

# Poster Abstracts from the Eighth Algorithmic Number Theory Symposium, ANTS-8

Communicated by Jonathan Sorenson  
 Computer Science and Software Engineering  
 Butler University  
 Indianapolis, Indiana, 46208 USA  
[sorenson@butler.edu](mailto:sorenson@butler.edu)  
<http://www.butler.edu/~sorenson>

## Abstract

The following twelve poster abstracts were presented at the ANTS-8 poster session.<sup>1</sup> ANTS-8 was held at the Banff Centre in Banff, Alberta Canada, May 17–22, 2008. The conference website, where many of the posters can be viewed online, is <http://ants.math.ualgary.ca/>.

## Calculating Really Big Cyclotomic Polynomials

**Andrew Arnold and Michael Monagan, Simon Fraser University, [ada26@sfu.ca](mailto:ada26@sfu.ca)**

The  $n$ <sub>th</sub> cyclotomic polynomial,  $\Phi_n(z)$ , is the monic polynomial whose  $\phi(n)$  distinct roots are the  $n$ <sub>th</sub> complex primitive roots of unity. That is,

$$\Phi_n(z) = \prod_{\substack{0 \leq k < n \\ \gcd(k,n)=1}} (z - e^{\frac{2\pi i}{n}k})$$

The first ten cyclotomic polynomials are as follows:

$$\Phi_1(z) = z - 1$$

$$\Phi_2(z) = z + 1$$

$$\Phi_3(z) = z^2 + z + 1$$

$$\Phi_4(z) = z^2 + 1$$

$$\Phi_5(z) = z^4 + z^3 + z^2 + z + 1$$

$$\Phi_6(z) = z^2 - z + 1$$

$$\Phi_7(z) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1$$

$$\Phi_8(z) = z^4 + 1$$

$$\Phi_9(z) = z^6 + z^3 + 1$$

$$\Phi_{10}(z) = z^4 - z^3 + z^2 - z + 1$$

<sup>1</sup>Poster session funding provided by Butler University. Special thanks to Teri Amberger and Amy Aldridge for their help in printing and shipping posters to Calgary, and also to Renate Scheidler.

Observe that all the coefficients in the polynomials above are either -1, 0, or 1. In fact, the first cyclotomic polynomial with a coefficient that is not -1, 0, or 1 is  $\Phi_{105}(z)$ . If we write  $\Phi_n(z) = \sum_{j=1}^{\phi(n)} a_n(m)z^m$ , then we let  $A_n = \max_{1 \leq m \leq \phi(n)} |a_n(m)|$  and  $S_n = \sum_{m=1}^{\phi(n)} |a_n(m)|$  be the height and length of  $\Phi_n(z)$ , respectively. The aim of our research is to study  $A_n$  and  $S_n$ . In particular, we are looking for cyclotomic polynomials with large heights.

We present two algorithms to calculate cyclotomic polynomials. Our first algorithm uses that for primes  $p \nmid n$ ,  $\Phi_{np}(z) = \Phi_n(z^p) \div \Phi_n(z)$ . We perform fast polynomial division via the discrete fast Fourier transform.

For our second algorithm, we use the identity:

$$\Phi_n(z) = \prod_{\substack{1 \leq k \leq n \\ k|n}} (z^k - 1)^{\mu(\frac{n}{k})}$$

We construct  $\Phi_n(z)$  as a quotient of sparse power series. This method allows us to calculate cyclotomic polynomials in an integer array completely in memory, thereby minimizing memory requirements.

Using the latter approach we are able to quickly calculate cyclotomic polynomials of order upwards of one billion. Amongst our findings we have found the cyclotomic polynomial of smallest order whose height exceeds its order; the first cyclotomic polynomial whose height exceeds its order squared; the first whose height exceeds machine precision ( $2^{64}$ ); a cyclotomic polynomial whose height exceeds its order raised to the fourth power; and all cyclotomic polynomials of squarefree order with six or more distinct factors up to order  $6 \cdot 10^8$ , and all with squarefree order with seven or more distinct factors up to  $10^9$ .

## Genus 2 curves with split Jacobians

Kevin Doerksen, Simon Fraser University, kdoerkse@sfu.ca

### *Winner of the ANTS-8 Best Poster Award*

Split Jacobians are special. For genus 2 curves, they can be recognized from the fact that  $C$  is a degree  $n$  cover of an elliptic curve for some integer  $n$ . One can classify split Jacobians of genus 2 curves by these  $n$ . If  $\psi : C \rightarrow E$  is a degree  $n$  cover then we say  $\text{Jac}(C)$  is  $(n, n)$  split.

To classify split Jacobians, one can look at all the possible configurations of the ramification points in the covering map  $\psi : C \rightarrow E$  (see for example Kuhn [3] and Shaska [4]). The degree  $n = 3$  case was solved by Shaska [6] and studied further in [5]. The degree  $n = 5$  case has also been solved in a preprint by Magaard, Shaska, and Völklein. The description of all odd cases greater than  $n = 5$  and all even cases greater than  $n = 2$  remain open questions. In this poster, we will explain techniques to classify  $(n, n)$ -split Jacobians and outline our progress on the degree 4 case.

We begin our poster by showing the degree  $n$  cover  $\psi : C \rightarrow E$  of the genus 2 curve  $C$  onto the elliptic curve  $E$  induces a degree  $n$  cover  $\phi : \mathbb{P}^1 \rightarrow \mathbb{P}^1$  such that the following diagram commutes:

$$\begin{array}{ccc} C & \xrightarrow{\psi} & E \\ \pi_C \downarrow & & \downarrow \pi_E \\ \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^1 \end{array}$$

here,  $\pi_C$  is the natural degree 2 cover of  $C$  onto  $\mathbb{P}^1$  and  $\pi_E$  is the degree 2 projection of  $E$  onto  $\mathbb{P}^1$  induced by  $\pi_C$ . Gerhard Frey and Ernst Kani give a complete description of this induced cover  $\phi$  of the projective lines in their 1988 paper [2]. Using this commutative diagram, it is possible to show that if  $n$  is odd, then there is only a handful of possible configurations of the ramification points. It was by studying these few possibilities that the  $(3, 3)$  and  $(5, 5)$  split Jacobians were characterized.

The next section of the poster deals with the case where  $n = 4$ . In general, the even cases have fewer restrictions on the distribution of the ramification points, and are therefore more difficult to characterize. In order to get around this hurdle, we build up the degree 4 case by first looking at the degree 2 case.

The ability to precisely describe and construct  $(n, n)$ -split Jacobians has important computational applications. It allows the construction of abelian varieties with special isogenies and allows new explicit visibility constructions (N. Bruin [1]).

## References

- [1] N. Bruin and E. V. Flynn. Exhibiting SHA[2] on hyperelliptic Jacobians. *J. Number Theory*, 118(2):266–291, 2006.
- [2] Gerhard Frey and Ernst Kani. Curves of genus 2 covering elliptic curves and an arithmetical application. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 153–176. Birkhäuser Boston, Boston, MA, 1991.
- [3] Robert M. Kuhn. Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc.*, 307(1):41–49, 1988.
- [4] T. Shaska. Curves of genus 2 with  $(N, N)$  decomposable Jacobians. *J. Symbolic Comput.*, 31(5):603–617, 2001.
- [5] T. Shaska. Genus 2 curves with  $(3, 3)$ -split Jacobian and large automorphism group. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 205–218. Springer, Berlin, 2002.
- [6] T. Shaska. Genus 2 fields with degree 3 elliptic subfields. *Forum Math.*, 16(2):263–280, 2004.

