On prime-order elliptic curves with embedding degrees $k = 3, 4$ and 6

Koray Karabina and Edlyn Teske

University of Waterloo

ANTS VIII, Banff, May 20, 2008

Outline

1. Introduction
   - Pairings and embedding degree
   - MNT curves: $k = 3, 4, 6$
2. Constructing MNT Curves
   - CM method
   - Frequency of MNT curves
3. Our Contributions
   - Relation between the MNT curves with $k = 4$ and $k = 6$
   - A deep analysis of MNT equations
   - A lower bound on MNT curves with bounded discriminant
4. Conclusion

Outline

1 Introduction
- Pairings and embedding degree
- MNT curves: $k = 3, 4, 6$

2 Constructing MNT Curves
- CM method
- Frequency of MNT curves

3 Our Contributions
- Relation between the MNT curves with $k = 4$ and $k = 6$
- A deep analysis of MNT equations
- A lower bound on MNT curves with bounded discriminant

4 Conclusion

Pairings and Embedding Degree

- $\mathbb{F}_q$ is a finite field, μ_r is the set of rth roots of unity in $\bar{\mathbb{F}}_q$
- $E/\mathbb{F}_q$ is an elliptic curve over $\mathbb{F}_q$
- $\#E(\mathbb{F}_q) = n = hr$, r is the largest prime divisor of n, $\gcd(r, q) = 1$
- $E[r]$ is the set of r-torsion points in $E(\bar{\mathbb{F}}_q)$
- Weil pairing $e_r : E[r] \times E[r] \rightarrow \mu_r$
  - e_r is bilinear, non-degenerate
  - $\mu_r \subseteq \mathbb{F}_{q^k}$ where $k \in \mathbb{Z}$ and $q^k \equiv 1 \pmod r$
  - The least positive such k is called the *embedding degree* of E

Pairings in Cryptography

- Applications
  - Identity Based Encryption, one-round three-party key agreement, short signature schemes
  - Other pairing functions: Tate, Ate, Eta
- We want (q, r, k) such that
  - E is constructible
  - e_r is efficiently computable
  - ECDLP in $E(\mathbb{F}_q)$ and DLP in $\mathbb{F}_{q^k}$ are equivalently-infeasible
  - e.g. For 80-bit security $q \approx 2^{170}, k = 6, \#E(\mathbb{F}_q) = r$

Prime-order Elliptic Curves with $k = 3, 4, 6$

- Let $\#E(\mathbb{F}_q) = n$ be prime and E have embedding degree $k = 3, 4, 6$
- Miyaji, Nakabayashi and Takano (2001) characterize such curves
- Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with trace $t = q + 1 - n$. Then
  1. $k = 3 \Leftrightarrow q = 12\ell^2 - 1$ and $t = -1 \pm 6\ell$ for some $\ell \in \mathbb{Z}$.
  2. $k = 4 \Leftrightarrow q = \ell^2 + \ell + 1$ and $t = -\ell, \ell + 1$ for some $\ell \in \mathbb{Z}$.
  3. $k = 6 \Leftrightarrow q = 4\ell^2 + 1$ and $t = 1 \pm 2\ell$ for some $\ell \in \mathbb{Z}$.
- Such curves are referred to as *MNT curves*

Outline

1 Introduction
- Pairings and embedding degree
- MNT curves: $k = 3, 4, 6$

2 Constructing MNT Curves
- CM method
- Frequency of MNT curves

3 Our Contributions
- Relation between the MNT curves with $k = 4$ and $k = 6$
- A deep analysis of MNT equations
- A lower bound on MNT curves with bounded discriminant

4 Conclusion

CM Method

- $k = 6 \Leftrightarrow q(\ell) = 4\ell^2 + 1$ and $t(\ell) = 1 \pm 2\ell$ for some $\ell \in \mathbb{Z}$.
- Find ℓ: $q(\ell)$ is a prime power, $n(\ell) = q(\ell) + 1 - t(\ell)$ is prime
- Use Complex Multiplication (CM) method to construct E over $\mathbb{F}_q$
  - *CM equation*: $4q - t^2 = DY^2$, $Y \in \mathbb{Z}$, $D > 0$ is square-free
    - D is called the *discriminant* of E.
  - Find a root, j_E, of the Hilbert class polynomial $H_D(x)$ over $\mathbb{F}_q$
  - Construct $E/\mathbb{F}_q$ with $j-invariant = j_E$

