ELLIPTIC CURVE PRIMALITY PROVING (ECPP)

JAAP TOP

Proving primality of a large number n which is expected to be prime, can be done using elliptic curves. This started with an idea of Shafi Goldwasser and Joe Kilian (1986). In the same year it was turned into a practical algorithm by A.O.L. (Oliver) Atkin. The algorithm was improved by several people, in particular by François Morain (1993), who jointly with Atkin turned it into an algorithm called ECPP (Elliptic Curve Primality Proving). An implementation of it called PRIMO can be downloaded from

`http://www.ellipsa.net/public/primo/index.html`

With PRIMO you can test/prove primality of numbers below 2^{10000}.

Many ideas in the Goldwasser-Kilian-Atkin-Morain algorithm are beyond the scope of this class. For instance, we will not discuss how given n, a useful cubic curve is found by the algorithm, to prove that n is prime. However, the basic strategy of the algorithm we can explain.

For this, we will assume n is a given odd integer which we expect to be a prime number. We want to work with curves given by an equation $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}/n\mathbb{Z}$. However, we do not know (yet) whether n is prime, so whether $\mathbb{Z}/n\mathbb{Z}$ is a field. So we have to extend the theory of elliptic curves a bit, to make it work over a ring such as $\mathbb{Z}/n\mathbb{Z}$. Define

$$\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$$

as the set of classes $(x : y : z)$ such that the ideal (x, y, z) is the full ring $\mathbb{Z}/n\mathbb{Z}$. Equality $(x : y : z) = (x' : y' : z')$ means, that a unit $u \in (\mathbb{Z}/n\mathbb{Z})^*$ exists such that $x = ux', y = uy'$ and $z = uz'$.

If $a, b, c \in \mathbb{Z}/n\mathbb{Z}$ are such that the discriminant D of x^3+ax^2+bx+c is a unit in $\mathbb{Z}/n\mathbb{Z}$, then we define

$$C(\mathbb{Z}/n\mathbb{Z}) := \left\{(x : y : z) \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) \mid y^2z = x^3 + ax^2z + bxz^2 + cz^3\right\}.$$

On $C(\mathbb{Z}/n\mathbb{Z})$ we define a group structure in the usual way with $O = (0 : 1 : 0)$ as the zero element for the group. Note that $(\mathbb{Z}/n\mathbb{Z})$ can contain points $\neq O$ with $z = 0$: for instance, if $n = m^2$ is a square, then $(m : 1 : 0)$ is such a point. For every prime number $p|n$ we have the reduction modulo p homomorphism

$$C(\mathbb{Z}/n\mathbb{Z}) \longrightarrow C(\mathbb{F}_p).$$

The algorithm is based on the following fact.

THEOREM. *Suppose m is an integer, and $q \geq (\sqrt[4]{n}+1)^2$ is a divisor of m.*

If $P \in C(\mathbb{Z}/n\mathbb{Z})$ satisfies

- $m \cdot P = O$;
- $\frac{m}{q} \cdot P = (x : y : z)$ *with* $z \in (\mathbb{Z}/n\mathbb{Z})^*$,

then

$$q \text{ is prime} \Rightarrow n \text{ is prime.}$$

To prove this, suppose $p|n$ is prime. Reduction modulo p then sends $\frac{m}{q} \cdot P$ to a point $Q \in C(\mathbb{F}_p)$, and we know $Q \neq O$ but $q \cdot Q = O$. this means that $Q \in C(\mathbb{F}_p)$ has order q, hence

$$(\sqrt[4]{n}+1)^2 \leq q \leq \#C(\mathbb{F}_p) < (\sqrt{p}+1)^2.$$

This implies $\sqrt{n} < p$. Now this inequality is true for every prime divisor p of n, and hence $n = p$ is prime. □

If we inspect the proof given here, we note that q is the order of an element in the image of the reduction map. This implies that q also divides $\#C(\mathbb{Z}/n\mathbb{Z})$. So to use the theorem for proving that n is prime, we need a curve C such that $\#C(\mathbb{Z}/n\mathbb{Z})$ is divisible by a rather large prime number q (roughly, somewhat larger than $\sqrt{n}$). And this q should be (much) smaller than n, since otherwise showing that q is prime may be as difficult as showing that n is prime. In practice, one usually looks for curves C with $\#C(\mathbb{Z}/n\mathbb{Z}) = 2q$. This implies, assuming that indeed n is prime, that $q < (\sqrt{n}+1)^2/2$, and this is (for $n \geq 6$) indeed smaller than n.

The resulting algorithm looks as follows.

(1) Select a curve C as above, with an integer m such that:
   - if indeed n is prime, then $m = \#C(\mathbb{Z}/n\mathbb{Z})$;
   - m has a proper divisor $q \geq (\sqrt[4]{n}+1)^2$ which is probably prime.

(2) Now pick a point $P \in C(\mathbb{Z}/n\mathbb{Z})$ until $\frac{m}{q} \cdot P$ has z-coordinate in $(\mathbb{Z}/n\mathbb{Z})^*$.
   Check that indeed $q \cdot \frac{m}{q} \cdot P = O$.

(3) Prove recursively that q is prime.