## A variant of Wiener’s attack on RSA with small secret exponent

**Andrej Dujella, University of Zagreb, duje@math.hr**

To speed up the RSA decryption one may try to use small secret decryption exponent  $d$ . The choice of a small  $d$  is especially interesting when there is a large difference in computing power between two communicating devices. However, in 1990, Wiener showed that if  $d < n^{0.25}$ , where  $n = pq$  is the modulus of the cryptosystem, then there exist a polynomial time attack on the RSA. He showed that  $d$  is the denominator of some convergent  $p_m/q_m$  of the continued fraction expansion of  $e/n$ , and therefore  $d$  can be computed efficiently from the public key  $(n, e)$ .

In 1997, Verheul and van Tilborg proposed an extension of Wiener’s attack that allows the RSA cryptosystem to be broken when  $d$  is a few bits longer than  $n^{0.25}$ . For  $d > n^{0.25}$  their attack

needs to do an exhaustive search for about  $2t + 8$  bits (under reasonable assumptions on involved partial convergents), where  $t = \log_2(d/n^{0.25})$ . In 2004, we introduced a slight modification of the Verheul and van Tilborg attack, based on Worley's result on Diophantine approximations of the form  $|\alpha - p/q| < c/q^2$ , for a positive real number  $c$ .

In both mentioned extensions of Wiener's attack, the candidates for the secret exponent are of the form  $d = rq_{m+1} + sq_m$ . We test all possibilities for  $d$ , and number of possibilities is roughly (number of possibilities for  $r$ )  $\times$  (number of possibilities for  $s$ ), which is  $O(D^2)$ , where  $d = Dn^{1/4}$ . There are two principal methods for testing:

- 1) compute  $p$  and  $q$  assuming  $d$  is correct guess;
- 2) test the congruence  $(M^e)^d \equiv M \pmod{n}$ , say for  $M = 2$ .

Here we present a new idea, which is to apply "meet-in-the-middle" to this second test. Let  $2^{eq_{m+1}} \pmod{n} = a$ ,  $(2^{eq_m})^{-1} \pmod{n} = b$ . Then we test the congruence  $a^r \equiv 2b^s \pmod{n}$ . We can do it by computing  $a^r \pmod{n}$  for all  $r$ , sorting the list of results, and then computing  $2b^s \pmod{n}$  for each  $s$  one at a time, and checking if the result appears in the sorted list. This decrease the time complexity of testings phase to  $O(D \log D)$  (with the space complexity  $O(D)$ ). We present also some variants of the proposed attack, which might be relevant for its practical implementation.

## References

- [1] D. Boneh, G. Durfee, *Cryptanalysis of RSA with private key  $d$  less than  $N^{0.292}$* , Advances in Cryptology - Proceedings of Eurocrypt '99, Lecture Notes in Comput. Sci. **1952** (1999), 1–11.
- [2] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29** (2004), 101–112.
- [3] A. Dujella, B. Ibrahimpaić, *On Worley's theorem in Diophantine approximations*, preprint.
- [4] J. Hinek, *On the Security of Some Variants of RSA*, Ph.D. Thesis, University of Waterloo, 2007.
- [5] R. Steinfeld, S. Contini, H. Wang, J. Pieprzyk, *Converse results to the Wiener attack on RSA*, Public Key Cryptography - PKC 2005, Lecture Notes in Comput. Sci. **3386** (2005), 184–198.
- [6] H.-M. Sun, M.-E. Wu, Y.-H. Chen, *Estimating the Prime-Factors of an RSA Modulus and an Extension of the Wiener Attack*, Applied Cryptography and Network Security, Lecture Notes in Comput. Sci. **4521** (2007), 116–128.
- [7] E. R. Verheul, H. C. A. van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Appl. Algebra Engrg. Comm. Computing **8** (1997), 425–435.
- [8] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), 553–558.
- [9] R. T. Worley, *Estimating  $|\alpha - p/q|$* , Austral. Math. Soc. Ser. A **31** (1981), 202–206.

# Computing the 2-distribution of points on Hermitian surfaces

**Frédéric A. B. Edoukou, CNRS, Institut de Mathématiques de Luminy, edoukou@iml.univ-mrs.fr**

A short description is first given of the fascinating use of the Hermitian curve  $C(2) : x_0^3 + x_1^3 + x_2^3 = 0$  of  $PG(2, 2^2)$  by the Russian mathematician V. Goppa (1981, 1983) in the construction of linear error-correcting codes. Subsequently the work of Goppa inspired many authors.

In 1985, I. Charkravarti suggested a generalization of Goppa construction based on his early work with R. C. Bose on Hermitian varieties by embedding the non-singular Hermitian surface  $X(2) : x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0$  of  $PG(3, 2^2)$  in a  $PG(9, 2^2)$  via the linear system of quadrics.

In 1986, R. Tobias and P. Spurr by a complete computer search (computer programs) compute the 2-distribution of points on this Hermitian surface  $X(2)$ . We define by  $h$ -distribution of points of a projective variety  $\mathcal{V}$  to be the decreasing sequence of the number of points in the section of  $\mathcal{V}$  by all hypersurfaces of degree  $h$ , associated with their multiplicities.

In 1993, A. B. Sørensen showed that computer program is not necessary in order to find the first family of points in the Hermitian surface  $X(2)$  of  $PG(3, 2^2)$ , and generalized his result on the first family of points in the Hermitian surface  $X(t) : x_0^{t+1} + x_1^{t+1} + x_2^{t+1} + x_3^{t+1} = 0$  of  $PG(3, t^2)$  by the following conjecture:

$$\#X_{Z(f)}(\mathbb{F}_q) \leq h(t^3 + t^2 - t) + t + 1.$$

where  $f$  is a homogenous form degree  $h$ , and  $\#X_{Z(f)}(\mathbb{F}_q)$  the number of points in the section of  $X$  by the surface defined by  $f$ .

In this poster we will resolve the conjecture of Sørensen for quadric. We will compute the 2-distribution of points on the Hermitian surface  $X(t)$ . The starting point for the resolution of the above problems is J. W. P. Hirschfeld classification of quadrics. The results of Hirschfeld on the geometry of Hermitian surfaces and quadric surfaces, as well as modifications of methods due to J. P. Serre are used to evaluate the number of points on hypersurfaces, to study  $X_Z(f)$  and to show the conjecture for  $h = 2$ .

A more subtle treatment based on the study on divisors on a surface, and the using of the result on the theorem of Ax on the Zeroes of polynomials over finite fields allow us to appreciate the 2-distribution of points on the surface  $X(t)$ .

## References

- [1] Y. Aubry and M. Perret, On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields, *Finite Fields and Their Applications* 10, (2004), 412-431.
- [2] I. M. Chakravarti, The generalized Goppa codes and related discrete designs from hermitian surfaces in  $PG(3, s^2)$ . *Lecture Notes in computer Sci* 311. (1986), 116-124.
- [3] F. A. B. Edoukou, Codes defined by forms of degree 2 on hermitian surface and Sørensen conjecture, *Finite Fields and Their Applications*, Volume 13, Issue 3, (2007), 616-627.
- [4] F. A. B. Edoukou, Error-Correcting codes constructed from algebraic varieties. Ph. D. Thesis, Université de la Méditerranée, Marseille, France, 2007.

- [5] V. Goppa, Algebraico-Geometric codes, V. D. Goppa, Math USSR Izvestiya Vol. 21 (1983) No. 1 75-91.
- [6] R. Hartshorne, Algebraic geometry, Graduate texts in mathematics 52, Springer-Verlag, 1977.
- [7] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Clarendon press. Oxford 1985.
- [8] P. P. Spurr, Linear codes over  $GF(4)$ . Master's Thesis, University of North Carolina at Chapel Hill, USA, 1986.
- [9] I. R. Shafarevich, Basic algebraic geometry 1, Springer-Verlag, 1994.
- [10] A. B. Sørensen, Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes. Ph. D. Thesis, Aarhus, Denmark, 1991.

