Finding ECM-friendly curves - A Galois approach

Sudarshan Shinde

The elliptic curve method (ECM) is a factorization algorithm widely used in cryptography. It was proposed in 1985 by Lenstra and improved a couple of months later by Montgomery using well-chosen curves. In order to compare different families of curves, he associated to each elliptic curve E and prime l, the mean valuation of l in the cardinality of E modulo random primes. More precisely, we set $\overline{v_l} = \mathbb{E}(v_l(\#(E(\mathbb{F}_p))))$ where the expectation is with respect to random primes p.

Montgomery increased $\overline{v_l}$ by forcing curves to have l-torsion points over $\mathbb{Q}$. Brier and Clavier further increased $\overline{v_2}$ by imposing torsion points over $\mathbb{Q}(i)$. In 2012, Barbulescu et al (cf [1]) produced families of elliptic curves with better mean valuation without adding any torsion points on $\mathbb{Q}(i)$. Moreover, they showed that it is impossible to change $\overline{v_l}$ without changing the degree of the l-torsion field, which has a generic value (cf [2]) in the sense in which the Galois group of an irreducible polynomial of degree n is generically $\mathcal{S}_n$.

In this talk we search families of elliptic curves with a larger valuation for $l = 2$ and $l = 3$ which boils down to searching families with non-generic Galois groups. Initially, we considered the method of Lagrange resolvant but this is not feasible for our polynomials of interest : the degree of division polynomials is quadratic in l.

We then present two algorithms which produce a system of polynomial equations characterising every subfamily of elliptic curves having non-generic $\overline{v_3}$ and every subfamily of Montgomery curves having non-generic $\overline{v_2}$.

Références

[1] Razvan Barbulescu, Joppe Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter Montgomery. Finding ecm-friendly curves through a study of galois properties. *The Open Book Series*, 1(1) :63–86, 2013.

[2] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4) :259–331, 1971.