GENERATORS OF JACOBIANS OF HYPERELLIPTIC CURVES

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. This paper provides a probabilistic algorithm to determine generators of the m-torsion subgroup of the Jacobian of a hyperelliptic curve of genus two.

1. Introduction

Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$, and $\mathcal{J}_C$ the Jacobian of C. Consider the rational subgroup $\mathcal{J}_C(\mathbb{F}_p)$. $\mathcal{J}_C(\mathbb{F}_p)$ is a finite abelian group, and

$$\mathcal{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \mathbb{Z}/n_3\mathbb{Z} \oplus \mathbb{Z}/n_4\mathbb{Z},$$

where $n_i \mid n_{i+1}$ and $n_2 \mid p-1$. Frey and Rück (1994) shows that if $m \mid p-1$, then the discrete logarithm problem in the rational m-torsion subgroup $\mathcal{J}_C(\mathbb{F}_p)[m]$ of $\mathcal{J}_C(\mathbb{F}_p)$ can be reduced to the corresponding problem in $\mathbb{F}_p^\times$ (Frey and Rück, 1994, corollary 1). In the proof of this result it is claimed that the non-degeneracy of the Tate pairing can be used to determine whether r random elements of the finite group $\mathcal{J}_C(\mathbb{F}_p)[m]$ in fact is an independent set of generators of $\mathcal{J}_C(\mathbb{F}_p)[m]$. This paper provides an explicit, probabilistic algorithm to determine generators of $\mathcal{J}_C(\mathbb{F}_p)[m]$.

In short, the algorithm outputs elements γ_i of the Sylow-ℓ subgroup Γ_ℓ of the rational subgroup $\Gamma = \mathcal{J}_C(\mathbb{F}_p)$, such that $\Gamma_\ell = \bigoplus_i \langle \gamma_i \rangle$ in the following steps:

(1) Choose random elements $\gamma_i \in \Gamma_\ell$ and $h_j \in \mathcal{J}_C(\mathbb{F}_p)$, $i, j \in \{1, \dots, 4\}$.
(2) Use the non-degeneracy of the tame Tate pairing τ to *diagonalize* the sets $\{\gamma_i\}_i$ and $\{h_j\}_j$ with respect to τ; i.e. modify the sets such that $\tau(\gamma_i, h_j) = 1$ if $i \neq j$ and $\tau(\gamma_i, h_i)$ is an ℓ^{th} root of unity.
(3) If $\prod_i |\gamma_i| < |\Gamma_\ell|$ then go to step 1.
(4) Output the elements γ_1, γ_2, γ_3 and γ_4.

The key ingredient of the algorithm is the diagonalization in step 2; this process will be explained in section 5.

We will write $\langle \gamma_i | i \in I \rangle = \langle \gamma_i \rangle_i$ and $\bigoplus_{i\in I} \langle \gamma_i \rangle = \bigoplus_i \langle \gamma_i \rangle$ if the index set I is clear from the context.

2. Hyperelliptic curves

A hyperelliptic curve is a smooth, projective curve $C \subseteq \mathbb{P}^n$ of genus at least two with a separable, degree two morphism $\phi : C \to \mathbb{P}^1$. In the rest of this

Date: April 25, 2007. The author is a Ph.D.-student at the Department of Mathematical Sciences, Faculty of Science, University of Aarhus.

2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 14Q05, 94A60.

Key words and phrases. Jacobians, hyperelliptic curves, complex multiplication, cryptography.

Research supported in part by a Ph.D. grant from CRYPTOMAThIC.

paper, let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$ of characteristic $p > 2$. By the Riemann-Roch theorem there exists an embedding $\psi : C \to \mathbb{P}^2$, mapping C to a curve given by an equation of the form

$$y^2 = f(x),$$

where $f \in \mathbb{F}_p[x]$ is of degree six and have no multiple roots (see Cassels and Flynn, 1996, chapter 1).