## Curves of genus 2 with many rational points via K3 surfaces

**Noam D. Elkies, Harvard University, elkies@math.harvard.edu**

Let  $C$  be a (smooth, projective, absolutely irreducible) curve of genus  $g \geq 2$  over a number field  $K$ . Faltings [Fa1, Fa2] proved that the set  $C(K)$  of  $K$ -rational points of  $C$  is finite, as conjectured by Mordell. The proof can even yield an effective upper bound on the size  $\#C(K)$  of this set (though not, in general, a provably complete list of points); but this bound depends on the arithmetic of  $C$ . This suggests the question of how  $\#C(K)$  behaves as  $C$  varies. Following [CHM], we define for each  $g \geq 2$  and  $K$ :

$$B(g, K) = \max_C \#C(K),$$

with  $C$  running over all curves over  $K$  of genus  $g$ ;

$$N(g, K) = \limsup_C \#C(K) [\leq B(g, K)],$$

(so infinitely many  $C$  have  $N$  rational points over  $K$ , but only finitely many have more than  $N$ ); and<sup>2</sup>  $N(g) = \max_K N(g, K)$ . It is not known whether either  $B(g, K)$  or  $N(g)$  is finite for any  $g, K$ ; even the question of whether  $N(2, \mathbf{Q}) < \infty$  is very much open. Caporaso, Harris and Mazur proved [CHM] that Lang's Diophantine conjectures [La] imply the finiteness of  $B(g, K)$ ,  $N(g)$  for any number field  $K$  and integer  $g \geq 2$ ; but the proof yields no estimates on these bounds.

While giving upper bounds seems hopeless at present, lower bounds are more tractable: we need only construct curves or families of curves with many rational points. We announce several new constructions, all using K3 surfaces of maximal Picard number. Specifically, we begin with the K3 surface  $S/\mathbf{Q}$  whose Néron–Severi group has rank 20 and discriminant  $-163$  and consists of divisor classes defined over  $\mathbf{Q}$ .<sup>3</sup> We use models of  $S$  as the double cover  $W^2 = P_6(X, Y, Z)$  of  $\mathbf{P}^2$  branched along a sextic curve  $C_6 : P_6(X, Y, Z) = 0$ . There is a finite but large number (50+) of lines  $l_i : \lambda_i(X, Y, Z) = 0$  on which  $P_6$  restricts to a perfect square (geometrically these are the tritangent lines of  $C_6$ ). The restriction  $P_6|_L$  of  $P_6$  to a generic line  $L \subset \mathbf{P}^2$  thus yields a genus-2 curve  $C_L : w^2 = P_6|_L$  with a pair of rational points above the intersection of  $L$  with each  $l_i$ .

---

<sup>2</sup>It is essential to use  $N(g, K)$  here rather than  $B(g, K)$ , because even for a single curve  $C$  over a number field  $K_0$  it is clear that by enlarging  $K \supset K_0$  we can make  $\#C(K)$  arbitrarily large.

<sup>3</sup>See [E1, p.9] for a model of  $S$  as an elliptic K3 surface with Mordell–Weil group  $(\mathbf{Z}/4\mathbf{Z}) \oplus \mathbf{Z}^4$ .

More detailed study of the configuration of the lines  $l_i$ , and of rational curves of higher degree in  $\mathbf{P}^2$  on which  $P_6$  restricts to a perfect square, leads to the following lower bounds.

**Theorem 1.** *There exist infinitely many genus-2 curves over  $\mathbf{Q}$  with at least 75 pairs of rational points. Thus  $N(2, \mathbf{Q}) \geq 150$ .*

The previous bound was Mestre's  $N(2, \mathbf{Q}) \geq 48$ ; Mestre's curves have 12 automorphisms, whereas our curves have no automorphisms other than the identity and the hyperelliptic involution.

**Theorem 2.** *There exist infinitely many genus-2 curves over  $\mathbf{Q}$  with a rational Weierstrass point and at least 59 pairs of rational points, for a total of  $\geq 119$ .*

Equivalently, there are infinitely many quintics  $P_5$  without repeated roots such that the Diophantine equation  $y^2 = P_5(x)$  has at least 119 rational solutions. We do not know of a previous record for such equations, but it would surely not exceed Mestre's 48 for an unrestricted genus-2 curve.

By varying  $L$  we have searched for individual genus-2 curves with even more rational points than promised by Theorems 1 and 2, using M. Stoll's program `ratpoints`. We did not succeed in improving Kulesz and Keller's lower bound of 588 on  $B(2, \mathbf{Q})$  [KK]. But their curve, like Mestre's curves, has 12 automorphisms, so its 588 points fall into "only" 49 orbits under the automorphism group. For genus-2 curves with minimal automorphism group, the record was 366 [St]. We raise this to at least 536 for the curve

$$y^2 = 2380^2x^6 + 947240x^5 - 29926671x^4 + 6414496x^3 + 46164876x^2 - 1258740x + 420^2.$$

For curves  $y^2 = P_5(x)$ , we find 347 points on

$$y^2 = 372468096x^5 - 830776095x^4 + 607949578x^3 - 108403791x^2 - 49652776x + 4028^2.$$

The degree-zero divisors on  $C_L$  supported on the known rational points generate a subgroup of  $\text{Jac}(C_L)$  of generic rank 18. We find infinitely many specializations of rank at least 21 over  $\mathbf{Q}$ , and two of rank at least 26, one of which is given by

$$y^2 = 80878009x^6 - 236558406x^5 - 1018244179x^4 \\ + 4436648480x^3 + 6445563464x^2 - 13620761544x + 68406^2.$$

This improves on Dreier's record of 25 [Dr] for an absolutely simple genus-2 Jacobian over  $\mathbf{Q}$ .

## References

- [CHM] Caporaso, L., Harris, J., and Mazur, B.: Uniformity of rational points. *J. Amer. Math. Soc.* **10** (1997), 1–35.
- [Dr] Dreier, R.: Examples of genus 2 curves over  $\mathbf{Q}$  with Jacobians of high Mordell–Weil rank. *Internat. Math. Res. Notices* **1997** #18, 875–880.
- [E1] Elkies, N.D.: Three lectures on elliptic surfaces and curves of high rank. arXiv:0709.2908.
- [Fa1] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366. Erratum: *Invent. Math.* **75** (1984), 381.
- [Fa2] Faltings, G.: Diophantine approximations on abelian varieties, *Ann. of Math.* **133** (1991), 549–576.

- [KK] Kulesz, L., and Keller, W.: Courbes algébriques de genre 2 et 3 possédant de nombreux points rationnels. *C. R. Acad. Sci. Paris Sér. 1* **321** (1995), 1469–1472.
- [La] Lang, S.: Hyperbolic and diophantine analysis, *Bull. AMS* **14** (1986), 159–205.
- [St] Stahlke, C.: Algebraic curves over  $\mathbf{Q}$  with many rational points and minimal automorphism group. *Internat. Math. Res. Notices* **1997**, 1–4.

## Abstract Infrastructures of Unit Rank Two

**Felix Fontein, University of Zürich, felix.fontein@math.uzh.ch**

On our poster, we want to give information on the infrastructure of a global field of unit rank two. The infrastructure of a global field is the set of all minima of a fractional ideal, together with the neighbor relation and the baby step operations [HMPLR87, Fon08c]. In the case of unit rank one, it is both used for computation of fundamental units [Buc85a] and for cryptography [SSW96, JSS07].