CM method and MNT curves ($k = 6$)

- CM method is practical if $D < 10^{10}$
- We should first fix D and find ℓ because otherwise $D \approx q$
  - CM equation is equivalent to the Pell (or MNT) equation

$$X^2 - 3DY^2 = -8 \text{ where } X = 6\ell - 1 \text{ or } X = 6\ell + 1$$

  - Fix D and solve for (X, Y) in the above equation
  - Set $q(\ell), t(\ell)$ and construct E

Solutions to Pell Equations

- $X^2 - DY^2 = m$: $m \in \mathbb{Z}$, $D \in \mathbb{N}$, D not a perfect square
- $x, y, u, v \in \mathbb{Z}$: $x^2 - Dy^2 = m, u^2 - Dv^2 = 1, \gcd(x, y) = 1$
- *Primitive solutions* to $X^2 - DY^2 = m$ in the class of $x + y\sqrt{D}$:

$$\pm(x + y\sqrt{D})(u + v\sqrt{D})^j, \; j \in \mathbb{Z}$$

Scarcity of MNT Curves

- MNT curves are constructible through the solutions of

$$X^2 - 3DY^2 = -8 \text{ where } X = 6\ell - 1 \text{ or } X = 6\ell + 1$$

- $q(\ell)$ and $n(\ell)$ must satisfy primality conditions
- The size of the solutions (X, Y) grow exponentially
- MNT curves are very rare!
  - Let $E(z) := \#\{E \text{ upto isogeny with } k = 6 \text{ and } D \leq z\}$
  - Luca-Shparlinski (2006) upper bound:

$$E(z) \ll z/(\log z)^2$$

Outline

MNT Curves with $k = 4$ and $k = 6$

- $E_4/\mathbb{F}_q, k = 4 \Leftrightarrow q = \ell^2 + l + 1$ and $t = -\ell, \ell + 1$
- $E_6/\mathbb{F}_q, k = 6 \Leftrightarrow q = 4\ell^2 + 1$ and $t = 1 \pm 2\ell$

$$\begin{array}{lcl} k = 6 & & k = 4 \\ E_6/\mathbb{F}_q & \Leftrightarrow & E_4/\mathbb{F}_n \\ \#E_6(\mathbb{F}_q) = n & & \#E_4(\mathbb{F}_n) = q \end{array}$$

Proof Sketch:
$$q = 4\ell^2 + 1,\ t = 1 - 2\ell$$
$$\text{Set } q' = n,\ n' = q,\ t' = q' + 1 - n'$$
$$q' = (2\ell)^2 + 2\ell + 1 = n,\ t' = 2\ell + 1$$

MNT Equation and the Curve Parameters ($k = 6$)

- $X^2 - 3DY^2 = -8$ has either zero or two solution classes: S_1, S_2
- $D \equiv 3 \pmod 8$
- -2 is a square modulo $3D$
- MNT curve parameters must come from S_1 and S_2: $\mathcal{E}_1, \mathcal{E}_2$
- $\mathcal{E}_1 = \mathcal{E}_2$

A Lower Bound on $E(z)$

Consider $X^2 - 3DY^2 = -8$ with $Y = 1$ and let

$$\begin{aligned} \mathcal{F}(z) &= \{D : D \in [1, z] \text{ is odd and squarefree, } 3D - 8 \text{ perfect square}\} \\ F(z) &= \#\mathcal{F}(z) \end{aligned}$$

If $x_D^2 = 3D - 8$ then we can show that $x_D = 6\ell_D \pm 1$

MNT theorem implies when $x_D = 6\ell_D + 1$ that

$$q_D = 4\ell_D^2 + 1, \; n_D = 4\ell_D^2 + 2\ell_D + 1$$

So, $D \leq z \Rightarrow q_D \leq z/2, \; n_D \leq 3z/4$

$$E(z) \geq F(z) \frac{1}{(\log z)^2} \geq ??$$

A Lower Bound on $E(z)$ cont'd

We write $3D - 8 = (6\ell \pm 1)^2$. Then we can show that

$$\begin{array}{l} D \text{ is odd and squarefree} \\ 3D-8 \text{ is a perfect square} \end{array} \Leftrightarrow D = 12\ell^2 \pm 4\ell + 3 \text{ is squarefree}$$