The set of principal divisors $\mathcal{P}(C)$ on C constitutes a subgroup of the degree zero divisors $\mathrm{Div}_0(C)$. The Jacobian $\mathcal{J}_C$ of C is defined as the quotient

$$\mathcal{J}_C = \mathrm{Div}_0(C)/\mathcal{P}(C).$$

Consider the subgroup $\mathcal{J}_C(\mathbb{F}_p) < \mathcal{J}_C$ of $\mathbb{F}_p$-rational elements. There exist numbers n_i, such that

$$\mathcal{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \mathbb{Z}/n_3\mathbb{Z} \oplus \mathbb{Z}/n_4\mathbb{Z}, \tag{1}$$

where $n_i \mid n_{i+1}$ and $n_2 \mid p-1$ (see Frey and Lange, 2006, proposition 5.78, p. 111). We wish to determine generators of the m-torsion subgroup $\mathcal{J}_C(\mathbb{F}_p)[m] < \mathcal{J}_C(\mathbb{F}_p)$, where $m \mid |\mathcal{J}_C(\mathbb{F}_p)|$ is the largest number such that $\ell \mid p-1$ for every prime number $\ell \mid m$.

3. Finite abelian groups

Miller (2004) shows the following theorem.

Theorem 1. *Let G be a finite abelian group of torsion rank r. Then for $s \geq r$ the probability that a random s-tuple of elements of G generates G is at least*

$$\frac{C_r}{\log\log|G|}$$

if $s = r$, and at least C_s if $s > r$, where $C_s > 0$ is a constant depending only on s (and not on $|G|$).

Proof. (Miller, 2004, theorem 3, p. 251) □

Combining theorem 1 and equation (1), we expect to find generators of $\Gamma[m]$ by choosing 4 random elements $\gamma_i \in \Gamma[m]$ in approximately $\frac{\log\log|\Gamma[m]|}{C_4}$ attempts.

To determine whether the generators are independent, i.e. if $\langle\gamma_i\rangle_i = \bigoplus_i \langle\gamma_i\rangle$, we need to know the subgroups of a cyclic ℓ-group G. These are determined uniquely by the order of G, since

$$\{0\} < \langle\ell^{n-1}g\rangle < \langle\ell^{n-2}g\rangle < \cdots < \langle\ell g\rangle < G$$

are the subgroups of the group $G = \langle g\rangle$ of order ℓ^n. The following corollary is an immediate consequence of this observation.

Corollary 2. *Let U_1 and U_2 be cyclic subgroups of a finite group G. Assume U_1 and U_2 are ℓ-groups. Let $\langle u_i\rangle < U_i$ be the subgroups of order ℓ. Then*

$$U_1 \cap U_2 = \{e\} \iff \langle u_1\rangle \cap \langle u_2\rangle = \{e\}.$$

Here $e \in G$ is the neutral element.

4. The tame Tate pairing

Let $\Gamma = \mathfrak{J}_C(\mathbb{F}_p)$ be the rational subgroup of the Jacobian. Consider a number $\lambda \mid \gcd(|\Gamma|, p-1)$. Let $g \in \Gamma[\lambda]$ and $h = \sum_i a_i P_i \in \Gamma$ be divisors with no points in common, and let

$$\overline{h} \in \Gamma/\lambda\Gamma$$

denote the class containing the divisor h. Furthermore, let $f \in \mathbb{F}_p(C)$ be a rational function on C with divisor $\operatorname{div}(f) = \lambda g$. Set $f(h) = \prod_i f(P_i)^{a_i}$. Then

$$e_\lambda(g, \overline{h}) = f(h)$$

is a well-defined pairing $\Gamma[\lambda] \times \Gamma/\lambda\Gamma \longrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^\lambda$, the *Tate pairing*; cf. Galbraith (2005). Raising to the power $\frac{p-1}{\lambda}$ gives a well-defined element in the subgroup $\mu_\lambda < \mathbb{F}_p^\times$ of the λ^{th} roots of unity. This pairing

$$\tau_\lambda : \Gamma[\lambda] \times \Gamma/\lambda\Gamma \longrightarrow \mu_\lambda$$

is called the *tame Tate pairing*.

Since the class $\overline{h}$ is represented by the element $h \in \Gamma$, we will write $\tau_\lambda(g, h)$ instead of $\tau_\lambda(g, \overline{h})$. Furthermore, we will omit the subscript λ and just write $\tau(g, h)$, since the value of λ will be clear from the context.

Hess (2004) gives a short and elementary proof of the following theorem.