One main emphasis lies on visualization, both of the set of minima together with baby steps (in the sense of J. Buchmann in [Buc85a]) and the generalized Voronoï algorithm. The generalized Voronoï algorithm was first described by J. Buchmann in [Buc85a, Buc85b] for number fields. In the case of purely cubic function fields, it has been introduced by Y. Lee, R. Scheidler and C. Yarrish in [LSY03]. Some screenshots of the current experimental version of our program can be seen on the second page; the shown cases are purely cubic function fields over  $\mathbb{F}_5$ . We also plan to present a live version on our laptop during the poster session.

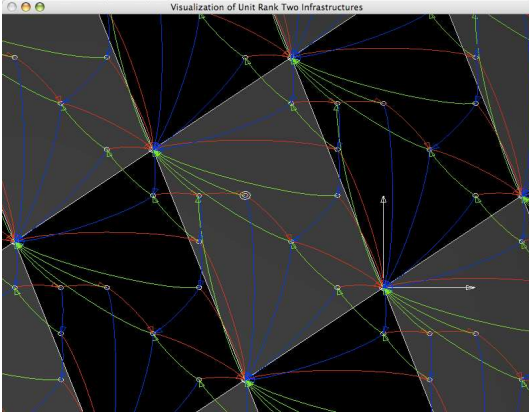
Depending on our progress, we also plan to include new results on the unit rank two case [Fon08a], which are related to the interpretation of certain unit rank one infrastructures as cyclic groups as in [Fon08b].

## References

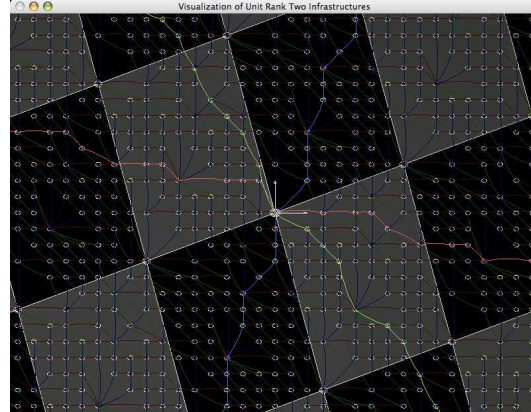
- [Buc85a] Johannes Buchmann. A generalization of Voronoï’s unit algorithm. I. *J. Number Theory*, 20(2):177–191, 1985.
- [Buc85b] Johannes Buchmann. A generalization of Voronoï’s unit algorithm. II. *J. Number Theory*, 20(2):192–209, 1985.
- [Fon08a] Felix Fontein. The infrastructure of a global field of arbitrary unit rank. In preparation.
- [Fon08b] Felix Fontein. Groups from cyclic infrastructures and Pohlig-Hellman in certain infrastructures, 2008. To appear in *Advances in Mathematics of Communications*.
- [Fon08c] Felix Fontein. The infrastructure of a global field of unit rank one, 2008. In preparation.
- [HMPLR87] Y. Hellegouarch, D. L. McQuillan, and R. Paysant-Le Roux. Unités de certains sous-anneaux des corps de fonctions algébriques. *Acta Arith.*, 48(1):9–47, 1987.
- [JSS07] M. J. Jacobson, R. Scheidler, and A. Stein. Cryptographic protocols on real hyperelliptic curves. *Adv. Math. Commun.*, 1(2):197–221, 2007.

- [LSY03] Y. Lee, R. Scheidler, and C. Yarrish. Computation of the fundamental units and the regulator of a cyclic cubic function field. *Experiment. Math.*, 12(2):211–225, 2003.
- [SSW96] R. Scheidler, A. Stein, and Hugh C. Williams. Key-exchange in real quadratic congruence function fields. *Des. Codes Cryptogr.*, 7(1-2):153–174, 1996. Special issue dedicated to Gustavus J. Simmons.

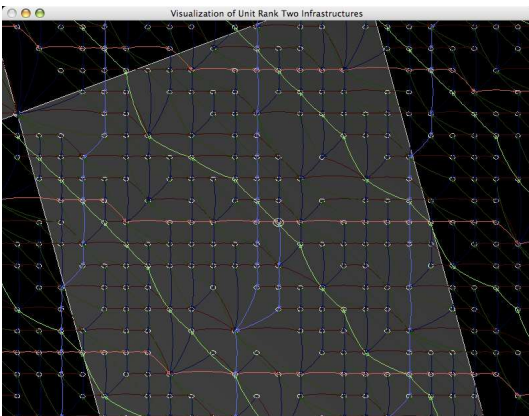
## Preview from Current Visualization Experiments



All minima with baby steps in all three different directions drawn.



The (two sided) Voronoï chains of 1 in different directions.



The Voronoï chains of a minimum together with their translates by the action of the unit group. In the blue direction, it has a non-trivial pre-period.

In all pictures, every second translate of a fundamental paralleloptope of the unit lattice is drawn in gray.

Each point's  $x$ -coordinate is the first valuation at infinity, and the  $y$ -coordinate is the second valuation at infinity. Red baby steps go in the direction of the first valuation, green baby steps into the direction of the second, and blue baby steps in the direction of the third.

## Computing $L$ -polynomials of Non-Hyperelliptic Genus 4 and 5 curves

Steven Galbraith and Raminder S. Ruprai, Royal Holloway University of London, [steven.galbraith@rhul.ac.uk](mailto:steven.galbraith@rhul.ac.uk) and [r.s.ruprai@rhul.ac.uk](mailto:r.s.ruprai@rhul.ac.uk)

Given a non-singular, projective, non-hyperelliptic curve  $C$  over  $\mathbb{F}_q$  where  $q$  is prime we present an algorithm that computes all the coefficients of the  $L$ -polynomial of  $C$ , in an expected time of  $\tilde{O}(q^2)$

in both the genus 4 and genus 5 case. We represent  $C$  as a plane model and if this model is of low degree the expected running time to recover all the coefficients of the  $L$ -polynomial can be reduced to  $\tilde{O}(q^{4/3})$ . This is an improvement on the previous best running time of  $\tilde{O}(q^{3/2})$  for genus 4 and  $\tilde{O}(q^2)$  for genus 5 given by Elkies in [2].

Let  $L(t) = \sum_{i=0}^{2g} a_i t^i$  be the  $L$ -polynomial of the curve of genus  $g$ . From the Theorem of Weil given in [5] we know that  $a_0 = 1$ ,  $a_{2g} = q^g$  and we have bounds on the other coefficients. A proof of Weil's Theorem can be found in [3]. Let  $J_C(\mathbb{F}_{q^k})$  denote the group of  $\mathbb{F}_{q^k}$ -rational points on the Jacobian Variety of  $C$ .

The algorithm consists of 2 stages. The first stage is based upon Diem's Index Calculus algorithm as described in [1]. We use an adapted version of the main algorithm in [1] to compute the  $\#J_C(\mathbb{F}_q)$ . This stage is the most time intensive and in both cases takes  $\tilde{O}(q^2)$  but for a plane model of low degree can take as little as  $\tilde{O}(q^{4/3})$ .

By simply counting the number of  $\mathbb{F}_q$ -rational points on  $C$ , which takes time  $\tilde{O}(q)$ , we have the unknown coefficients  $a_1$  and  $a_{2g-1}$  by Weil's Theorem. By Lemma 1 in [4] we have that  $\#J_C(\mathbb{F}_q) = L(1)$  and  $\#J_C(\mathbb{F}_{q^2}) = L(1) \cdot L(-1)$ . We can write  $L(-1)$  as a function of  $L(1)$  and the coefficients  $a_1, \dots, a_g$ . Using 'Baby-Step Giant-Step' techniques developed by Sutherland in [4] we can compute possible values of  $L(-1)$  and therefore possible values of  $\#J_C(\mathbb{F}_{q^2})$  that can be checked. As we have computed the values of  $L(1)$  and  $a_1$  we can find the correct value of  $L(-1)$  and the remaining unknown coefficients in time  $\tilde{O}(q^{3/4})$  for genus 4 and  $\tilde{O}(q^{5/4})$  for genus 5.

