COMPUTER SEARCH FOR CURVES WITH MANY POINTS AMONG ABELIAN COVERS OF GENUS 2 CURVES OVER $\mathbf{F}_{13}$

KARL RÖKAEUS

Abstract.[1] We construct curves over $\mathbf{F}_{13}$ with many rational points, giving new entries for the tables *manYPoints.org* [5].

Background and results

For q a prime power and g a non-negative integer, let $\mathrm{N}_q(g)$ be the maximum possible number of rational points on a projective, non-singular and geometrically irreducible curve of genus g defined over $\mathbf{F}_q$. The intervals in which $\mathrm{N}_q(g)$ in known to lie, together with references, are given in the tables [5]. In this report we improve upon the lower bounds by constructing curves with many points for some genera over $\mathbf{F}_{13}$. We do this by going through unramified abelian covers of all curves of genus 2, using first the Magma [1] package *G2Twists* [4] to list all the genus 2 curves, and then class field theory to list unramified abelian covers of each curve. Below we give a list of genus and number of points of the best curves that we found, and then an appendix containing all the data required to construct them; we refer to [8] for details about how the search was organized (see also [7], where we performed the same search over smaller fields). We mention that the class field theoretic methods employed here have been used before by various authors; see [2] and [6], and the references therein.

The criteria used to decide if a curve has many points, and hence if it should be included in the tables [5], is that it has more than $b(q,g)/\sqrt{2}$ points, where $b(q,g)$ is the best known upper bound for $\mathrm{N}_q(g)$, see [3]. For $q = 13$ the lower bounds of the tables were empty for $g \geq 5$, and we hence include in this report all curves that we found that has more than $b(q,g)/\sqrt{2}$ points.

The results are given in the table below; we give integers g and N such that there exists a genus g curve with N points, and then the interval $[b(q,g)/\sqrt{2}, b(q,g)]$. The details required to construct these curves are given in the appendix, as the output of a Magma session.

Existence of curves over $\mathbf{F}_{13}$ of genus g with N rational points.

g	N	$[\frac{b(g)}{\sqrt{2}}, b(g)]$	g	N	$[\frac{b(g)}{\sqrt{2}}, b(g)]$	g	N	$[\frac{b(g)}{\sqrt{2}}, b(g)]$
5	40	[32,44]	14	65	[65,91]	29	140	[114,161]
6	50	[37,52]	15	84	[68,96]	32	124	[124,175]
7	48	[42,58]	16	90	[72,101]	33	128	[127,179]
8	56	[45,63]	17	96	[75,105]	35	136	[133,187]
9	56	[49,68]	18	85	[78,110]	36	140	[136,191]
10	63	[51,72]	19	90	[82,115]	37	144	[138,195]
11	70	[55,77]	20	95	[85,119]	41	160	[150,211]
12	66	[58,82]	21	100	[88,124]	43	168	[155,219]
13	72	[62,87]	22	105	[92,129]			

Date: June 23, 2011.

[1]The author is supported by the Wenner-Gren Foundations Postdoctoral Grant

Acknowledgments. The author thanks the Wenner-Gren Foundations for financial support; the Korteweg-de Vries Institute at the University of Amsterdam for hospitality; and Gerard van der Geer for his hospitality and for helpful conversations and comments.

References

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput., 24 (1997), 235-265.

[2] G. van der Geer, *Hunting for curves with many points*, In: C. Xing et al. (Eds.): IWCC 2009, LNCS 5557, pp. 82–96, 2009. Available electronically: arXiv:0902.3882 (2009)

[3] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, Math. Comp 69, (2000), no 230 pp. 797–810

[4] R. Lercier and C. Ritzenthaler, *G2Twists v1.1 : Reconstruction of genus 2 curves from their invariants and twists over a finite field*, Magma package, incorporated in the official magma distribution, since version 2.15, April 2009.

