UNIVERSITY OF AARHUS
DEPARTMENT OF MATHEMATICS

ISSN: 1397–4076

EMBEDDING DEGREE OF HYPERELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

by Christian Robenhagen Ravnshøj

Preprint Series No.: 5

May 2007

2007/05/22

Ny Munkegade, Bldg. 1530
DK-8000 Aarhus C, Denmark

http://www.imf.au.dk
institut@imf.au.dk

EMBEDDING DEGREE OF HYPERELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. Consider the Jacobian of a genus two curve defined over a finite field and with complex multiplication. In this paper we show that if the ℓ-Sylow subgroup of the Jacobian is not cyclic, then the embedding degree of the Jacobian with respect to ℓ is one.

1. Introduction

In elliptic curve cryptography it is essential to know the number of points on the curve. Cryptographically we are interested in elliptic curves with large cyclic subgroups. Such elliptic curves can be constructed. The construction is based on the theory of complex multiplication, studied in detail by Atkin and Morain (1993). It is referred to as the *CM method*.

Koblitz (1989) suggested the use of hyperelliptic curves to provide larger group orders. Therefore constructions of hyperelliptic curves are interesting. The CM method for elliptic curves has been generalized to hyperelliptic curves of genus two by Spallek (1994), and efficient algorithms have been proposed by Weng (2003) and Gaudry *et al* (2005).

Both algorithms take as input a primitive, quartic CM field K (see section 3 for the definition of a CM field), and give as output a hyperelliptic genus two curve C defined over a prime field $\mathbb{F}_p$. A prime number p is chosen such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_K$, where $\mathfrak{O}_K$ is the ring of integers of K. We have $K = \mathbb{Q}(\eta)$ and $K \cap \mathbb{R} = \mathbb{Q}(\sqrt{D})$, where $\eta = i\sqrt{a + b\xi}$ and

$$\xi = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \mod 4, \\ \sqrt{D}, & \text{if } D \equiv 2, 3 \mod 4. \end{cases}$$

In this paper, the following theorem is established.

Theorem 1. *Let C be a hyperelliptic curve of genus two defined over $\mathbb{F}_p$ with $\mathrm{End}(C) \simeq \mathfrak{O}_K$, where K is a primitive, quartic CM field as defined in definition 6. Assume that the p-power Frobenius under this isomorphism is given by the number $\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta$, where ξ and η are given as above and $c_i \in \mathbb{Z}$. Consider a prime number $\ell \mid |\mathcal{J}_C(\mathbb{F}_p)|$ with $\ell \neq p$, $\ell \nmid D$ and $\ell \nmid c_2$. Assume that the ℓ-Sylow subgroup of $\mathcal{J}_C(\mathbb{F}_p)$ is not cyclic. Then $p \equiv 1 \mod \ell$, i.e. the embedding degree of $\mathcal{J}_C(\mathbb{F}_p)$ with respect to ℓ is one.*

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 $\phi : C \to \mathbb{P}^1$. Let C be a hyperelliptic curve of

2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 11G15, 14Q05, 94A60.
Key words and phrases. Jacobians, hyperelliptic curves, complex multiplication, cryptography.
Research supported in part by a PhD grant from CRYPTOMAThIC.

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 0 divisors $\mathrm{Div}_0(C)$. The Jacobian $\mathcal{J}_C$ of C is defined as the quotient

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

Let $\ell \neq p$ be a prime number. The ℓ^n-torsion subgroup $\mathcal{J}_C[\ell^n] < \mathcal{J}_C$ of elements of order dividing ℓ^n is then (Lang, 1959, theorem 6, p. 109)

$$\mathcal{J}_C[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}, \tag{1}$$

i.e. $\mathcal{J}_C[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank four.

The order of p modulo ℓ plays an important role in cryptography.

Definition 2 (Embedding degree)**.** Consider a prime number ℓ dividing the order of $\mathcal{J}_C(\mathbb{F}_p)$, where ℓ is different from p. The embedding degree of $\mathcal{J}_C(\mathbb{F}_p)$ with respect to ℓ is the least number k, such that $p^k \equiv 1 \mod \ell$.