## References

- [1] Claus Diem. Index calculus in class groups of plane curves of small degree. In *Proceedings of Algorithm Number Theory Symposium - ANTS VII*, volume 4076 of *Springer-Verlag LNCS*, pages 543–557. Springer-Verlag, 2006.
- [2] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D.A. Buell and J.T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin*, volume 7 of *Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998.
- [3] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. 1996.
- [4] Andrew V. Sutherland. A generic approach to searching for jacobians. *to appear in Mathematics of Computation*, 2007.
- [5] André Weil. Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55:497–508, 1949.

## A Statistical Look at Maps of the Discrete Logarithm

**Joshua Holden and Nathan Lindle, Rose-Hulman Institute of Technology**  
 holden@rose-hulman.edu and lindlenw@rose-hulman.edu

Several algorithms in cryptography are based on the apparent difficulty of solving the discrete logarithm. It, like integer factorization, is attractive in cryptography because the inverse (modular

	100043			100057		
	Predicted	Observed	P-value	Predicted	Observed	P-value
Components	6.392	6.389	0.842	6.392	6.364	0.134
Variance	5.158	5.117	0.230	5.158	5.098	0.368
Cyclic nodes	395.417	395.303	0.920	395.445	395.858	0.842
Variance	42543.192	42227.348	0.272	42549.173	42781.153	0.690
Avg cycle	198.208	198.319	0.920	198.222	198.215	1
Variance	27210.527	<b>20392.727</b>	0	27214.349	<b>20680.648</b>	0
Avg. tail	197.212	197.178	1	197.226	196.768	0.548
Variance	27210.956	<b>7362.882</b>	0	27214.778	<b>7335.733</b>	0
Max cycle	247.495	247.261	0.764	247.512	247.302	0.920
Variance	NA	23806.218	NA	NA	23985.249	NA
Max tail	547.935	541.827	0	547.974	541.701	0
Variance	NA	26848.354	NA	NA	23985.249	NA

Table 1: (Holden-Lindle) Observed and theoretical statistics for  $p=100043$  and  $p=100057$

exponentiation) is much easier to compute. The paper “Mapping the Discrete Logarithm” by Daniel Coulter and Joshua Holden takes a look at the functional graphs that can be generated using the function  $x \mapsto g^x \pmod{p}$  where  $p$  is a prime number. It turns out the structure of the graph is largely determined by the interaction between  $g$  and  $p-1$ , and this interaction gives us an easy way to generate many binary functional graphs by choosing the correct values for  $g$ . In “Mapping the Discrete Logarithm” the authors extracted some statistics from graphs with  $p$  near 100,000. Their work showed evidence that binary functional graphs generated through modular exponentiation were very close to the theoretical values for random binary functional graphs.

This second look tells a slightly different story though. Using many of the same techniques as in the previous paper, we were able to generate values for the theoretical variance in several of the statistics which were measured. While the variance in the number of components and the number of cyclic nodes is similar to the theoretical variance for binary functional graphs, the variance in the average cycle length and the average tail length are far from what was expected. T-tests were also performed to determine if the theoretical and observed means were statistically similar. The results show that in some cases this is true, but in others the test shows that seemingly small differences could actually be quite significant. We have also applied a t-test on the variance to determine the significance of the deviation from what we expected.

Through some optimizations to the code used for the previous paper, as well as a conversion from C++ to C, we are now able to complete trials much more quickly. This has allowed us to test values of  $p$  near 200,000, and we have run tests on 33 primes between 100,00 and 200,00. The following is a tabulation of some of the statistics we have gathered, along with the variation, theoretical variation, and the P-value obtained after running a two-tailed t-test on the observed statistic comparing it to the theoretical value. The results here (unusual average cycle variation, average tail variation and maximum tail) are consistent with the rest of our results.

	106261			200087		
	Predicted	Observed	P-value	Predicted	Observed	P-value
Components	6.422	6.370	0.022	6.738	6.745	0.368
Variance	5.188	5.176	0.920	5.505	5.517	0.690
Cyclic nodes	407.551	408.433	0.690	559.620	562.252	0.006
Variance	45199.846	44488.375	0.272	85318.241	85825.849	0.230
Avg. Cycle	204.275	206.612	0.110	280.310	281.659	0.046
Variance	28907.991	<b>22003.465</b>	0	54537.238	<b>41358.233</b>	0
Avg. Tail	203.279	201.644	0.058	279.313	278.974	0.424
Variance	28908.420	<b>7578.376</b>	0	54537.668	<b>14731.689</b>	0
Max cycle	255.070	256.986	0.230	350.012	351.356	0.058
Variance	NA	25629.420	NA	NA	48068.838	NA
Max tail	564.756	554.905	0	775.570	769.207	0
Variance	NA	27602.038	NA	NA	54039.057	NA

Table 2: (Holden-Lindle) Observed and theoretical statistics for  $p=200087$  and  $p=106261$

## Minimal Heights and Regulators for Elliptic Surfaces

Sonal Jain, New York University Courant Institute of Mathematical Sciences, jain@cims.nyu.edu

Let  $K$  be a number field or function field. Let  $E$  be an elliptic curve over  $K$ , nonconstant in the case  $K$  is a function field. Néron and Tate independently showed that there is a canonical height function  $\hat{h} : E(K) \rightarrow [0, \infty)$ . In the case that  $K$  is a function field,  $\hat{h}$  takes its values in  $\mathbb{Q}$ . The quotient  $E(K)/E(K)_{tors}$  is a finitely generated free abelian group on which  $\hat{h}$  descends to a positive definite quadratic form. If  $P$  is a non-torsion point, one may ask: How small can  $\hat{h}(P)$  be? A conjecture by Lang postulates a uniform lower bound for the canonical height of non-torsion points on elliptic curves.

**Conjecture 1.** (Lang) *If  $K = \mathbb{Q}$ , then  $\hat{h}(P) \gg \log |\Delta_E|$ , and more generally if  $K$  is number field, then  $\hat{h}(P) \geq C_K \log |N_{K/\mathbb{Q}} \Delta_{E/K}|$ . Over  $\mathbb{C}(t)$  or  $\mathbb{C}(C)$  for  $C$  a curve, the same bound holds with  $\log |N_{K/\mathbb{Q}} \Delta_{E/K}|$  replaced by the discriminant degree  $12n$ .*

This conjecture was proven by Hindry-Silverman in 1988 under the hypothesis of the ABC conjecture of Masser-Oesterlé [3]. Mason had already proved the ABC conjecture over function fields [4], and hence Lang’s conjecture is true for function fields. Thus, it is natural to ask: What is the length of the shortest vector in the lattice  $E(K)/E(K)_{tors}$ , i.e. what is the best possible value of  $C_K$ ?

Hindry and Silverman determined an explicit value for  $C_K$  that was approximately  $6 \cdot 10^{-11}$ . In 2002 Elkies, using two new ideas, improved the value of  $C_K$  to about  $1/25330 \approx 3.9 \cdot 10^{-5}$  and conjectured what the best value of  $C_K$  should be [2]. First, he proved that for purposes of minimizing the canonical height  $\hat{h}$ , it suffices to consider only curves with semistable reduction. Second, he showed Hindry-Silverman’s estimation of  $\hat{h}(P)$  can be vastly improved by viewing the problem as one of linear programming.

In this poster we show how to generalize Elkies' methods to elliptic curves of rank 2. If  $E/K$  has rank bigger than 1, The determination of the constant  $C_K$  appearing in Lang's Conjecture gives one a lower bound for the volume of the fundamental domain of the lattice  $E(K)/E(K)_{tors}$ . It is natural to ask: what smallest possible volume of a fundamental domain for the lattice  $E(K)/E(K)_{tors}$ ?