[5] *manYPoints.org*, Tables of upper and lower bounds for the maximum number of points on a genus g curve over different finite fields. Moderators: G. van der Geer, E. Howe, K. Lauter, C. Ritzenthaler

[6] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields*, LMS Lecture Note Series 285, 2001

[7] K. Rökaeus, *Computer search for curves with many points among unramified covers of genus 2 curves over* $\mathbf{F}_5$, $\mathbf{F}_7$, $\mathbf{F}_9$ *and* $\mathbf{F}_{11}$, Report, available under *manYPoints.org*, http://manypoints.org/upload/1369548137.pdf

[8] K. Rökaeus, *Computer search for curves with many points among abelian covers of genus 2 curves*, To appear.

Appendix

This appendix contains the output from a Magma session, displaying data sufficient to construct one curve for each entry in the table above. It is to be read as follows: For every post, first comes a pair (g, N) such that there exists a projective, non-singular and geometrically irreducible curve over $\mathbf{F}_{13}$, of genus g and with N rational points. Next come all details required to prove this: First a genus 2 curve C given as a hyperelliptic curve by an equation of the form $y^2 = f(x)$. On the next lines is a list M of points on the curve, where the curve is viewed as being embedded in the weighted projective plane with weights 1,3 and 1, respectively, on x, y and z. Let O be any point in M. Then the image of M under the map $p \mapsto [p - O]\colon C(\mathbf{F}_{13}) \to \mathrm{Jac}(C)(\mathbf{F}_{13})$ is contained in a subgroup of index $g - 1$. By class field theory (see [2]), C has an unramified abelian cover of degree $g - 1$ in which all points in M splits; this cover then has genus g and $|M| \cdot (g - 1) = N$ rational points.

```
-----------------------------------------------
<5, 40>

Hyperelliptic Curve defined by y^2 = x^6 + 11*x^5 + x^4 + 11*x^3 +
x^2 + 11*x + 1 over GF(13)

[ (1 : 1 : 0), (1 : 12 : 0), (0 : 1 : 1), (0 : 12 : 1), (2 : 1 : 1),
 (2 : 12 : 1), (6 : 0 : 1), (7 : 8 : 1), (7 : 5 : 1), (11 : 0 : 1) ]
-----------------------------------------------
<6, 50>

Hyperelliptic Curve defined by y^2 = 12*x^6 + 8*x^4 + 8*x^2 + 12
over GF(13)

[ (2 : 11 : 1), (2 : 2 : 1), (3 : 9 : 1), (3 : 4 : 1), (4 : 9 : 1),
```

```
(4 : 4 : 1), (5 : 0 : 1), (6 : 3 : 1), (6 : 10 : 1), (8 : 0 : 1) ]
-----------------------------------------------
<7, 48>

Hyperelliptic Curve defined by y^2 = 3*x^6 + 11*x^5 + 9*x^4 + 4*x^3 +
x^2 + 6*x + 8 over GF(13)

[ (1 : 9 : 1), (1 : 4 : 1), (8 : 0 : 1), (9 : 11 : 1), (9 : 2 : 1),
(11 : 11 : 1), (11 : 2 : 1), (12 : 0 : 1) ]
-----------------------------------------------
