# Ordinary abelian varieties having small embedding degree

Paula Cristina Valença

*joined work with*

Steven Galbraith and James McKee

P.Valenca@rhul.ac.uk

Royal Holloway University of London

# Plan

- On the problem of using abelian varieties with small embedding degree
  - Introducing the MNT curves
- Extending MNT curves with co-factors
- The genus $2$ case

# Embedding degree

$\mathbb{F}_q$ finite field, $J/\mathbb{F}_q$ Jacobian of a curve.

The *embedding degree* is the smallest positive integer $k$

$$r \mid q^k - 1$$

where $r$ is the largest prime divisor of $\#J$.
In particular, $r \mid \Phi_k(q)$ *($k$-cyclotomic polynomial)*.

# Embedding degree

$\mathbb{F}_q$ finite field, $J/\mathbb{F}_q$ Jacobian of a curve.

The *embedding degree* is the smallest positive integer $k$

$$r \mid q^k - 1$$

where $r$ is the largest prime divisor of $\#J$.
In particular, $r \mid \Phi_k(q)$ *($k$-cyclotomic polynomial)*.

*Motivation:* use of Weil and Tate pairings in cryptographic protocols - provide a mapping from $G \subset J$ to $\mathbb{F}^*_{q^k}$.

# Cyclotomic Polynomials

| $\mathbf{n}$ | $\varphi(\mathbf{n})$ | $\mathbf{\Phi_n(q)}$ |
|---|---|---|
| 1 | 1 | $q-1$ |
| 2 | 1 | $q+1$ |
| 3 | 2 | $q^2+q+1$ |
| 4 | 2 | $q^2+1$ |
| 5 | 4 | $q^4+q^3+q^2+q+1$ |
| 6 | 2 | $q^2-q+1$ |
| 7 | 6 | $q^6+q^5+q^4+q^3+q^2+q+1$ |
| 8 | 4 | $q^4+1$ |
| 9 | 6 | $q^6+q^3+1$ |
| 10 | 4 | $q^4-q^3+q^2-q+1$ |
| 11 | 10 | $q^{10}+q^9+q^8+q^7+q^6+q^5+q^4+q^3+q^2+q+1$ |
| 12 | 4 | $q^4-q^2+1$ |

# Suitable elliptic curves

- **supersingular**
- **MNT curves** (*Miyaji, Nakabayashi, Takano*)

# Suitable elliptic curves

- **supersingular** : for example,
  - $q = 3^{2m}, n = 3^{2m} \pm 3^m + 1$ $(k = 3)$
  - $q = 3^{2m+1}, n = 3^{2m+1} \pm 3^{m+1} + 1$ $(k = 6)$
- **MNT curves** (*Miyaji, Nakabayashi, Takano*)

# Suitable elliptic curves

- **supersingular**
- **MNT curves** (*Miyaji, Nakabayashi, Takano*) : for $k \in \{3, 4, 6\}$ ($\varphi(k) = 2$), find $q(l), t(l) \in \mathbb{Z}[l]$ *s.t.*

$$n(l) := q(l) - t(l) + 1 \mid \Phi_k(q(l))$$

| **k** | **q** | **t** | **n** |
|---|---|---|---|
| $3$ | $12l^2 - 1$ | $-1 \pm 6l$ | $12l^2 \pm 6l + 1$ |
| $4$ | $l^2 + l + 1$ | $-l, l + 1$ | $l^2 + 2l + 2, l^2 + 1$ |
| $6$ | $4l^2 + 1$ | $1 \pm 2l$ | $4l^2 \pm 2l + 1$ |

# Extending these methods

- Extending MNT curves with co-factors
- The genus 2 case

# Extending these methods

- Extending MNT curves with co-factors
  - instead of $n \mid \Phi_k(q)$, have $r \mid \Phi_k(q)$ where $n = hr$ ($r$ is the largest such factor)
- The genus 2 case

# co-factors: $k = 6$

Write

$$\lambda r = \Phi_6(q) = q^2 - q + 1$$

# co-factors: $k = 6$

Write

$$\lambda r = \Phi_6(q) = q^2 - q + 1$$

$$\Rightarrow \frac{n}{q}\big((q+t+1) - \lambda/h\big) = 3 - \frac{t^2}{q}$$

# co-factors: $k = 6$

Write

$$\lambda r = \Phi_6(q) = q^2 - q + 1$$

$$\Rightarrow \frac{n}{q}\big((q+t+1) - \lambda/h\big) = 3 - \frac{t^2}{q}$$

Writing $\lambda/h = \lfloor \lambda/h \rfloor + \epsilon$, $\epsilon > 0$ $(\gcd(\lambda, h) = 1)$ and using Hasse's bound

$$-4/3 + \epsilon < q + t + 1 - \lfloor \lambda/h \rfloor < 3 + \epsilon < 4$$

for $q > 64$, and so $v := q + t + 1 - \lfloor \lambda/h \rfloor \in \{-1, 0, 1, 2, 3\}$

# co-factors (cont.)

Substituting $v$ in

$$n(v - \epsilon) = 3q - t^2$$

leads to solving a quadratic in $t$ whose discriminant must be a square.
Writing $\epsilon = u/h$, find $x$ *s.t.*

$$x^2 = M + Nq$$

where $M, N \in \mathbb{Z}$, depending solely on $u$ and $h$.

# co-factors (cont.)

Substituting $v$ in

$$n(v-\epsilon) = 3q - t^2$$

leads to solving a quadratic in $t$ whose discriminant must be a square.