Theorem 3. *The tame Tate pairing τ is bilinear and non-degenerate.*

Corollary 4. *For every element $g \in \Gamma$ of order λ an element $h \in \Gamma$ exists, such that $\mu_\lambda = \langle \tau(g, h) \rangle$.*

Proof. (Silverman, 1986, corollary 8.1.1., p. 98) gives a similar result for elliptic curves and the Weil pairing. The proof of this result only uses that the pairing is bilinear and non-degenerate. Hence it applies to corollary 4. □

Remark 5. In the following we only need the existence of the element $h \in \Gamma$, such that $\mu_\lambda = \langle \tau(g, h) \rangle$; we do not need to find it.

5. Generators of $\Gamma[m]$

As in the previous section, let $\Gamma = \mathfrak{J}_C(\mathbb{F}_p)$ be the rational subgroup of the Jacobian. We are searching for elements $\gamma_i \in \Gamma[m]$ such that $\Gamma[m] = \bigoplus_i \langle \gamma_i \rangle$. As an abelian group, $\Gamma[m]$ is the direct sum of its Sylow subgroups. Hence, we only need to find generators of the Sylow subgroups of $\Gamma[m]$.

Set $N = |\Gamma|$ and let $\ell \mid \gcd(N, p-1)$ be a prime number. Choose four random elements $\gamma_i \in \Gamma$. Let $\Gamma_\ell < \Gamma$ be the Sylow-ℓ subgroup of Γ, and set $N_\ell = |\Gamma_\ell|$. Then $\frac{N}{N_\ell}\gamma_i \in \Gamma_\ell$. Hence, we may assume that $\gamma_i \in \Gamma_\ell$. If all the elements γ_i are equal to zero, then we choose other elements $\gamma_i \in \Gamma$. Hence, we may assume that some of the elements γ_i are non-zero.

Let $|\gamma_i| = \lambda_i$, and re-enumerate the γ_i's such that $\lambda_i \leq \lambda_{i+1}$. Since some of the γ_i's are non-zero, we may choose an index $\nu \leq 4$, such that $\lambda_\nu \neq 1$ and $\lambda_i = 1$ for $i < \nu$. Choose λ_0 minimal such that $\lambda = \frac{\lambda_\nu}{\lambda_0} \mid p-1$. Then $\mathbb{F}_p$ contains an element ζ of order λ. Now set $g_i = \frac{\lambda_i}{\lambda}\gamma_i$, $\nu \leq i \leq 4$. Then $g_i \in \Gamma[\lambda]$, $\nu \leq i \leq 4$. Finally, choose four random elements $h_i \in \Gamma$.

Let

$$\tau : \Gamma[\lambda] \times \Gamma/\lambda\Gamma \longrightarrow \langle \zeta \rangle$$

be the tame Tate pairing. Define remainders α_{ij} modulo λ by

$$\tau(g_i, h_j) = \zeta^{\alpha_{ij}}.$$

By corollary 4, for any of the elements g_i we can choose an element $h \in \Gamma$, such that $|\tau(g_i, h)| = \lambda$. Assume that $\Gamma/\lambda\Gamma = \langle \overline{h}_1, \overline{h}_2, \overline{h}_3, \overline{h}_4 \rangle$. Then $\overline{h} = \sum_i q_i \overline{h}_i$, and so

$$\tau(g_i, h) = \zeta^{\alpha_{i1}q_1 + \alpha_{i2}q_2 + \alpha_{i3}q_3 + \alpha_{i4}q_4}.$$

If $\alpha_{ij} \equiv 0 \pmod{\ell}$, $1 \leq j \leq 4$, then $|\tau(g_i, h)| < \lambda$. Hence, if $\Gamma/\lambda\Gamma = \langle \overline{h}_1, \overline{h}_2, \overline{h}_3, \overline{h}_4 \rangle$, then for all $i \in \{\nu, \dots, 4\}$ we can choose a $j \in \{1, \dots, 4\}$, such that $\alpha_{ij} \not\equiv 0 \pmod{\ell}$.