<8, 56>

Hyperelliptic Curve defined by y^2 = 5*x^6 + x^4 + 11*x^3 + 5*x^2 +
9*x + 9 over GF(13)

[ (3 : 3 : 1), (3 : 10 : 1), (6 : 7 : 1), (6 : 6 : 1), (7 : 8 : 1),
(7 : 5 : 1), (9 : 0 : 1), (12 : 0 : 1) ]
-----------------------------------------------
<9, 56>

Hyperelliptic Curve defined by y^2 = 10*x^5 + 11*x^4 + 10*x^2 +
5*x + 10 over GF(13)

[ (1 : 0 : 0), (7 : 9 : 1), (7 : 4 : 1), (8 : 1 : 1), (8 : 12 : 1),
(12 : 9 : 1), (12 : 4 : 1) ]
-----------------------------------------------
<10, 63>

Hyperelliptic Curve defined by y^2 = 10*x^6 + 10*x^5 + 5*x^4 +
5*x^3 + x^2 + 12*x + 10 over GF(13)

[ (0 : 7 : 1), (0 : 6 : 1), (2 : 0 : 1), (7 : 1 : 1), (7 : 12 : 1),
(11 : 8 : 1), (11 : 5 : 1) ]
-----------------------------------------------
<11, 70>

Hyperelliptic Curve defined by y^2 = 9*x^6 + 2*x^4 + 2*x^3 + 9*x^2 +
2*x + 3 over GF(13)

[ (1 : 3 : 0), (1 : 10 : 0), (0 : 9 : 1), (0 : 4 : 1),
(5 : 0 : 1), (8 : 0 : 1),(10 : 0 : 1) ]
-----------------------------------------------
<12, 66>

Hyperelliptic Curve defined by y^2 = 6*x^6 + 2*x^5 + 11*x^4 + 2*x^3 +
9*x^2 + 9*x + 12 over GF(13)

[ (2 : 11 : 1), (2 : 2 : 1), (3 : 7 : 1), (3 : 6 : 1), (9 : 8 : 1),
 (9 : 5 : 1) ]
-----------------------------------------------
<13, 72>
```

```
Hyperelliptic Curve defined by y^2 = x^6 + 11*x^5 + x^4 + 11*x^3 +
x^2 + 11*x + 1 over GF(13)

[ (1 : 1 : 0), (1 : 12 : 0), (0 : 1 : 1), (0 : 12 : 1), (6 : 0 : 1),
(11 : 0 : 1) ]
-----------------------------------------------
<14, 65>

Hyperelliptic Curve defined by y^2 = 5*x^6 + 3*x^5 + 9*x^4 + 7*x^3 +
3*x^2 + 12*x + 12 over GF(13)

[ (7 : 7 : 1), (7 : 6 : 1), (8 : 8 : 1), (8 : 5 : 1), (11 : 0 : 1) ]
-----------------------------------------------
<15, 84>

Hyperelliptic Curve defined by y^2 = 5*x^6 + x^4 + 11*x^3 + 5*x^2 +
9*x + 9 over GF(13)

[ (3 : 3 : 1), (3 : 10 : 1), (6 : 7 : 1), (6 : 6 : 1), (9 : 0 : 1),
(12 : 0 : 1)]
-----------------------------------------------
<16, 90>

Hyperelliptic Curve defined by y^2 = x^6 + 11*x^5 + x^4 + 11*x^3 +
x^2 + 11*x + 1 over GF(13)

[ (5 : 9 : 1), (5 : 4 : 1), (6 : 0 : 1), (8 : 7 : 1), (8 : 6 : 1),
(11 : 0 : 1)]
-----------------------------------------------
<17, 96>

Hyperelliptic Curve defined by y^2 = 2*x^6 + 11 over GF(13)

[ (1 : 0 : 1), (3 : 0 : 1), (4 : 0 : 1), (9 : 0 : 1), (10 : 0 : 1),
(12 : 0 : 1)]
-----------------------------------------------
<18, 85>

Hyperelliptic Curve defined by y^2 = x^6 + 8*x^5 + 8*x^4 +
3*x^3 + 3*x + 7 over GF(13)

[ (1 : 1 : 0), (1 : 12 : 0), (4 : 0 : 1), (8 : 0 : 1), (10 : 0 : 1) ]
-----------------------------------------------
<19, 90>