An endomorphism $\varphi : \mathcal{J}_C \to \mathcal{J}_C$ induces a $\mathbb{Z}_\ell$-linear map

$$\varphi_\ell : T_\ell(\mathcal{J}_C) \to T_\ell(\mathcal{J}_C)$$

on the ℓ-adic Tate-module $T_\ell(\mathcal{J}_C)$ of $\mathcal{J}_C$ (Lang, 1959, chapter VII, §1). The map φ_ℓ is given by φ as described in the following diagram:

$$\begin{array}{ccccccc}
\cdots & \xrightarrow{[\ell]} & \mathcal{J}_C[\ell^{n+1}] & \xrightarrow{[\ell]} & \mathcal{J}_C[\ell^n] & \xrightarrow{[\ell]} & \cdots \\
 & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} & & \\
\cdots & \xrightarrow{[\ell]} & \mathcal{J}_C[\ell^{n+1}] & \xrightarrow{[\ell]} & \mathcal{J}_C[\ell^n] & \xrightarrow{[\ell]} & \cdots
\end{array}$$

Here, the horizontal maps $[\ell]$ are the multiplication-by-ℓ map. Hence, φ is represented by a matrix $M \in \mathrm{Mat}_{4\times 4}(\mathbb{Z}/\ell\mathbb{Z})$ on $\mathcal{J}_C[\ell]$. Let $P(X) \in \mathbb{Z}[X]$ be the characteristic polynomial of φ (see Lang, 1959, pp. 109–110), and let $P_M(X) \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of the restriction of φ to $\mathcal{J}_C[\ell]$. Then (Lang, 1959, theorem 3, p. 186)

$$P(X) \equiv P_M(X) \mod \ell. \tag{2}$$

Since C is defined over $\mathbb{F}_p$, the mapping $(x, y) \mapsto (x^p, y^p)$ is an isogeny on C. This isogeny induces the p-power Frobenius endomorphism φ on the Jacobian $\mathcal{J}_C$. The characteristic polynomial $P(X)$ of φ is of degree four (Tate, 1966, theorem 2, p. 140), and by the definition of $P(X)$ (see Lang, 1959, pp. 109–110),

$$|\mathcal{J}_C(\mathbb{F}_p)| = P(1),$$

i.e. the number of $\mathbb{F}_p$-rational elements of the Jacobian is determined by $P(X)$.

3. CM fields

An elliptic curve E with $\mathbb{Z} \neq \mathrm{End}(E)$ is said to have *complex multiplication*. Let K be an imaginary, quadratic number field with ring of integers $\mathfrak{O}_K$. K is a *CM field*, and if $\mathrm{End}(E) \simeq \mathfrak{O}_K$, then E is said to have *CM by* $\mathfrak{O}_K$. More generally a CM field is defined as follows.

Definition 3 (CM field)**.** A number field K is a CM field, if K is a totally imaginary, quadratic extension of a totally real number field K_0.

In this paper only CM fields of degree $[K : \mathbb{Q}] = 4$ are considered. Such a field is called a *quartic* CM field.

Remark 4. Consider a quartic CM field K. Let $K_0 = K \cap \mathbb{R}$ be the real subfield of K. Then K_0 is a real, quadratic number field, $K_0 = \mathbb{Q}(\sqrt{D})$. By a basic result on quadratic number fields, the ring of integers of K_0 is given by $\mathfrak{O}_{K_0} = \mathbb{Z} + \xi\mathbb{Z}$, where

$$\xi = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \mod 4, \\ \sqrt{D}, & \text{if } D \equiv 2, 3 \mod 4. \end{cases}$$

Since K is a totally imaginary, quadratic extension of K_0, a number $\eta \in K$ exists, such that $K = K_0(\eta)$, $\eta^2 \in K_0$. The number η is totally imaginary, and we may assume that $\eta = i\eta_0$, $\eta_0 \in \mathbb{R}$. Furthermore we may assume that $-\eta^2 \in \mathfrak{O}_{K_0}$; so $\eta = i\sqrt{a + b\xi}$, where $a, b \in \mathbb{Z}$.

Let C be a hyperelliptic curve of genus two. Then C is said to have CM by $\mathfrak{O}_K$, if $\mathrm{End}(C) \simeq \mathfrak{O}_K$. The structure of K determines whether C is irreducible. More precisely, the following theorem holds.

