Pairing-Friendly Fields

Koblitz & Menezes – A field is defined as pairing-friendly with repect to a cryptographic pairing of embedding degree k>2, if p=1 mod 12. Let F_{p^k} be a pairing-friendly field, and let Є be an element in F_p that is neither a square nor a cube. Then the polynomial X^k - Є is irreducible. Nice binomial irreducible! Easy to build a tower of extensions. Nice for automatic generation of finite field code!

Pairing friendly fields

Therefore to be a pairing-friendly field then p=1 mod 3 and p=1 mod 4 (a little restrictive!)

Consider now a pairing-friendly elliptic curve which supports "efficient arithmetic". Then for the Tate pairing e(P,Q) if 6|k, and the CM discriminant is D=3, then Q can be a point on the sextic twist $E(F_{p^{k/6}})$. If 4|k and D=4, then Q can be a point on the quartic twist $E(F_{p^{k/4}})$.

Pairing friendly fields

Main result (indeed only result!)

For pairing friendly fields as applied to pairing-friendly curves with efficient arithmetic, then automatically p=1 mod 3 or p=1 mod 4. So we are already half-way towards being able to use a pairing-friendly field.

Pairing-friendly Fields

In the case $D=3$ the elliptic curve is of the form $y^2=x^3+B$. Therefore $p=1 \bmod 3$, as otherwise the elliptic curve is supersingular with embedding degree 2.

In the case $D=4$ the elliptic curve is of the form $y^2=x^3+Ax$. Therefore $p=1 \bmod 4$, as otherwise the elliptic curve is supersingular with embedding degree 2.