Assume that either $n \in \{3,4,5\}$, $p \in [2n+1, 4n+1]$, and C_n has good reduction modulo p, or that $n \in \{4,5\}$, $p \in [2(n-1)+1, 4(n-1)+1]$, and C_n has semi-stable reduction modulo p as in type (3) of Proposition 8. If there exists a quotient of J_n whose rank over $\mathbb{Q}$ is less than its dimension, then $|C_n(\mathbb{Q})| \le 2 \cdot 2^{n+1}$, so that $C_n(\mathbb{Q})$ has at most one (class of) non-obvious point.*

Proof. Assume that there is an abelian variety $A/\mathbb{Q}$ quotient of J_n over $\mathbb{Q}$, of rank strictly less than $\dim(A)$. Suppose that there exists a prime p and an integer $d < p$ such that $p^d > 2g(C_n) - 1 + d$. Let $\mathcal{X}/\mathcal{O}_K$ denote a regular model of C_n/K. Then Theorem 1.1 of [7] (the method of Chabauty-Coleman) shows that

$$(s+1)2^{n+1} \le |C_n(\mathbb{Q})| \le |\mathcal{X}_{\mathbb{F}_p}(\mathbb{F}_p)| + \frac{p-1}{p-d}(2g(C_n) - 2).$$

With our choice of primes, we use $d = 2$. When C_n has good reduction, we have $|\mathcal{X}_{\mathbb{F}_p}(\mathbb{F}_p)| = |\overline{C_n}(\mathbb{F}_p)|$. Using Lemma 9, we obtain that the bound on the right is less than $3 \cdot 2^{n+1}$. Since a non-obvious rational point always has $2^{n+1} - 1$ other rational points equivalent to it, the result follows. When C_n has semi-stable reduction of type (3), we use $|\mathcal{X}_{\mathbb{F}_p}(\mathbb{F}_p)| \le 2|\overline{C}_{n-1}(\mathbb{F}_p)|$ and proceed similarly. $\square$

To produce the next examples, let us introduce a different set of equations for the curve $C(a_1^2, \dots, a_n^2)/K$. Consider the curve $D(a_1, \dots, a_n)/K$ in $\mathbb{P}^n$ defined as the closure in $\mathbb{P}^n$ of the affine curve given by the $n-1$ equations

$$a_1 X(Y_i^2 - 1) = a_i Y_i (X^2 - 1), \text{ for } i = 2, \dots, n.$$

(As the reader will easily verify, when $n > 2$, the homogenous system of equations associated with the above system does not define a curve in $\mathbb{P}^n$, but contains also a linear subspace.) A birational map over K between $D(a_1, \dots, a_n)$ and $C(a_1^2, \dots, a_n^2)$ is given as follows:

$$(X, Y_2, \dots, Y_n) \longmapsto \left(\frac{2a_1 X}{X^2 - 1} : a_1 \frac{X^2+1}{X^2-1} : a_2 \frac{Y_2^2+1}{Y_2^2-1} : \dots : a_n \frac{Y_n^2+1}{Y_n^2-1} : 1\right).$$

Example 11 Let p be an odd prime. For each $2 \le n \le (p-1)/2$, we exhibit a curve $C_n/\mathbb{Q}$ with good reduction modulo p, and with a non-obvious rational point. Choose a positive integer g which is a primitive root modulo p. Then let $a_1 := g^{n-1}(p^2 - 1)$, and for $i = 2, \dots, n$, let

$$a_i := g^{i-2}(p^2 g^{2n+2-2i} - 1).$$

Modulo p, we find that $a_1 \equiv -g^{n-1}$ and $a_i \equiv -g^{i-2}$. Since g is chosen to be a primitive root modulo p, the squares of these residue classes are all distinct in $\mathbb{F}_p^*$, so $C(a_1^2, \dots, a_n^2)$ has good reduction modulo p. The coefficients a_i are constructed so that the point

$$(X, Y_2, \dots, Y_n) = (p, g^{n-1}p, g^{n-2}p, \dots, gp)$$

is a non-obvious point on the curve $D(a_1, \dots, a_n)$ (here $Y_i = g^{n+1-i}p$). It is easy to verify that the equations $a_1 p((g^{n+1-i}p)^2 - 1) = a_i g^{n+1-i} p(p^2 - 1)$ are satisfied.

It is not trivial to construct examples of curves C_n with two or more non-equivalent non-obvious points and having good reduction at a 'small' prime $p \le 4n+1$. One finds in [6], p. 757, a curve C_3 with $(a_1, a_2, a_3) = (1320, 3780, 11760)$ with 3 non-obvious non-equivalent points and good reduction modulo $p = 13$.

Using examples in [6], p. 758, one finds a curve $C_4(a_1^2, a_2^2, a_3^2, a_4^2)/\mathbb{Q}$ of rank at least $3g(C_4) + 5$ and a curve C_3 of rank at least $4g(C_3)$. We do not know what is the minimal possible rank over $\mathbb{Q}$ of a curve $C_4/\mathbb{Q}$. For $(a_1, a_2, a_3, a_4) = (1, 2, 3, 4)$ or $(1, 3, 4, 5)$, the rank is 7, and the latter curve has Chabauty rank at most 6.

Example 12 The above example lets us exhibit, for each odd prime p, an integral distance set S with $p + 1$ elements, not all on a line, and such that the distance between any two elements of the set is not divisible by p. Simply take the rational distance set $S = \{(0, \pm a_i), i = 1, \dots, (p-1)/2, (\pm\frac{2a_1 p}{p^2-1}, 0)\}$ and clear the denominators.

References

[1] L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points* J. Amer. Math. Soc. **10** (1997), 1–35.

[2] G. Frey, E. Kani, and H. Völklein, *Curves with infinite K-rational geometric fundamental group*, Aspects of Galois theory (Gainesville, FL, 1996), 85–118, London Math. Soc. Lecture Note Ser., 256, Cambridge Univ. Press, Cambridge, 1999.

[3] R. Guy, *Unsolved problems in number theory*, Third edition. Problem Books in Mathematics. Springer-Verlag, New York, 2004.

[4] G. Huff, *Diophantine problems in geometry and elliptic ternary forms*, Duke Math. J. **15** (1948), 443–453.

[5] E. Kani and M. Rosen, *Idempotent relations and factors of jacobians*, Math. Ann. **284** (1989), 307–327.

[6] J. Lagrange and J. Leech, *Two triads of squares*, Math. Comp. **46** (1986), 751–758.

[7] D. Lorenzini and T. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), 47–77.

[8] Magma, version V2.11-7, http://magma.maths.usyd.edu.au/magma/

[9] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

[10] mwrank, http://www.maths.nott.ac.uk/personal/jec/mwrank/index.html

[11] PARI/GP, version `2.1.5`, Bordeaux, 2004, http://pari.math.u-bordeaux.fr/.

[12] W. Peeples Jr., *Elliptic curves and rational distance sets*, Proc. Amer. Math. Soc. **5** (1954), 29–33.

[13] J. Solymosi, *Note on integral distances*, U.S.-Hungarian Workshops on Discrete Geometry and Convexity (Budapest, 1999/Auburn, AL, 2000), Discrete Comput. Geom. **30** (2003), 337–342.

Dino Lorenzini
Department of Mathematics
University of Georgia
Athens, GA 30602, USA