A Family of Jacobians Suitable for Discrete Log Cryptosystems

Neal Koblitz, Dept. of Mathematics GN-50,
Univerity of Washington, Seattle WA 98195

Abstract. *We investigate the jacobians of the hyperelliptic curves $v^2 + v = u^{2g+1}$ over finite fields, and discuss which are likely to have "almost prime" order.*

1. The discrete logarithm problem in a finite abelian group A consists in finding for given $a, b \in A$ an integer m such that $a = mb$, if such m exists. In cases when the discrete log problem appears to be intractable in A, one can construct certain public key cryptosystems in which taking large multiples of a group element is the trapdoor function. The first examples of A that were considered were the multiplicative groups of finite fields. However, because some special techniques for attacking the discrete log problem are available in that case, it is useful to study other sources of finite abelian groups. In [6] we investigated the use of the jacobians of hyperelliptic curves defined over finite fields.

In the present article we consider an especially simple family of such curves. We first give an algorithm for the group law for this family. Next, we recall how to compute the number of points in terms of jacobi sums. In order for the discrete log problem to be intractible, we would like the number of points on the jacobian to be "almost prime" in the sense of [6]. Some necessary conditions for this are given, and some examples are tabulated.

2. For each positive integer g (the *genus*) we consider the hyperelliptic curve $v^2 + v = u^{2g+1}$ defined over the field $\mathbf{F}_p$ of p elements, where p is a prime not dividing $2g + 1$. Let $K = \mathbf{F}_{p^n}$. A *K-divisor* is a finite formal sum $D = \sum m_i P_i$ of $\overline{K}$-points on the curve which is fixed by any $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Its *degree* is $\sum m_i$. The finite abelian group of K-points of the jacobian, denoted $\mathrm{J}(K)$, is the quotient of the group of K-divisors of degree zero by the subgroup of divisors of rational functions (defined over K) on the curve. Every element $D \in \mathrm{J}(K)$ is uniquely associated to a pair of functions $a, b \in K[u]$ for which $\deg a \leq g$, $\deg b < \deg a$, and $b(u)^2 + b(u) - u^{2g+1}$ is divisible by $a(u)$; namely, D is the equivalence class of the g.c.d. of the divisors of the functions

S. Goldwasser (Ed.): Advances in Cryptology - CRYPTO '88, LNCS 403, pp. 94-99, 1990.

$a(u)$ and $b(u) - v$. The element D of $\mathbf{J}(K)$ is then denoted $\mathrm{div}(a, b)$. For more details, see [6] and [2].

To add two elements $\mathrm{div}(a_1, b_1)$, $\mathrm{div}(a_2, b_2) \in \mathbf{J}(K)$, one proceeds in two stages. First, let $d = d(u)$ be the g.c.d. of the three polynomials $a_1(u)$, $a_2(u)$ and $b_1(u) + b_2(u) + 1$; and choose $s_1(u)$, $s_2(u)$ and $s_3(u)$ to be polynomials in u such that $d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + 1)$. Next, set $a = a_1 a_2 / d^2$ and

$$b(u) = (s_1(u)a_1(u)b_2(u) + s_2(u)a_2(u)b_1(u) + s_3(u)(b_1(u)b_2(u) + u^{2g+1}))/d(u) \pmod{a(u)}.$$

In stage 2, if $\deg a > g$, we replace the pair (a, b) by the equivalent pair (a', b') defined by setting $a'(u) = (u^{2g+1} - b(u)^2 - b(u))/a(u)$ and $b'(u) = -b(u) - 1 \pmod{a'(u)}$. Since $\deg a' < \deg a$, successive application of this procedure leads to a pair $\mathrm{div}(a'', b'')$ with $\deg a'' \leq g$ such that $\mathrm{div}(a'', b'') = \mathrm{div}(a_1, b_1) + \mathrm{div}(a_2, b_2)$. This concludes the description of the group law in $\mathbf{J}(K)$.