Hyperelliptic Curve defined by y^2 = 10*x^6 + 5*x^5 + 9*x^3 +
11*x^2 + 11*x + 12 over GF(13)

[ (0 : 8 : 1), (0 : 5 : 1), (5 : 0 : 1), (6 : 0 : 1), (11 : 0 : 1) ]
-----------------------------------------------
<20, 95>
```

```
Hyperelliptic Curve defined by y^2 = 2*x^6 + 2*x^3 + 12 over GF(13)

[ (0 : 8 : 1), (0 : 5 : 1), (2 : 0 : 1), (5 : 0 : 1), (6 : 0 : 1) ]
------------------------------------------------
<21, 100>

Hyperelliptic Curve defined by y^2 = 9*x^6 + 2*x^4 + 2*x^3 +
9*x^2 + 2*x + 3 over GF(13)

[ (1 : 3 : 0), (1 : 10 : 0), (0 : 9 : 1), (0 : 4 : 1), (5 : 0 : 1) ]
------------------------------------------------
<22, 105>

Hyperelliptic Curve defined by y^2 = x^6 + x^3 + 9 over GF(13)

[ (1 : 1 : 0), (1 : 12 : 0), (7 : 0 : 1), (8 : 0 : 1), (11 : 0 : 1) ]
------------------------------------------------
<29, 140>

Hyperelliptic Curve defined by y^2 = 2*x^6 + 2*x^3 + 9 over GF(13)

[ (0 : 3 : 1), (0 : 10 : 1), (1 : 0 : 1), (3 : 0 : 1), (9 : 0 : 1) ]
------------------------------------------------
<32, 124>

Hyperelliptic Curve defined by y^2 = 6*x^6 + 3*x^4 + 9*x^3 +
2*x^2 + 2*x + 4 over GF(13)

[ (1 : 0 : 1), (2 : 0 : 1), (3 : 0 : 1), (7 : 0 : 1) ]
------------------------------------------------
<33, 128>

Hyperelliptic Curve defined by y^2 = 12*x^6 + 10*x^5 + 6*x^4 + 5*x^3 +
6*x^2 + 10*x + 12 over GF(13)

[ (4 : 7 : 1), (4 : 6 : 1), (6 : 0 : 1), (11 : 0 : 1) ]
------------------------------------------------
<35, 136>

Hyperelliptic Curve defined by y^2 = 9*x^6 + 3*x^5 + 3*x^4 + 4*x^3 +
11*x^2 + 5*x + 3 over GF(13)

[ (9 : 0 : 1), (10 : 3 : 1), (10 : 10 : 1), (11 : 0 : 1) ]
------------------------------------------------
<36, 140>

Hyperelliptic Curve defined by y^2 = 9*x^6 + 2*x^4 + 2*x^3 + 9*x^2 +
2*x + 3 over GF(13)

[ (5 : 0 : 1), (6 : 0 : 1), (8 : 0 : 1), (10 : 0 : 1) ]
------------------------------------------------
<37, 144>
```

```
Hyperelliptic Curve defined by y^2 = x^6 + 4*x^3 + 12 over GF(13)

[ (1 : 1 : 0), (1 : 12 : 0), (0 : 8 : 1), (0 : 5 : 1) ]
-----------------------------------------------
<41, 160>

Hyperelliptic Curve defined by y^2 = 2*x^6 + 5*x^5 + 12*x^4 + 12*x^3 +
x^2 + 5*x + 11 over GF(13)

[ (3 : 0 : 1), (4 : 0 : 1), (8 : 11 : 1), (8 : 2 : 1) ]
-----------------------------------------------
<43, 168>

Hyperelliptic Curve defined by y^2 = 4*x^6 + 7*x^5 + x^4 + 7*x^3 +
11*x^2 + 12*x over GF(13)

[ (0 : 0 : 1), (1 : 9 : 1), (1 : 4 : 1), (9 : 0 : 1) ]
-----------------------------------------------
```

Karl Rökaeus, Korteweg de Vries Instituut voor Wiskunde, Universiteit van Amsterdam, P.O. Box 94248, 1090 GE Amsterdam, The Netherlands

E-mail address: S.K.F.Rokaeus@uva.nl