Writing $\epsilon = u/h$, find $x$ *s.t.*

$$x^2 = M + Nq$$

where $M, N \in \mathbb{Z}$, depending solely on $u$ and $h$.

$M$ must be a quadratic residue $\mod N$.

# Valid pairs $(q, t)$ for $k = 6$

| h | q | t |
|---|---|---|
| 1 | $4l^2 + 1$ | $\pm 2l + 1$ |
| 2 | $8l^2 + 6l + 3$ | $2l + 2$ |
| | $24l^2 + 6l + 1$ | $-6l$ |
| 3 | $12l^2 + 4l + 3$ | $-2l + 1$ |
| | $84l^2 + 16l + 1$ | $-14l - 1$ |
| | $84l^2 + 128l + 49$ | $14l + 11$ |
| $\dots$ | $\dots$ | $\dots$ |

- Curves can be constructed by using Complex Multiplication, solving a Pell-type equation.

# Extending these methods

- Extending MNT curves with co-factors
- The genus 2 case
  - Embedding degree $k \in \{5, 8, 10, 12\}$ ($\varphi(k) = 4$)
  - Heuristics suggest similar results (in frequency)
  - …but the earlier method no longer applies

# Extending these methods

- Extending MNT curves with co-factors
- The genus 2 case
  - Embedding degree $k \in \{5, 8, 10, 12\}$ ($\varphi(k) = 4$)
  - Heuristics suggest similar results (in frequency)
  - ...but the earlier method no longer applies

Alternative approach: consider $q = q(l)$ as a quadratic polynomial in $\mathbb{Z}[l]$ and note that we are looking to factorise

$$\Phi_k(q(l)) = n_1(l)n_2(l)$$

# Factoring $\Phi_k(q(l))$

1. Let $q(l)$ be a quadratic polynomial over $\mathbb{Q}[l]$. Then, one of two cases may occur:
   (a) $\Phi_k(q(l))$ is irreducible over the rationals, with degree $2\varphi(k)$
   (b) $\Phi_k(q(l)) = n_1(l)n_2(l)$, where $n_1(l), n_2(l)$ are irreducible over the rationals, degree $\varphi(k)$
2. A criterion for case (b) is $q(z) = \zeta_k$ having a solution in $\mathbb{Q}(\zeta_k)$, where $\zeta_k$ is a primitive complex $k$-th root of unity.

*(Note: applies to both elliptic and hyperelliptic curves. . . )*

# Two approaches

Two equivalent approaches present themselves

1. expand $\Phi_k(q(l)) = n_1(l)n_2(l)$ and try to solve the Diophantine system of equations
2. solve $q(z) = \zeta_k$ over $\mathbb{Q}(\zeta_k)$

# Retrieving the MNT curves

Here $k \in \{3, 4, 6\}$ and $[\mathbb{Q}(\zeta_k) : \mathbb{Q}] = 2$.
Example ($k = 6$): Completing the square and clearing denominators, we get

$$w^2 + b = c\zeta_6$$

where $b, c \in \mathbb{Z}$ and $w \in \mathbb{Z}(\zeta_6)$. Writing $w = A + B\zeta_6$, leads to solving

$$\begin{cases} B(2A+B) & = c \\ B^2 - A^2 & = b \end{cases}$$

and, by fixing $b$, retrieving the previous examples.

# Hyperelliptic curves (genus 2)

Here $k \in \{5, 8, 10, 12\}$ and $[\mathbb{Q}(\zeta_k) : \mathbb{Q}] = 4$.
As before, $w^2 + b = c\zeta_k$, but

$$w = A + B\zeta_k + C\zeta_k^2 + D\zeta_k^3$$

which now leads to four quadratics in integers $A, B, C$ and $D$, two of which homogeneous that must vanish.

# An example: $k = 8$

$\underline{k = 8}$:

$$\begin{cases} 2AD + 2BC & = 0 \\ 2AC + B^2 - D^2 & = 0 \end{cases}$$

$$\Rightarrow D^3 - B^2 D + 2BC^2 = 0$$

# An example: $k = 8$

$\underline{k = 8}$:

$$\begin{cases} 2AD + 2BC & = 0 \\ 2AC + B^2 - D^2 & = 0 \end{cases}$$

$$\Rightarrow D^3 - B^2D + 2BC^2 = 0$$

- latter corresponds to an elliptic curve with rank $0$
- none of its four points leads to a solution to the system

# An example: $k = 8$

$\underline{k = 8}$:

$$\begin{cases} 2AD + 2BC & = 0 \\ 2AC + B^2 - D^2 & = 0 \end{cases}$$

$$\Rightarrow D^3 - B^2 D + 2BC^2 = 0$$

- latter corresponds to an elliptic curve with rank $0$
- none of its four points leads to a solution to the system
- there exists no rational quadratic polynomial $q(l)$ *s.t.* $\Phi_8(q(l))$ splits.

# Some solutions

| **k** | **h** | **q** |
|---|---|---|
| 5 | 1 | $l^2$ |
| | 404 | $1010l^2 + 525l + 69$ |
| 10 | 4 | $10l^2 + 5l + 2$ |
| | 11 | $11l^2 + 10l + 3$ |
| | 11 | $55l^2 + 40l + 8$ |
| 12 | 1 | $2^{2m+1}$ |

$q = 2l^2, 6l^2$ ( $k = 12$ )

$q = 5l^2$ ( $k = 5$ )

# Questions

P.Valenca@rhul.ac.uk