3. Let g be a fixed positive integer, let $\mathbf{J}(K)$ denote the K-points of the jacobian of the curve $v^2 + v = u^{2g+1}$ defined over $\mathbf{F}_p$, where the degree $d = 2g + 1$ is prime to p, and let N_n denote $\#(\mathbf{J}(\mathbf{F}_{p^n}))$. As explained in [6], the zeta-polynomial $Z(T) = Z_g(T)$

$$Z(T) = \prod_{j=1}^{g} (T - \alpha_j)(T - \overline{\alpha}_j)$$

of the curve $v^2 + v = u^{2g+1}$ is related to N_n as follows:

$$N_n = \prod_{j=1}^{g} |1 - \alpha_j^n|^2.$$

The polynomial $Z(T)$ is computed from the number of $\mathbf{F}_{p^n}$-solutions of $v^2 + v = u^{2g+1}$ for $n = 1, 2, \ldots, g$, and the result is as follows (see, e.g., [13]).

For simplicity, we shall henceforth suppose that $d = 2g + 1$ is prime. In practice, this is the only case we shall be interested in, because of Theorem 4(1a) below. Let f denote the multiplicative order of p modulo d, so that $d | p^f - 1$, and let h denote $2g/f$. Let χ be a fixed character of $\mathbf{F}_{p^f}^*$ of order d, i.e., $\chi(\rho) = e^{2\pi i/d}$ for some generator ρ of $\mathbf{F}_{p^f}^*$. Let m_j, $1 \leq j \leq h$, run through a set of representatives of $(\mathbf{Z}/d\mathbf{Z})^*$ modulo the

subgroup $\{p, p^2, \ldots, p^f\}$, and let χ_j denote the character χ^{m_j}. For $j = 1, 2, \ldots, h$ let J_j denote the jacobi sum

$$J_j = \sum_{x \in \mathbf{F}_{p^f}} \chi_j(x)\chi_j(1-x).$$

Then J_j is a complex number of absolute value $p^{f/2}$, and

$$Z(T) = \prod_{j=1}^{h} (T^f + J_j).$$

In what follows we shall suppose that n is prime to f, in which case the preceding formula for $Z(T)$ implies that

$$N_n = \prod_{j=1}^{h} (1 + (-1)^{n+1} J_j^n).$$

For cryptographic purposes, we wish to choose g and n so that N_n is "almost prime" in the sense of [6]. For n prime this means that $N_n/N_1 = \prod_{j=1}^{g} |(1-\alpha_j^n)/(1-\alpha_j)|^2$ is prime. Clearly this is possible only if n is prime to f. A second necessary condition is that $Z_g(T)$ not factor over the rational numbers. The theorem that follows describes classes of g which must be avoided, and also a class of g for which $Z_g(T)$ is irreducible.

4. Theorem. *Let $g > 1$ be an integer. Then:*

(1) *the polynomial $Z_g(T)$ factors over the rationals* (a) *if $d = 2g+1$ is composite; or* (b) *if $d = 2g+1$ is prime and either* (i) *p is a quadratic nonresidue modulo d, or else* (ii) *p has order g modulo d and g is even.*

(2) *the polynomial $Z_g(T)$ is irreducible over the rationals if $d = 2g+1$ is a prime, g is odd, and p has order g modulo d.*

The proof of this theorem is straightforward, and will be omitted.

Corollary. *For $p = 2$ and $g < 100$, the polynomial $Z_g(T)$ is irreducible over* $\mathbf{Q}$ *for $g = 1, 3, 11, 15, 23, 35, 39, 51, 83, 95, 99$, and is reducible over* $\mathbf{Q}$ *for all other values except possibly for $g = 36, 44, 56, 63, 75$.*

5. Thus, in order to find examples of almost prime $\#\mathrm{J}(\mathbf{F}_{p^n})$, we must choose g so as not to fall in cases (1a) or (1b) of Theorem 4, and choose n prime to f.

