IMRN International Mathematics Research Notices
1997, No. 1

Algebraic Curves over $\mathbb{Q}$ with Many Rational Points and Minimal Automorphism Group

Colin Stahlke

1 Introduction

In [1], Caporaso, Harris, and Mazur show that the following conjecture would follow from one of Lang's diophantine conjectures (see Conjecture 5.7 in [4]).

Uniformity Conjecture. For each number field K and every $g \geq 2$ there exists a finite number $B(K, g)$ such that every smooth curve of genus g defined over K has at most $B(K, g)$ K-rational points. □

So they ask in [2]: How many rational points can an algebraic curve have?

Recently Kulesz found the following hyperelliptic curve with at least 588 rational points (see [3]):

$$y^2 = 278271081x^2(x^2 - 9)^2 - 229833600(x^2 - 1)^2.$$

Its automorphism group has order 12, so its Jacobian splits in the product of two isogenous elliptic curves.

We will give a curve with at least 336 rational points whose Jacobian does not split. After the submission of this paper we actually found such a curve with at least 366 rational points. Yet another curve with rank $(J(\mathbb{Q})) \geq 22$ improves the results of [5] and [6].

Received 14 August 1996.
Communicated by Barry Mazur.

2 Generating curves of genus 2 with absolutely irreducible Jacobian and with many rational points

We follow the method of J.-F. Mestre described by M. Stoll in [5], [6], and we make use of the idea of Keller and Kulesz that a curve with some rational points might have even more [3]. Stoll constructs hyperelliptic curves whose Jacobians are simple and have large rank. On these curves he finds up to $2 \cdot 104$ rational points.

We generate hyperelliptic curves that have rational points with 14 given x-coordinates $x_1, \ldots, x_{14} \in \mathbb{Q}$. There are uniquely determined rational numbers $a_0, \ldots, a_6$ and $b_0, \ldots, b_6$ such that

$$\prod_{i=1}^{14}(x - x_i) = (x^7 + a_6x^6 + a_5x^5 + \cdots + a_0)^2 - (b_6x^6 + b_5x^5 + \cdots + b_0).$$

The hyperelliptic curve

$$y^2 = b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

has at least 28 rational points, i.e., $(x_i, \pm(x_i^7 + a_6x_i^6 + a_5x_i^5 + \cdots + a_0))$. A change of coordinates gives an equation with only integer coefficients. We choose them such that their greatest common divisor is squarefree. These coefficients can still be very large. They tend to be much smaller if we choose the x_i to be integers. Doing this means no loss of generality but only another change of coordinates. By the same reasoning we can fix x_1 to be, say, -12. An extensive search using computers gave the following curve:

$$\begin{aligned} y^2 = {} & 1306881\,x^6 + 18610236\,x^5 - 46135758\,x^4 - 1536521592\,x^3 \\ & - 2095359287\,x^2 + 32447351356\,x + 89852477764. \end{aligned}$$

This curve is generated by choosing

$$(x_1, x_2, \ldots, x_{14}) = (-12, -11, -9, -7, -6, -5, -2, 2, 3, 6, 7, 9, 16, 17).$$

It has minimal automorphism group. Its Jacobian is absolutely irreducible and has rank $(J(\mathbb{Q})) \geq 16$. Curves whose Jacobians have higher rank tend to have much less rational points. We give the 168 x-coordinates with naïve height (maximum of the absolute value of numerator and denominator) less than 1000000 rational point pairs on the curve. This gives a total of 336 points:

-1281, -49, -41, -14, -12, -11, -9, -7, -6, -5, -2, 2, 3, 6, 7, 9, 16, 17, 75, 427, $-43/2$, $-7/2$, $-106/3$, $-17/3$, $-7/3$, $-5/3$, $17/3$, $22/3$, $28/3$, $73/3$, $91/3$, $-121/5$, $-14/5$, $232/5$, $-43/6$, $-41/6$, $-23/6$, $-107/7$, $-62/7$, $-57/7$, $-26/7$, $-49/8$, $-39/8$, $-56/11$, $-14/11$, $46/11$, $35/12$, $-97/13$, $-47/13$, $111/13$, $93/14$, $-139/15$, $19/16$, $-161/19$, $-72/19$, $91/19$,