Theorem 5. *Let C be a hyperelliptic curve of genus two with* $\mathrm{End}(C) \simeq \mathfrak{O}_K$*, where K is a quartic CM field. Then C is reducible if, and only if, $K/\mathbb{Q}$ is Galois with Galois group* $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*.*

Proof. (Shimura, 1998, proposition 26, p. 61). □

Theorem 5 motivates the following definition.

Definition 6 (Primitive, quartic CM field)**.** A quartic CM field K is called primitive if either $K/\mathbb{Q}$ is not Galois, or $K/\mathbb{Q}$ is Galois with cyclic Galois group.

The CM method for constructing curves of genus two with prescribed endomorphism ring is described in detail by Weng (2003) and Gaudry *et al* (2005). In short, the CM method is based on the construction of the class polynomials of a primitive, quartic CM field K with real subfield K_0 of class number $h(K_0) = 1$. The prime number p has to be chosen such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_K$. By Weng (2003) we may assume that $x \in \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$.

4. Properties of $\mathcal{J}_C(\mathbb{F}_p)$

Consider a primitive, quartic CM field K with real subfield K_0 of class number $h(K_0) = 1$, and let p be an uneven prime number such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$. The main result of this paper, given by the following theorem, concerns a curve of genus two with $\mathfrak{O}_K$ as endomorphism ring.

Theorem 7. *With the notation as in remark 4, let C be a hyperelliptic curve of genus two defined over $\mathbb{F}_p$ with $\mathrm{End}(C) \simeq \mathfrak{O}_K$. Assume that the p-power Frobenius under this isomorphism is given by the number $\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta$, where $c_i \in \mathbb{Z}$. Consider a prime number $\ell \mid |\mathcal{J}_C(\mathbb{F}_p)|$ with $\ell \neq p$, $\ell \nmid D$ and $\ell \nmid c_2$. Assume that the ℓ-Sylow subgroup of $\mathcal{J}_C(\mathbb{F}_p)$ is not cyclic. Then $p \equiv 1 \mod \ell$, i.e. the embedding degree of $\mathcal{J}_C(\mathbb{F}_p)$ with respect to ℓ is one.*

Proof. Consider a prime number $\ell \mid |\mathcal{J}_C(\mathbb{F}_p)|$ with $\ell \nmid pc_2D$. If $\ell = 2$, then obviously $p \equiv 1 \mod \ell$. Hence we may assume that $\ell \neq 2$. Assume that the ℓ-Sylow subgroup S of $\mathcal{J}_C(\mathbb{F}_p)$ is not cyclic. Then S contains a subgroup $U \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$. So

$$(\mathbb{Z}/\ell\mathbb{Z})^2 < \mathcal{J}_C(\mathbb{F}_p)[\ell] < \mathcal{J}_C[\ell].$$

Let $\{e_1, e_2\} \subseteq \mathcal{J}_C(\mathbb{F}_p)$ be a basis of $(\mathbb{Z}/\ell\mathbb{Z})^2$. Expand by the isomorphism (1) this set to a basis $\{e_1, e_2, f_1, f_2\}$ of $\mathcal{J}_C[\ell]$. It then follows that 1 is an eigenvalue of the Frobenius with eigenvectors e_1 and e_2, i.e. 1 is an eigenvalue of multiplicity at least two.

First we assume that $D \equiv 2, 3 \mod \ell$. Let $P(X)$ be the characteristic polynomial of the Frobenius. Since the conjugates of ω are given by $\omega_1 = \omega$, $\omega_2 = \overline{\omega}_1$, ω_3 and $\omega_4 = \overline{\omega}_3$, where

$$\omega_3 = c_1 - c_2\sqrt{D} + i(c_3 - c_4\sqrt{D})\sqrt{a - b\sqrt{D}},$$

it follows that

$$P(X) = \prod_{i=1}^{4}(X - \omega_i) = X^4 - 4c_1X^3 + (2p + 4(c_1^2 - c_2^2D))X^2 - 4c_1pX + p^2.$$

Since 1 is an eigenvalue of the Frobenius of multiplicity at least two, the characteristic polynomial $P(X)$ is divisible by $(X-1)^2$ modulo ℓ. Now,

$$P(X) = Q(X) \cdot (X-1)^2 + R(X),$$

where

$$\begin{aligned} R(X) = 4(1 - 3c_1 - (c_1 - 1)p + 2(c_1^2 - c_2^2D))X \\ + p^2 - 2p - 4(c_1^2 - c_2^2D) + 8c_1 - 3. \end{aligned}$$