For $p = 2$, here are the first few values of g with irreducible $Z_g(T)$:

$$Z_1(T) = T^2 + 2$$

$$Z_3(T) = T^6 - 2T^3 + 8$$

$$Z_{11}(T) = T^{22} - 48T^{11} + 2048$$

$$Z_{15}(T) = T^{30} - 6T^{25} - 16T^{20} + 352T^{15} - 512T^{10} - 6144T^5 + 32768$$

In the case $p = 2$ and $g = 3$, we tested $\#\mathbf{J}(\mathbf{F}_{2^n})$ for all primes $n < 50$, and found the following list of all the almost prime cases, i.e., where this number is 7 times a prime. (We wish to thank Andrew Odlyzko for verifying primality of the three large unfactored integers below, using the Cohen-Lenstra algorithm.)

n	$\#\mathbf{J}(\mathbf{F}_{2^n})$
2	$7 \cdot 11$
13	$7 \cdot 7\,85367\,56663$
29	$7 \cdot 2\,21060\,72130\,09916\,78702\,83191$
47	$7 \cdot 39\,82275\,92830\,90398\,46698\,24190\,47946\,07809\,61207$

6. Remarks. 1. If $\mathbf{J}$ is the jacobian of $v^2 + v = u^d$ with $d = 2g + 1$ prime, it is not hard to show that $d | \#\mathbf{J}(\mathbf{F}_p)$. This prevents $\#\mathbf{J}(\mathbf{F}_p)$ from being prime for all but very small values of p and d (since $\#\mathbf{J}(\mathbf{F}_p) \sim p^g$). However, $\#\mathbf{J}(\mathbf{F}_p)/d \sim p^g/d$ may be prime. For example, in the first table above, for $g = 15$, $d = 31$, $p = 2$ we have $\#\mathbf{J}(\mathbf{F}_2) = Z_{15}(1) = 31 \cdot 853$.

2. For fixed prime p, part (2) of Theorem 4 gives us a source of jacobians over $\mathbf{F}_p$ with irreducible $Z_g(T)$: the curves $v^2 + v = u^d$ with d a prime $\equiv 3 \pmod 4$ for which p is the square of a primitive root modulo d. For fixed p, the frequency with which such d occur is given by a (generalization of a) conjecture of E. Artin, according to which there is a positive constant probability that a prime $d \equiv 3 \pmod 4$ has p as the square of a primitive root. For example, when $p = 2$ (in which case $d \equiv 7 \pmod 8$), since 2 must be a quadratic residue modulo d), the number of $d < x$ with the desired property is conjecturally asymptotic to

$$c\frac{x}{4 \log x}, \qquad c = \prod_{\text{primes } l \geq 3} \left(1 - \frac{1}{l(l-1)}\right) \approx 0.746 \cdots.$$

More information about Artin's conjecture can be found in [11, p. 80-83 and 222-225].

3. In searching for suitable jacobians of curves over finite fields $\mathbf{F}_{p^n}$, one can take several points of view. (a) One can fix the genus g and the field (i.e., p and n), and let the coefficients of the curve's equation vary. One expects, roughly speaking, that as these coefficients vary the number of points on the jacobian will be nearly uniformly distributed in an interval of the form $\left(p^{gn} - cp^{(g-1/2)n},\ p^{gn} + cp^{(g-1/2)n}\right)$. This has been studied in detail in the cases $g = 1$, $n = 1$, p large (see [8]) and $g = 2$, $n = 1$, p large (see [1]).

(b) One can fix a curve with rational coefficients, and consider the jacobian of its reduction modulo p (i.e., over $\mathbf{F}_p$) as p varies. In the case $g = 1$, conjectural formulas for the probability that the corresponding elliptic curve has a prime number of points are given in [5].