Enumerate the h_i such that $\alpha_{44} \not\equiv 0 \pmod{\ell}$. Now assume a number $j < 4$ exists, such that $\alpha_{4j} \not\equiv 0 \pmod{\lambda}$. Then $\zeta^{\alpha_{4j}} = \zeta^{\beta_1 \alpha_{44}}$, and replacing h_j with $h_j - \beta_1 h_4$ gives $\alpha_{4j} \equiv 0 \pmod{\lambda}$. So we may assume that

$$\alpha_{41} \equiv \alpha_{42} \equiv \alpha_{43} \equiv 0 \pmod{\lambda} \qquad \text{and} \qquad \alpha_{44} \not\equiv 0 \pmod{\ell}.$$

Assume similarly that a number $j < 4$ exists, such that $\alpha_{j4} \not\equiv 0 \pmod{\lambda}$. Now set $\beta_2 \equiv \alpha_{44}^{-1}\alpha_{j4} \pmod{\lambda}$. Then $\tau(g_j - \beta_2 g_4, h_4) = 1$. So we may also assume that

$$\alpha_{14} \equiv \alpha_{24} \equiv \alpha_{34} \equiv 0 \pmod{\lambda}.$$

Repeating this process recursively, we may assume that

$$\alpha_{ij} \equiv 0 \pmod{\lambda} \qquad \text{and} \qquad \alpha_{44} \not\equiv 0 \pmod{\ell}.$$

Again $\nu \leq i \leq 4$ and $1 \leq j \leq 4$.

The discussion above is formalized in the following algorithm.

Algorithm 1. As input we are given a hyperelliptic curve C of genus two defined over a prime field $\mathbb{F}_p$, the number $N = |\Gamma|$ of $\mathbb{F}_p$-rational elements of the Jacobian, and a prime factor $\ell \mid \gcd(N, p-1)$. The algorithm outputs elements $\gamma_i \in \Gamma_\ell$ of the Sylow-ℓ subgroup Γ_ℓ of Γ, such that $\langle \gamma_i \rangle_i = \bigoplus_i \langle \gamma_i \rangle$ in the following steps.

(1) Compute the order N_ℓ of the Sylow-ℓ subgroup of Γ.
(2) Choose elements $\gamma_i \in \Gamma$, $i \in I := \{1, 2, 3, 4\}$. Set $\gamma_i := \frac{N}{N_\ell}\gamma_i$.
(3) Choose elements $h_j \in \Gamma$, $j \in J := \{1, 2, 3, 4\}$.
(4) Set $K := \{1, 2, 3, 4\}$.
(5) For k' from 0 to 3 do the following:
  (a) Set $k := 4 - k'$.
  (b) If $\gamma_i = 0$, then set $I := I \setminus \{i\}$. If $|I| = 0$, then go to step 2.
  (c) Compute the orders $\lambda_\kappa := |\gamma_\kappa|$, $\kappa \in K$. Re-enumerate the γ_κ's such that $\lambda_\kappa \leq \lambda_{\kappa+1}$, $\kappa \in K$. Set $I := \{5 - |I|, 6 - |I|, \dots, 4\}$.
  (d) Set $\nu := \min(I)$, and choose λ_0 minimal such that $\lambda := \frac{\lambda_\nu}{\lambda_0} \mid p - 1$. Set $g_\kappa := \frac{\lambda_\kappa}{\lambda}\gamma_\kappa$, $\kappa \in I \cap K$.
    (i) If $g_k = 0$, then go to step 6.
    (ii) If $\tau(g_k, h_j)^{\lambda/\ell} = 1$ for all $j \leq k$, then go to step 3.
  (e) Choose a primitive λ^{th} root of unity $\zeta \in \mathbb{F}_p$. Compute α_{kj} and $\alpha_{\kappa k}$ from $\tau(g_k, h_j) = \zeta^{\alpha_{kj}}$ and $\tau(g_\kappa, h_k) = \zeta^{\alpha_{\kappa k}}$, $1 \leq j < k$, $\kappa \in I \cap K$. Re-enumerate $h_1, \dots, h_k$ such that $\alpha_{kk} \not\equiv 0 \pmod{\ell}$.
  (f) For $1 \leq j < k$, set $\beta \equiv \alpha_{kk}^{-1}\alpha_{kj} \pmod{\lambda}$ and $h_j := h_j - \beta h_k$.
  (g) For $\kappa \in I \cap K \setminus \{k\}$, set $\beta \equiv \alpha_{kk}^{-1}\alpha_{\kappa k} \pmod{\lambda}$ and $\gamma_\kappa := \gamma_\kappa - \beta\frac{\lambda_k}{\lambda_\kappa}\gamma_k$.
  (h) Set $K := K \setminus \{k\}$.
(6) Output γ_1, γ_2, γ_3 and γ_4.