175/19, −61/20, −116/21, 79/21, 185/21, 713/21, −403/25, −133/25, 19/25, −454/29, −217/29, −111/31, 27/31, 139/31, 403/33, −121/37, 679/37, 714/37, 233/38, −729/43, −427/43, −152/43, 181/43, 273/43, −47/49, 314/53, −406/57, −277/57, −196/57, 353/57, −629/73, −470/73, −287/75, −373/77, −1462/89, −14/93, −7431/107, −7/107, 599/107, −343/111, −5579/113, −358/113, 861/125, 371/131, −421/133, −1267/137, 560/137, −577/151, 1169/155, 358/157, −839/159, −217/159, −179/159, −82/159, −1477/169, −2023/192, 1403/232, 6062/233, 17564/257, −3367/267, −1309/269, 1571/285, 2506/307, −3269/309, 3262/327, −3542/349, −1838/361, 4346/363, −1318/371, 882/373, −5124/389, −1189/389, 6418/393, −1325/397, −3539/436, −1673/445, −3323/478, 2986/481, −9563/487, −553/548, −3134/643, 7126/733, 799/1032, −5117/1033, −21577/1119, −973/1213, −1155/1279, 19909/1338, −8773/1499, −22997/1609, −18367/1643, −18937/1757, −36099/2041, 27596/2273, −18466/3351, −21155/3378, 21329/3469, −2051/3531, −50155/4881, 28126/4911, 47243/6665, −38906/7307, −25693/8202, −31470/8321, −24941/9931, 3698/10069, −51763/10601, 25137/16699, −156677/27579, −429919/33954, −192437/52719, −213677/129607

Our new curve with at least 366 points and rank $(J(\mathbb{Q})) \geq 18$ is given by

$$(x_1, x_2, \ldots, x_{14}) = (-12, -11, -10, -9, -8, -4, -1, 1, 5, 8, 9, 10, 14, 18).$$

The 14-tuple $(-12, -11, -10, -9, -6, -4, -3, 1, 2, 4, 6, 9, 11, 12)$ gives a curve with rank $(J(\mathbb{Q})) > 22$ but we only find 120 points on it.

3 Generating curves of genus 3 with many rational points

There are uniquely determined $a_0, \ldots, a_8$ and $b_0, \ldots, b_8$ such that

$$\prod_{i=1}^{18}(x - x_i) = (x^9 + a_8x^8 + a_7x^7 + \cdots + a_0)^2 - (b_8x^8 + b_7x^7 + b_6x^6 + \cdots + b_0).$$

The curve of genus 3

$$y^2 = b_8x^8 + b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

has at least 36 rational points. Searching this family gave the following curve:

$$y^2 = 76\,x^8 + 671\,x^7 - 8539\,x^6 - 89512\,x^5 + 147851\,x^4 + 3076727\,x^3 + 6159667\,x^2 - 3720486\,x - 3527271.$$

We give the 52 x-coordinates with naïve height less than 1000000 rational point pairs on

this curve, giving a total of 104 points:

$$-47, -12, -11, -9, -8, -7, -6, -5, -4, -3, -2, -1, 1, 2, 5, 7, 8, 9, 11, 14, 15, 23, 193, -11/3, 4/3, -73/4, -21/4, 11/4, -23/5, -55/8, -11/8, -77/15, 34/15, -99/17, 31/17, -163/19, -11/19, 27/19, -87/25, 34/25, -223/31, -199/31, -29/31, -253/36, -227/51, -517/61, 411/61, 463/61, -369/79, -733/127, -509/157, -189/292$$

This curve is generated by choosing

$$(x_1, \ldots, x_{18}) = (-12, -11, -9, -8, -6, -5, -4, -3, -2, -1, 1, 2, 7, 8, 9, 11, 14, 15).$$

The curve has minimal automorphism group. It is remarkable that we find only rational points of small naïve height on the curve.

The search for curves of higher genus did not give curves with many more rational points than the given ones.

Acknowledgments

I wish to thank B. Mazur for introducing me to the subject and N. Elkies and M. Stoll for their marvelous C-program that finds rational points on hyperelliptic curves very fast, using a sieving method. I would also like to thank F. Grunewald for offering me an excellent research environment.

References

[1] L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points*, to appear in J. Amer. Math. Soc.

[2] ———, "How many rational points can a curve have?" in *The Moduli Space of Curves*, *(Texel Island*, *1994)*, Progr. Math. **129**, Birkhäuser, Boston, 1995, 13–31.

[3] L. Kulesz, *Courbes algébriques de genre* 2 *possédant de nombreux points rationnels*, C. R. Acad. Sci. Paris, Sér. I Math. **321** (1995), 1469–1472.

[4] S. Lang, *Hyperbolic and diophantine analysis*, Bull. Amer. Math. Soc. **14** (1986), 159–205.

[5] M. Stoll, *Two simple* 2*-dimensional abelian varieties defined over* $\mathbb{Q}$ *with Mordell-Weil group of rank at least* 19, C. R. Acad. Sci. Paris, Sér. I Math. **321** (1995), 1341–1345.

[6] ———, *An example of a simple* 2*-dimensional abelian variety defined over* $\mathbb{Q}$ *with Mordell-Weil group of rank at least* 20, C. R. Acad. Sci. Paris, Sér. I Math. **322** (1996), 849–851.

Mathematisches Institut der Universität Bonn, Wegelerstraße 10, D-53115 Bonn, Germany; colin@rhein.iam.uni-bonn.de *or* colin@math.harvard.edu