Given a basis reduced  $(P, Q)$  of the lattice  $E(K)/E(K)_{tors}$ , we show how one can use linear programming to compute a lower bound for any positive form  $a\hat{h}(P) + b\langle P, Q \rangle + c\hat{h}(Q)$ , i.e.  $a, b, c$  satisfy  $0 < c, -c < a, -(a + c)/2 < b$ . For example, we prove the following:

**Theorem 1.** *Let  $(P, Q)$  be a reduced basis for a rank 2 subgroup of an elliptic surface of discriminant degree  $12n$  over  $\mathbb{P}^1(\mathbb{C})$ , so  $\hat{h}(P) \leq \hat{h}(Q)$ . The canonical height of  $Q$  is at least  $12nC_0$ , where  $C_0 = 1/3595$ . If one replace  $\mathbb{P}^1(\mathbb{C})$  by a curve of  $C$  of genus  $g$ , then  $\hat{h}(Q) \geq (12n)C_0 - (g - 1)D_0$  for some absolute constant  $D_0$ .*

Using the lower bound for  $\hat{h}(P)$ , the above result immediately gives a new lower bound for the regulator  $R(P, Q) \geq \hat{h}(P)\hat{h}(Q) - \hat{h}(P)^2/4$ .

Furthermore, we normalize by the discriminant degree  $12n$  to find lower bounds  $B_{(a,b,c)}$  for thousands of forms  $a\hat{h}(P) + b\langle P, Q \rangle + c\hat{h}(Q)$ . Each lower bound determines a plane  $ax + by + cz \geq B_{(a,b,c)}$  in the 3-dimensional space of reduced 2-dimensional quadratic forms. The asymptotically obtainable region sits on one side of the form, and by minimizing enough forms one can restrict the shape of the region in  $\mathbb{R}^3$ .

Using parameter counting heuristics, we are able to improve each lower bound and compute what should be supporting planes for the region. For example, the best possible value for the constant  $C_0$  in the theorem above is, conjecturally,  $19/5059$ . We use the data generated by computing thousands of supporting planes to draw the actual shape of the asymptotically obtainable region in  $\mathbb{R}^3$ . Furthermore, because the linear program changes in a predictable fashion as we vary the parameters  $a, b$  and  $c$ , we are able to deduce that the boundary of the region must be piecewise smooth. We make a conjecture about the actual shape of the region, and attempt to identify the elliptic surface with the minimal regulator as a point on the boundary of the region.

## References

- [1] Cox, D.A., Zucker, S.: Intersection Numbers of Elliptic Surfaces. *Inventiones Mathematicae* **53** (1979), 1-44.
- [2] Elkies, N.D.: Points of Low Height on Elliptic Curves and Surfaces I: Elliptic surfaces over  $\mathbb{P}^1$  with small  $d$ .
- [3] Hindry, M., Silverman, J.H.: The canonical height and integral points on elliptic curves. *Inventiones Mathematicae* **93** (1988), 419-450.
- [4] Mason, R.C.: *Diophantine Equations over Function Fields*, London Math. Soc. Lect. Note Ser. **96**, Cambridge Univ. Press 1984.
- [5] PARI/GP, versions 2.1.14. Bordeaux, 2000-4, <http://pari.math.u-bordeaux.fr>.
- [6] Shioda, T.: Some remarks on elliptic curves over function fields. *Astérisque* **209** (1992) *proceedings of Journées Arithmétiques 1991* (Genève), D.F. Coray and Y.-F. S. Petermann, eds., 99-114.

- [7] Silverman, J.H.: Computing Heights on Elliptic Curves. *Math. of Computation* **51** #183 (July 1988), 339-358.
- [8] Szpiro, L.: Discriminant et conducteur des courbes elliptiques. *Astérisque* **183** (1990) *Seminaire sur les Pinceaux de Courbes Elliptiques, Paris* 1988, 7-18.

## Implementing a Feasible Attack against ECC2K-130 Certicom Challenge

Ahmad Lavasani, Concordia University, [ahmad.lavasani@gmail.com](mailto:ahmad.lavasani@gmail.com)

Reza Mohammadi, Sharif University of Technology, [remohammadi@gmail.com](mailto:remohammadi@gmail.com)

Popularity of Elliptic Curve Cryptography (ECC) is increasing compared to other common Public Key Cryptosystems such as RSA and DSA due to the more efficient cryptosystem scheme that they offer in the terms of memory and bandwidth. In November 1997, Certicom introduced the ECC Challenge in order to appreciate the evaluation of ECC Cryptography. To date, all 109-bit ECC challenges have been solved and the easiest unsolved challenge is the ECC2K-130 problem.

The curve used in ECC2K-130 is the unique Koblitz Curve [5] defined over  $\text{GF}(2^{131})$ . The best known attack for a general elliptic curve is Parallel Pollard's Rho attack (known also as Pollard's Lambda) suggested by van Oorschot and Wiener [6]. This method can be improved significantly for Koblitz Curves using the method of Wiener and Zuccherato [7].

In this work, based on the implementation of Robert Harley and his team [8] who broke the last Koblitz Curve Challenge of Certicom, ECC2K-108, on April 2000 [9], we aim to mount a Pollard's Lambda attack to break ECC2K-130. We present different aspects of efficiently attacking ECC2K-130. In this way we employed new technological advancement such as SSE2 (Streaming SIMD Extensions 2) registers to speed up the arithmetic used in the attack. We also studied and compared different random walk functions and chose the function that exploits the Frobenius Automorphism while minimizing overhead in each iteration. We also improve some of critical algorithms, such as the bit-counting algorithm and  $\text{GF}(2^{131})$ -product to take advantage of CPU structure and our point representation.

By employing Berkeley Open Infrastructure for Network Computing (BOINC), we obtained a more interactive way to manage the distributed computation. This may improve the performance of the attack in several ways. For example, we can save the computation spent on a trail which does not terminate at a distinguished point. Another example is the ability of centrally supervising clients' performances and adjusting clients' parameters individually to reach their optimum performance.

The practical results we obtained from our current running implementation suggest that the attack would successfully solve the challenge in a feasible amount of time (a conservative time estimate would be less than 2 years using 20,000 partially active computers).

## References

- [1] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation* 48 (1987), pp. 203-209.

- [2] J. Silverman, J. Suzuki, Elliptic curve discrete logarithms and the index calculus, Advances in Cryptology ASIACRYPT98, Beijing, October 1998, ed. by K. Ohta and D. Pei, Lecture Notes in Computer Science 1514, Springer-Verlag, Berlin, 1998, 110125
- [3] [http://www.certicom.com/index.php?action=company,press\\_archive&view=307](http://www.certicom.com/index.php?action=company,press_archive&view=307)
- [4] [http://www.certicom.com/index.php?action=ecc,ecc\\_challenge](http://www.certicom.com/index.php?action=ecc,ecc_challenge)
- [5] N.Koblitz. CMcurves with good cryptographic properties, Proc. Crypto 91, Springer-Verlag (1992) pp. 279 287
- [6] P.C. van Oorschot, M.J. Wiener, Parallel collision search with cryptanalytic applications, Journal of Cryptology, vol 12, num 1, pp 1-28, Winter 1999, Springer-Verlag.
- [7] M. J. Wiener and R. Zuccherato, Faster Attacks on Elliptic Curve Cryptosystems, Selected Areas of Cryptography, Springer, LNCS 1556, pp. 190200, 1999.
- [8] <http://crystal.inria.fr/harley/ecdl7/readMe.html>
- [9] <http://www.inria.fr/presse/pre67.en.html>
- [10] [http://www.certicom.com/index.php?action=ecc,ecc\\_challenge](http://www.certicom.com/index.php?action=ecc,ecc_challenge)
- [11] D. Hankerson, A. J. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag, 2004.
- [12] R.Gallant, R.Lambert, and S.Vanstone, Improving the parallelized Pollard lambda search on anomalous binary curves. Math. Comp. 69 (2000), no. 232, 16991705