Remark 6. Algorithm 1 consists of a small number of

(1) calculations of orders of elements $\gamma \in \Gamma_\ell$,
(2) multiplications of elements $\gamma \in \Gamma$ with numbers $a \in \mathbb{Z}$,
(3) additions of elements $\gamma_1, \gamma_2 \in \Gamma$,
(4) evaluations of pairings of elements $\gamma_1, \gamma_2 \in \Gamma$ and
(5) solving the discrete logarithm problem in $\mathbb{F}_p$, i.e. to determine α from ζ and $\xi = \zeta^\alpha$.

By (Miller, 2004, proposition 9), the order $|\gamma|$ of an element $\gamma \in \Gamma_\ell$ can be calculated in time $O(\log^3 N_\ell)\mathcal{A}_\Gamma$, where $\mathcal{A}_\Gamma$ is the time for adding two elements of Γ. A multiple $a\gamma$ or a sum $\gamma_1 + \gamma_2$ is computed in time $O(\mathcal{A}_\Gamma)$. By Frey and Rück (1994), the pairing $\tau(\gamma_1, \gamma_2)$ of two elements $\gamma_1, \gamma_2 \in \Gamma$ can be evaluated in time $O(\log N_\ell)$. Finally, by Pohlig and Hellmann (1978) the discrete logarithm problem in $\mathbb{F}_p$ can be solved in time $O(\log p)$. We may assume that addition in Γ is easy, i.e. that $\mathcal{A}_\Gamma < O(\log p)$. Hence algorithm 1 runs in expected time $O(\log p)$.

Careful examination of algorithm 1 gives the following lemma.

Lemma 7. *Let Γ_ℓ be the Sylow-ℓ subgroup of Γ, $\ell \mid p-1$. Algorithm 1 determines elements $\gamma_i \in \Gamma_\ell$ and $h_i \in \Gamma$, $1 \le i \le 4$, such that one of the following cases holds.*

(1) $\alpha_{11}\alpha_{22}\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\lambda}$, $i \ne j$, $i, j \in \{1, 2, 3, 4\}$.
(2) $\gamma_1 = 0$, $\alpha_{22}\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\lambda}$, $i \ne j$, $i, j \in \{2, 3, 4\}$.
(3) $\gamma_1 = \gamma_2 = 0$, $\alpha_{33}\alpha_{44} \not\equiv 0 \pmod{\ell}$ *and* $\alpha_{ij} \equiv 0 \pmod{\lambda}$, $i \ne j$, $i, j \in \{3, 4\}$.
(4) $\gamma_1 = \gamma_2 = \gamma_3 = 0$.

If $|\gamma_i| = \lambda_i$, then $\lambda_i \le \lambda_{i+1}$. Set $\nu = \min\{i|\lambda_i \ne 1\}$, and define λ_0 as the least number, such that $\lambda = \frac{\lambda_\nu}{\lambda_0} \mid p-1$. Set $g_i = \frac{\lambda_i}{\lambda}\gamma_i$, $\nu \le i \le 4$. Then the numbers α_{ij} above are determined by

$$\tau(g_i, h_j) = \zeta^{\alpha_{ij}},$$

where τ is the tame Tate pairing $\Gamma[\lambda] \times \Gamma/\lambda\Gamma \to \mu_\lambda = \langle\zeta\rangle$.

Theorem 8. *Algorithm 1 determines elements γ_1, γ_2, γ_3 and γ_4 of the Sylow-ℓ subgroup of Γ, $\ell \mid p-1$, such that $\langle\gamma_i\rangle_i = \bigoplus_i \langle\gamma_i\rangle$.*

Proof. Choose elements $\gamma_i, h_i \in \Gamma$ such that the conditions of lemma 7 are fulfilled. Set $\lambda_i = |\gamma_i|$, and let $\nu = \min\{i|\lambda_i \ne 1\}$. Define λ_0 as the least number, such that $\lambda = \frac{\lambda_\nu}{\lambda_0} \mid p-1$. Set $g_i = \frac{\lambda_i}{\lambda}\gamma_i$. Then the α_{ij}'s from lemma 7 are determined by

$$\tau(g_i, h_j) = \zeta^{\alpha_{ij}}.$$

We only consider case 1 of lemma 7, since the other cases follow similarly. We start by determining $\langle\gamma_3\rangle \cap \langle\gamma_4\rangle$. Assume that $g_3 = ag_4$. Then