Let $f_+(\ell) = 12\ell^2 + 4\ell + 3$, $\mathcal{F}_+(z) = \{D \in [5, z] : \; D = f_+(\ell) \text{ is squarefree}\}$

Fact: (G. Ricci, 1933) $\#\{\ell : 0 < \ell \leq L \text{ and } f_+(\ell) \text{ is square free}\} \approx c_{f_+} L$ where

$$\begin{aligned} c_{f_+} &= \prod_{p \text{ prime}} (1 - w_{f_+}(p)/p^2) \\ w_{f_+}(p) &= \#\{a \in [1, p^2] : \; f_+(a) \equiv 0 \pmod{p^2}\} \end{aligned}$$

A Lower Bound on $E(z)$ cont'd

In our case,

$$F_+(z) \;=\; \#\mathcal{F}_+(z) \;\approx\; c_{f_+} L_+$$
$$D \in [5, z] \;\Leftrightarrow\; L_+ \approx \sqrt{z/12}$$

$w_{f_+}(3) = 1$ and $w_{f_+}(p) = 0, 2$

$$w_{f_+}(p) = 2 \;\Leftrightarrow\; \left(\frac{-2}{p}\right) = 1 \;\Leftrightarrow\; p \equiv 1, 3 \pmod 8$$

A Lower Bound on $E(z)$ cont'd

Hence,

$$c_{f_+} = c_{f_-} = \prod_{p \text{ prime}} (1 - w_{f_+}(p)/p^2)$$
$$= \frac{8}{9} \cdot \prod_{p \equiv 1,3 \pmod 8} (1 - 2/p^2),$$

$$F(z) = F_+(z) + F_-(z)$$
$$> (c_{f_+}(z) + c_{f_-}(z) - 2\epsilon)\sqrt{z/12}$$
$$> 0.857\sqrt{z/3}$$

and

$$E(z) \geq F(z)\frac{1}{(\log z)^2} \geq 0.49\frac{\sqrt{z}}{(\log z)^2}$$

Experimental Results on $E(z)$

Let $E_B(z) = \#$ MNT curves $E/\mathbb{F}_q : k = 6, \; q < 2^B, \; D \leq z$

	$R(B,z) = E_B(z)/(0.49\frac{\sqrt{z}}{(\log z)^2})$, where $z = 2^i$.					
i	$B = 100$	$B = 160$	$B = 300$	$B = 500$	$B = 700$	$B = 1000$
13	25.63	27.46	27.46	27.46	27.46	27.46
14	27.02	30.02	30.02	30.02	30.02	30.02
15	26.81	30.46	30.46	30.46	30.46	30.46
16	26.47	29.41	29.41	29.41	29.41	29.41
17	26.61	29.74	29.74	29.74	29.74	29.74
18	25.43	27.92	27.92	27.92	27.92	27.92
19	25.42	27.86	28.35	28.35	28.35	28.35
20	24.51	26.81	27.19	27.19	27.57	27.57
21	23.58	25.67	26.87	27.47	28.06	28.06
22	26.64	28.73	29.66	30.12	30.81	30.81
23	27.40	29.72	30.62	30.98	32.05	32.41
24	28.54	30.88	32.12	32.67	33.64	34.05
25	29.30	31.52	32.79	33.32	34.17	34.48

Outline

1. Introduction
   - Pairings and embedding degree
   - MNT curves: $k = 3, 4, 6$
2. Constructing MNT Curves
   - CM method
   - Frequency of MNT curves
3. Our Contributions
   - Relation between the MNT curves with $k = 4$ and $k = 6$
   - A deep analysis of MNT equations
   - A lower bound on MNT curves with bounded discriminant
4. Conclusion

Concluding Remarks

- A detailed analysis of MNT equations
  - $1-1$ correspondence between MNT curves with $k=4$ and $k=6$
  - More efficient and explicit algorithms for MNT curve parameters
- A lower bound for the number of MNT curves
  - The lower bound can be improved
    $X^2 - 3DY^2 = -8$ with $Y = 3, 9$ gives an improvement by a factor $(1 + 1/3 + 1/9)$
- Q. # MNT curves $E/\mathbb{F}_q$ with $D \leq z$ and $L < q < U$?

THANKS!