Since $R(X) \equiv 0 \mod \ell$, it follows that

$$1 - 3c_1 - (c_1 - 1)p + 2(c_1^2 - c_2^2D) \equiv 0 \mod \ell. \tag{3}$$

Since $|\mathcal{J}_C(\mathbb{F}_p)| = P(1)$, we know that

$$(p+1)^2 - 4c_1(p+1) + 4(c_1^2 - c_2^2D) \equiv 0 \mod \ell. \tag{4}$$

By equation (3) we see that $4(c_1^2 - c_2^2D) \equiv 2(c_1 - 1)p - 2 + 6c_1 \mod \ell$. Substituting this into equation (4) we get

$$(p+1)^2 - 4c_1(p+1) + 2(c_1 - 1)p - 2 + 6c_1 \equiv 0 \mod \ell;$$

so either $p \equiv 1 \mod \ell$ or $p \equiv 2c_1 - 1 \mod \ell$. Assume $p \equiv 2c_1 - 1 \mod \ell$. Then

$$R(X) \equiv 4c_2^2D(-2X + 1) \equiv 0 \mod \ell.$$

Since $\ell \nmid 2c_2D$, this is a contradiction. So if $D \equiv 2, 3 \mod 4$, then $p \equiv 1 \mod \ell$.

Now consider the case $D \equiv 1 \mod 4$. We now have

$$\omega_3 = c_1 + c_2\frac{1 - \sqrt{D}}{2} + i\left(c_3 + c_4\frac{1 - \sqrt{D}}{2}\right)\sqrt{a + b\frac{1 - \sqrt{D}}{2}},$$

and it follows that the characteristic polynomial of the Frobenius is given by

$$P(X) = X^4 - 2cX^3 + (2p + c^2 - c_2^2d)X^2 - 2pcX + p^2,$$

where $c = 2c_1 + c_2$. We see that $P(X) = Q(X)(X-1)^2 + R(X)$, where

$$R(X) = ((4-2c)p + 2c^2 - 6c - 2c_2^2 D + 4)X + p^2 - 2p - 3 + 4c - c^2 + c_2^2 D.$$

Since $R(X) \equiv 0 \mod \ell$, it follows that

$$p^2 - 2p - 3 + 4c - c^2 + c_2^2 D \equiv 0 \mod \ell, \tag{5}$$

and since $|\mathcal{J}_C(\mathbb{F}_p)| = P(1)$, we know that

$$(p+1)^2 - 2c(p+1) + c^2 - c_2^2 D \equiv 0 \mod \ell. \tag{6}$$

From equation (5) and (6) it follows that

$$p^2 - cp + c - 1 \equiv 0 \mod \ell,$$

i.e. $p \equiv 1 \mod \ell$ or $p \equiv c - 1 \mod \ell$. Assume $p \equiv c - 1 \mod \ell$. Then

$$R(X) \equiv c_2^2 D(-2X + 1) \equiv 0 \mod \ell,$$

again a contradiction. So if $D \equiv 1 \mod 4$, then $p \equiv 1 \mod \ell$. □

Consider the case $\ell \mid c_2$. Then the characteristic polynomial of the Frobenius modulo ℓ is given by

$$P(X) \equiv (X^2 - 2c_1 X + p)^2 \mod \ell,$$

independently of the remainder of D modulo 4. Observe that

$$X^2 - 2c_1 X + p = (X + 1 - 2c_1)(X - 1) + p - 2c_1 + 1.$$

Hence, $p \equiv 2c_1 - 1 \mod \ell$, i.e.

$$P(X) \equiv (X-1)^2 (X-p)^2 \mod \ell.$$

So the following theorem holds.

Theorem 8. *With the notation as in remark 4, let C be a hyperelliptic curve of genus two defined over $\mathbb{F}_p$ with $\mathrm{End}(C) \simeq \mathfrak{O}_K$. Assume that the p-power Frobenius under this isomorphism is given by the number $\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta$, where $c_i \in \mathbb{Z}$. Consider a prime number $\ell \mid |\mathcal{J}_C(\mathbb{F}_p)|$ with $\ell \neq p$, $\ell \mid c_2$. Assume that the ℓ-Sylow subgroup of $\mathcal{J}_C(\mathbb{F}_p)$ is not cyclic. Then either*

1. $\mathcal{J}_C(\mathbb{F}_p)[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, *or*
2. $p \equiv 1 \mod \ell$ *and* $\mathcal{J}_C(\mathbb{F}_p)[\ell] = \mathcal{J}_C[\ell]$.