$$1 = \tau(g_3, h_4) = \tau(ag_4, h_4) = \zeta^{a\alpha_{44}},$$

i.e. $a \equiv 0 \pmod{\lambda}$. Hence $\langle\gamma_3\rangle \cap \langle\gamma_4\rangle = \{0\}$. Then we determine $\langle\gamma_2\rangle \cap \langle\gamma_3, \gamma_4\rangle$. Assume $g_2 = ag_3 + bg_4$. Then

$$1 = \tau(g_2, h_3) = \tau(ag_3, h_3) = \zeta^{a\alpha_{33}},$$

i.e. $a \equiv 0 \pmod{\lambda}$. In the same way,

$$1 = \tau(g_2, h_4) = \zeta^{b\alpha_{44}},$$

i.e. $b \equiv 0 \pmod{\lambda}$. Hence $\langle\gamma_2\rangle \cap \langle\gamma_3, \gamma_4\rangle = \{0\}$. Similarly $\langle\gamma_1\rangle \cap \langle\gamma_2, \gamma_3, \gamma_4\rangle = \{0\}$. Hence $\langle\gamma_i\rangle_i = \bigoplus_i \langle\gamma_i\rangle$. □

From theorem 8 we get the following probabilistic algorithm to determine generators of the m-torsion subgroup $\Gamma[m] < \Gamma$, where $m \mid |\Gamma|$ is the largest divisor of $|\Gamma|$ such that $\ell \mid p-1$ for every prime number $\ell \mid m$.

Algorithm 2. As input we are given a hyperelliptic curve C of genus two defined over a prime field $\mathbb{F}_p$, the number $N = |\Gamma|$ of $\mathbb{F}_p$-rational elements of the Jacobian, and the prime factors $p_1, \dots, p_n$ of $\gcd(N, p-1)$. The algorithm outputs elements $\gamma_i \in \Gamma[m]$ such that $\Gamma[m] = \bigoplus_i \langle \gamma_i \rangle$ in the following steps.

(1) Set $\gamma_i := 0$, $1 \leq i \leq 4$. For $\ell \in \{p_1, \dots, p_n\}$ do the following:
   (a) Use algorithm 1 to determine elements $\tilde{\gamma}_i \in \Gamma_\ell$, $1 \leq i \leq 4$, such that $\langle \tilde{\gamma}_i \rangle_i = \bigoplus_i \langle \tilde{\gamma}_i \rangle$.
   (b) If $\prod_i |\tilde{\gamma}_i| < |\Gamma_\ell|$, then go to step 1a.
   (c) Set $\gamma_i := \gamma_i + \tilde{\gamma}_i$, $1 \leq i \leq 4$.

(2) Output γ_1, γ_2, γ_3 and γ_4.

Remark 9. By remark 6, algorithm 2 has expected running time $O(\log p)$. Hence algorithm 2 is an efficient, probabilistic algorithm to determine generators of the m-torsion subgroup $\Gamma[m] < \Gamma$, where $m \mid |\Gamma|$ is the largest divisor of $|\Gamma|$ such that $\ell \mid p-1$ for every prime number $\ell \mid m$.

Remark 10. The strategy of algorithm 1 can be applied to *any* finite, abelian group Γ with bilinear, non-degenerate pairings into cyclic groups. For the strategy to be efficient, the pairings must be efficiently computable, and the discrete logarithm problem in the cyclic groups must be easy.

References

J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2. London Mathematical Society Lecture Note Series. Cambridge University Press, 1996.

G. Frey and T. Lange. Varieties over Special Fields. In H. Cohen and G. Frey, editors, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pp. 87–113. Chapman & Hall/CRC, 2006.

G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, vol. 62, pp. 865–874, 1994.

S. Galbraith. Pairings. In I.F. Blake, G. Seroussi and N.P. Smart, editors, *Advances in Elliptic Curve Cryptography.* London Mathematical Society Lecture Note Series, vol. 317, pp. 183–213. Cambridge University Press, 2005.

F. Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math.*, no. 82, pp. 28–32, 2004.

V.S. Miller. The Weil Pairing and Its Efficient Calculation. *J. Cryptology*, no. 17, pp. 235–261, 2004.

S. Pohlig and M. Hellmann. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Inform. Theory*, vol. 24, pp. 106–110, 1978.

J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.

Department of Mathematical Sciences, University of Aarhus, Ny Munkegade, Building 1530, DK-8000 Aarhus C

E-mail address: cr@imf.au.dk