## A Straight Line Program Computing the Integer Greatest Common Divisor

**Sidi Mohamed Sedjelmaci, Université Paris-Nord, [sms@lipn.univ-paris13.fr](mailto:sms@lipn.univ-paris13.fr)**

While NC algorithms have been discovered for the basic arithmetic operations, the parallel complexity of some fundamental problems as integer gcd is still open, since first being raised in a paper of Cook [2]. Many authors attempt to design fast parallel integer GCD algorithms. Chor and Goldreich [1] proposed  $O(n/\log n)_\epsilon$  parallel time with  $O(n^{1+\epsilon})$  number of processors, for any  $\epsilon > 0$ . Sorenson [4] and the author [3] also suggest other parallel algorithms with the same parallel performance. Since then, no major improvements have been made. In this paper, we propose a straight line program computing the integer GCD. It has polynomial size, but the outputs are polynomials with exponential degree. This work is a first attempt to improve the parallel complexity of integer GCD, thanks to Valiant et al. [5] contraction method, and, as far as we know, it is the first straight line program for computing the integer GCD. Throughout this paper, we represent the input integers as formal strings of bits.

## The Integer GCD Algorithm

*Input:*  $x, y > 0$  odds ;

*Output:*  $\text{gcd}(x, y)$  ;

$$\begin{pmatrix} u \\ v \end{pmatrix} \leftarrow \begin{pmatrix} x \\ y \end{pmatrix} ;$$

**While** ( $u \neq v$ )

$$\begin{pmatrix} u \\ v \end{pmatrix} \leftarrow \begin{pmatrix} v \\ (u+v)/2^t \end{pmatrix} ; \text{ s.t.: } (u+v)/2^t \text{ is odd.}$$

**EndWhile**

**Return**  $u$ .

**Example:** Let  $(x, y) = (35, 19)$  we obtain in turn:

$$\begin{pmatrix} 35 \\ 19 \end{pmatrix} \rightarrow \begin{pmatrix} 19 \\ 27 \end{pmatrix} \rightarrow \begin{pmatrix} 27 \\ 23 \end{pmatrix} \rightarrow \begin{pmatrix} 23 \\ 25 \end{pmatrix} \rightarrow \begin{pmatrix} 25 \\ 3 \end{pmatrix} \rightarrow \begin{pmatrix} 3 \\ 7 \end{pmatrix} \rightarrow \begin{pmatrix} 7 \\ 5 \end{pmatrix} \rightarrow \begin{pmatrix} 5 \\ 3 \end{pmatrix} \rightarrow \begin{pmatrix} 3 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

**Theorem 1.** : *Let  $u, v \geq 1$  be two odd integers of  $n$  bits,  $n \geq 1$ , such that  $|u - v| = r2^t > 1$ , with  $r \geq 1$  odd, and  $t \geq 1$ . Let  $(u_k, v_k)$  be the sequence of consecutive values of  $u$  and  $v$ , obtained in the GCD algorithm. Then*

*i)  $\max\{u_{t+1}, v_{t+1}\} < (3/4) \max\{u, v\}$ .*

*ii) The algorithm terminates after at most  $n^2/\log_2(4/3)$  iterations and returns  $\text{gcd}(u, v)$ .*

*iii) The (**While**  $u \neq v$ ) condition can be replaced by (**For**  $i = 1$  to  $3n^2$ ) in the GCD algorithm.*

**Proof:** The case  $u = v$  is trivial. We assume that  $t \geq 3$ ,  $u \neq v$  and  $(u, v) = (v_0 + r2^t, v_0)$ , the case  $(u, v) = (u_0, u_0 + r2^t)$  is similar. The  $t$  first iterations give in turn

$$\begin{pmatrix} u_0 = v_0 + r2^t \\ v_0 \end{pmatrix} \rightarrow \begin{pmatrix} v_0 \\ v_0 + r2^{t-1} \end{pmatrix} \rightarrow \begin{pmatrix} v_0 + r2^{t-1} \\ v_0 + r2^{t-2} \end{pmatrix} \cdots \rightarrow \begin{pmatrix} v_0 + r2^{t-2} + \dots + 2r \\ 1/2^m\{v_0 + r2^{t-2} + \dots + r\} \end{pmatrix}$$

After  $t$  iterations, the integer  $2^m v_t = v_0 + r2^{t-2} + \dots + r$  is even. So  $v_t < (1/2)u_0$  and  $u_t < u_0$ . Then, after  $t + 1$  iterations, we have  $u_{t+1} = v_t < (1/2)u_0$  and  $v_{t+1} \leq (1/2)(u_t + v_t) < (3/4)u_0$ . Similarly, if  $u_{t+1} = v_{t+1}$ , it stops and returns the result:  $u_{t+1} = \text{gcd}(u, v)$ . Otherwise  $|u_{t+1} - v_{t+1}| = r2^{t^2} > 1$ , then we repeat the same process to the pair  $(u_{t+1}, v_{t+1})$ . Since  $t_1 = t < n$ ,  $t_2 < n, \dots, t_p < n$ , then after  $pn$  iterations we have  $1 \leq \max\{u_{pn}, v_{pn}\} < (3/4)^p \max\{u, v\} < (3/4)^p 2^n$ . Moreover, the **For** and the **While** versions of the algorithm give the same pair  $(u_i, v_i)$  until we reach a pair  $(u_k, v_k)$  such that  $u_k = v_k$ , with  $k \leq pn < \lfloor n^2/\log_2(4/3) \rfloor$ . At this point, the **While** version of the algorithm terminates and returns  $u_k$ , and the **For** algorithm loops with the same consecutive pair  $(u_k, v_k)$ , with  $v_k = u_k$ , until the  $(3n^2)$ th iteration. The cases  $t = 1$  or  $t = 2$  are trivial. Hence the result.

While the addition of two  $n$  bits is trivial, the instruction  $A \rightarrow A/2^t$ ,  $A > 0$ , can be done as follows (we set  $A = (a_n, a_{n-1}, \dots, a_1)$ , and  $a_{n+1} = 0$ ) :

**For**  $k = 1$  to  $n - 1$  **Do**

$$c = (1 - a_1) ;$$

**For**  $i = 1$  **to**  $n$  **Do**  $a_i = c \cdot a_{i+1} + (1 - c) \cdot a_i$   
**EndFor**  
**Return**  $A' = (a_n, a_{n-1}, \dots, a_1)$ .

The **For** version of the GCD algorithm is clearly a straight-line program using only the ring operations  $+$ ,  $-$ , and  $\times$  on bits with  $O(n^4)$  steps, however the degree of the polynomials generated by the program is exponential.

## References

- [1] B. Chor and O. Goldreich, An improved parallel algorithm for integer GCD, *Algorithmica*. **5** (1990).
- [2] S. Cook, A Taxonomy of Problems with Fast Parallel Algorithms, *Information and Control*. **64** (1985) 2–22.
- [3] M.S. Sedjelmaci, On a Parallel Lehmer-Euclid GCD Algorithm, *Proceedings of the International Symposium on Symbolic and Algebraic Computation ISSAC'2001* (2001) 303–308.
- [4] J. Sorenson, Two Fast GCD Algorithms, *J. of Algorithms* **16** (1994) 110–144.
- [5] L.G. Valiant, S. Skyum, S. Berkowitz and C. Rackoff, Fast parallel computation of polynomials using few processors, *SIAM J. Computing* **12** No.4 (1983) 641–644.