Proof. If $p \not\equiv 1 \mod \ell$, then 1 is not an eigenvalue of the Frobenius of multiplicity three, i.e. $\mathcal{J}_C(\mathbb{F}_p)[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$. If $p \equiv 1 \mod \ell$, then 1 is an eigenvalue of the Frobenius of multiplicity four, i.e. $\mathcal{J}_C(\mathbb{F}_p)[\ell] = \mathcal{J}_C[\ell]$. □

5. Applications

Let C be a hyperelliptic curve of genus two defined over $\mathbb{F}_p$ with $\mathrm{End}(C) \simeq \mathfrak{O}_K$. Write

$$\mathcal{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z} \times \mathbb{Z}/n_4\mathbb{Z}, \tag{7}$$

where $n_i \mid n_{i+1}$ and $n_2 \mid p - 1$ (see Frey and Lange, 2006, proposition 5.78, p. 111). We recall the following result on the prime divisors of the number n_2.

Theorem 9. *With the notion as above, let $\ell \mid n_2$ be an odd prime number. Then $\ell \leq Q$, where*

$$Q = \max\{a, D, a^2 - b^2 D\},$$

if $D \equiv 2, 3 \mod 4$, and

$$Q = \max\{a, D, 4a(a+b) - b^2(D-1), aD + 2b(D-1)\},$$

if $D \equiv 1 \mod 4$. If $\ell > D$, then $c_1 \equiv 1 \mod \ell$ and $c_2 \equiv 0 \mod \ell$.

Proof. Ravnshøj (2007a). □

Let the Frobenius be given by the number $\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta$, $c_i \in \mathbb{Z}$, and consider a prime number $\ell \mid |\mathcal{J}_C(\mathbb{F}_p)|$, $\ell \neq p$.

Corollary 1. *If $\ell \nmid c_2$ and $\ell > Q$, then the ℓ-Sylow subgroup S of $\mathcal{J}_C(\mathbb{F}_p)$ is either of rank two and $p \equiv 1 \mod \ell$, or S is cyclic.*

By Ravnshøj (2007b), if $p \equiv 1 \mod \ell$, then there exists an efficient, probabilistic algorithm to determine generators of the ℓ-Sylow subgroup of $\mathcal{J}_C(\mathbb{F}_p)$. Hence the following corollary holds.

Corollary 2. *If $\ell \nmid D$ and $\ell \nmid c_2$, then there exists an efficient, probabilistic algorithm to determine generators of the ℓ-Sylow subgroup S of $\mathcal{J}_C(\mathbb{F}_p)$.*

Proof. If $p \equiv 1 \mod \ell$, then the corollary is given by Ravnshøj (2007b). If $p \not\equiv 1 \mod \ell$, then S is cyclic by theorem 7. Assume $|S| = \ell^n$. Then S has $\ell^n - \ell^{n-1}$ elements of order ℓ^n. Hence the probability that a random element $\sigma \in S$ generates S is $1 - \ell^{-1}$, and choosing random elements $\sigma \in S$ until an element of order ℓ^n is found will be an efficient, probabilistic algorithm to determine generators of S. □

6. Acknowledgement

I would like to thank my supervisor Johan P. Hansen for inspiration on theorem 8.

References

A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, vol. 61, pp. 29–68, 1993.

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.

P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng. The p-adic CM-Method for Genus 2. 2005. `http://arxiv.org`.

N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, vol. 1, pp. 139–150, 1989.

S. Lang. *Abelian Varieties*. Interscience, 1959.

C.R. Ravnshøj. *Large Cyclic Subgroups of Jacobians of Hyperelliptic Curves*. 2007a. `http://arxiv.org`.

C.R. Ravnshøj. *Generators of Jacobians of Hyperelliptic Curves*. 2007b. `http://arxiv.org`.

G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998.

A.-M. Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*. Ph.D. thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.

J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, vol. 2, pp. 134–144, 1966.

A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, vol. 72, pp. 435–458, 2003.

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

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