(c) One can fix $\mathbf{F}_p$ (or a finite extension of $\mathbf{F}_p$) and also fix a curve with coefficients in that field. One then considers $\mathbf{J}(\mathbf{F}_{p^n})$, i.e., the group of points of $\mathbf{J}$ with coordinates in a finite extension of the field of definition, which is chosen so that $\#\mathbf{J}(\mathbf{F}_{p^n})$ is "almost prime" in the sense of [6]. For this, the curve must have been chosen so that its zeta-polynomial $Z(T) = \prod_{j=1}^{2g}(T - \alpha_j)$ is irreducible over $\mathbf{Q}$, i.e., all of the α_j are conjugates of $\alpha = \alpha_1$. Suppose, for example, that the curve is defined over $\mathbf{F}_p$, it has irreducible zeta-polynomial, and one considers extensions $\mathbf{F}_{p^n}$ of prime degree n. In that case one is interested in primality of the norm of the algebraic integer $(\alpha^n - 1)/(\alpha - 1)$ as n varies. This is a generalization of the Mersenne prime problem, and most likely the frequency of occurrence of prime values is predicted by a heuristic estimate of the same form as in the classical Mersenne case (see [12]).

The point of view (c) is illustrated in the second table above.

(d) One can fix the field of definition $\mathbf{F}_{p^n}$ and examine a family of curves of varying genus. This was the point of view in the first table above. Even if p^n is small, the size of the group of points will grow rapidly with the genus, since it is of order p^{gn}. If one wants $\#\mathbf{J}$ to be a prime number or the product of a large prime and a small factor, then a necessary condition is that the zeta-polynomial be irreducible.

One advantage of point of view (d), in addition to the possible desirability of having one more parameter to vary (the genus g), is that one can limit oneself to curves with special symmetry properties (e.g., the family considered in this report), and this seems to make it possible to compute the number of points much more rapidly (and also carry out the algorithm for finding multiples of points somewhat faster) than in the case of a general curve.

In conclusion, we recall that, because index calculus type algorithms for finding discrete logs in $\mathbf{F}_{p^n}^*$ apparently do not carry over to elliptic curves (see [9]) or hyperelliptic curves, the only known algorithm for finding discrete logs in $\mathbf{J}(\mathbf{F}_{p^n})$ takes

time roughly proportional to the square root of the largest prime factor in $\#J(\mathbf{F}_{p^n})$. Thus, as far as we know, discrete log cryptosystems using $J(\mathbf{F}_{p^n})$ seem to be secure for relatively small p^n (even when $p = 2$). From the standpoint of implementation, this feature may outweigh the added time required to compute the more complicated group operation.

References

[1] L. M. Adleman and Ming-Deh A. Huang, "Recognizing primes in random polynomial time," preprint.

[2] D. Cantor, "Computing in the jacobian of a hyperelliptic curve," *Math. of Computation*, **48** (1987), 95-101.

[3] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.

[4] N. Koblitz, "Elliptic curve cryptosystems," *Math. of Computation*, **48** (1987), 203-209.

[5] N. Koblitz, "Primality of the number of points on an elliptic curve over a finite field," *Pacific J. Math.*, **131** (1988), 157-165.

[6] N. Koblitz, "Hyperelliptic cryptosystems," to appear.

[7] N. Koblitz and D. Rohrlich, "Simple factors in the jacobian of a Fermat curve," *Can. J. Math.*, **30** (1978), 1183-1205.

[8] H. W. Lenstra, Jr., "Factoring integers with elliptic curves," Report 86-18, Mathematisch Instituut, Universiteit van Amsterdam, 1986.

[9] V. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology - Crypto '85*, Springer-Verlag, New York, 1986, 417-426.

[10] A. M. Odlyzko, "Discrete logarithms and their cryptographic significance," *Advances in Cryptography: Proceedings of Eurocrypt 84*, Springer-Verlag, New York, 1985, 224-314.

[11] D. Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985.

[12] S. S. Wagstaff, Jr., "Divisors of Mersenne Numbers," *Math. of Computation*, **40** (1983), 385-397.

[13] A. Weil, "Numbers of solutions of equations in finite fields," *Bull. Amer. Math. Soc.*, **55** (1949), 497-508.