## The discrete logarithm problem on elliptic curves defined over $\mathbb{Q}$

Masaya Yasuda, Fujitsu Laboratories Ltd., myasuda@labs.fujitsu.com

The discrete logarithm problem on elliptic curves defined over a field  $K$  is: given an  $E$  be an elliptic curve over  $K$ , a point  $S \in E(K)$ , and a point  $T \in \langle S \rangle$ , find the integer  $d \in \mathbb{Z}$  such that  $T = [d]S$ . In the case where  $K = \mathbb{F}_q$  is a finite field with  $q$  elements, there are a number of ways of approaching the solution to this problem (see [1]). On the other hand, the solution to this problem in the case where  $K = \mathbb{Q}$  is the field of rational numbers is not well known. The purpose of this study is to give an algorithm for the discrete logarithm problem on elliptic curves defined over  $\mathbb{Q}$ . Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . Fix a point  $S \in E(\mathbb{Q})$ . Assume that the order of  $S$  is of infinite. The subset  $\{[d]S \mid d \in \mathbb{Z}_{\geq 0}\}$  of the group  $\langle S \rangle$  is denoted by  $\langle S \rangle_+$ . Given a point  $T \in \langle S \rangle_+$ . Our main idea to find the positive integer  $d$  such that  $T = [d]S$  is based on the method solving the discrete logarithm problem for an anomalous elliptic curve over a prime field (see [2]).

Let  $p$  be a prime number where  $E$  has good reduction. Denote  $\tilde{E}$  the reduction of  $E$  modulo  $p$  and let  $\pi : E(\mathbb{Q}_p) \rightarrow \tilde{E}(\mathbb{F}_p)$  be the reduction map (see [3]). For  $n \geq 1$ , define a subgroup of  $E(\mathbb{Q}_p)$  by

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid v(x(P)) \leq -2n\} \cup \{O\},$$

where  $v$  is the normalized  $p$ -adic valuation. We have the exact sequence of abelian groups

$$0 \rightarrow E_1(\mathbb{Q}_p) \rightarrow E(\mathbb{Q}_p) \xrightarrow{\pi} \tilde{E}(\mathbb{F}_p) \rightarrow 0$$

(see [3]). The group  $E_1(\mathbb{Q}_p)$  is isomorphic to the group of  $p\mathbb{Z}_p$ -valued points of the one-parameter formal group  $\mathcal{E}$  associated to  $E$  (see [3]). For  $n \geq 1$ , the subgroup  $E_n(\mathbb{Q}_p)$  of  $E_1(\mathbb{Q}_p)$  corresponds to the subgroup  $\mathcal{E}(p^n\mathbb{Z}_p)$  of  $\mathcal{E}(p\mathbb{Z}_p)$  under the isomorphism  $E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p)$ . Moreover, for  $n \geq 1$  there is the isomorphisms of groups

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \simeq \mathcal{E}(p^n\mathbb{Z}_p)/\mathcal{E}(p^{n+1}\mathbb{Z}_p) \simeq p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} \tag{0.1}$$

(see [3]). Let  $N$  be the order of the group  $\tilde{E}(\mathbb{F}_p)$ . Let  $h_p$  be a composition of the following maps

$$h_p : E(\mathbb{Q}) \xrightarrow{\iota} E(\mathbb{Q}_p) \xrightarrow{[N]} E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p), \tag{0.2}$$

where  $\iota$  is the inclusion map and  $[N]$  is multiplication by  $N$ . For a point  $Q \in E(\mathbb{Q})$ , we can compute  $h_p(Q) \in \mathcal{E}(p\mathbb{Z}_p)$  as follows:

$$h_p(Q) = -\frac{x}{y} \quad (\text{where } [N]Q = (x, y) \in E_1(\mathbb{Q}_p)).$$

Combining the map (0.2) with the isomorphisms (0.1), we give the following algorithm for finding the positive integer  $d$  such that  $T = [d]S$ :

Input: $E$ : elliptic curve over $\mathbb{Q}$ , $S$ : rational point of $E$ of infinite order, $T \in \langle S \rangle_+$ . Output: $d \in \mathbb{Z}_{\geq 0}$ s.t. $T = [d]S$ .
<ol style="list-style-type: none"> <li>1. <math>a \leftarrow 0</math>.</li> <li>2. While <math>a = 0</math> do:           <ol style="list-style-type: none"> <li>2.1. Choose a prime <math>p</math> at which <math>E</math> has good reduction.</li> <li>2.2. Compute the order of <math>\tilde{E}(\mathbb{F}_p)</math> and <math>N \leftarrow \#\tilde{E}(\mathbb{F}_p)</math>.</li> <li>2.3. Compute <math>[N]S = (x, y)</math> and <math>z \leftarrow -x/y</math>.</li> <li>2.4. <math>a \leftarrow z/p \pmod{p}</math>.</li> </ol> </li> <li>3. <math>n \leftarrow 0</math> and <math>\ell \leftarrow 1</math>.</li> <li>4. While <math>T \neq 0</math> do:           <ol style="list-style-type: none"> <li>4.1. Compute <math>[N]T = (x, y)</math> and <math>w \leftarrow -x/y</math>.</li> <li>4.2. <math>b \leftarrow w/p^\ell</math>.</li> <li>4.3. <math>\bar{d}_n \leftarrow b/a \pmod{p}</math> and <math>d_n \leftarrow \text{lift}(\bar{d}_n)</math>.</li> <li>4.4. <math>T \leftarrow T - [d_n]S</math> and <math>S \leftarrow [p]S</math>.</li> <li>4.5. <math>n \leftarrow n + 1</math> and <math>\ell \leftarrow \ell + 1</math>.</li> </ol> </li> <li>5. <math>d \leftarrow d_0 + d_1p + d_2p^2 + \dots + d_{n-1}p^{n-1}</math>.</li> <li>6. Return(<math>d</math>).</li> </ol>

For example, let  $E$  be the elliptic curve over  $\mathbb{Q}$  given by the Weierstrass equation

$$E : y^2 + y = x^3 - x.$$

The Mordell-Weil group  $E(\mathbb{Q})$  has rank 1 and a point  $S = (0, 0)$  is a generator for  $E(\mathbb{Q})$ . Moreover, the elliptic curve  $E$  has good reduction outside 37. Let  $T = [d]S = (x(T), y(T)) \in \langle S \rangle_+$  be as follows:

$$x(T) = -\frac{3148929681285740316}{2846153597907293521}, \quad y(T) = -\frac{2181616293371330311419201915}{4801616835579099275862827431}.$$

The above algorithm is dependent on the choice of the prime  $p$  where  $E$  has good reduction. At first, set  $p = 3$ . Then the above algorithm gives  $d_0 = 2$ ,  $d_1 = 0$ ,  $d_2 = 0$ ,  $d_3 = 1$  and

$$d = 2 + 0 \cdot p + 0 \cdot p^2 + 1 \cdot p^3 = 29.$$

Secondly, set  $p = 5$ . Then the above algorithm gives  $d_0 = 4$ ,  $d_1 = 0$ ,  $d_2 = 1$  and

$$d = 4 + 0 \cdot p + 1 \cdot p = 29.$$

This shows that for each  $p$ , the above algorithm gives the  $p$ -adic expansion of  $d$ .

The result is as follows:

**Theorem 1.** *For each  $p$ , the above algorithm gives the  $p$ -adic expansion of  $d$ .*

## References

- [1] I. Blake, G. Seroussi and N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press (1999).
- [2] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves," *Comm. Math. Univ Sancti Pauli* **47** (1998) Cpp.81-92.
- [3] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. Springer-Verlag, Berlin-Heidelberg-New York (1986).