11/12/04

Algorithm: Pollard's
Group $\mathbb{Z}_p^*$
Fact about group, $a \in \mathbb{Z}_p^*$ has order b
then $p \mid a^b - 1$.

How it works: we choose a, k product of small primes.
and we find $\gcd(a^k - 1, n)$.

<u>Lenstra's algorithm</u>

$C(\mathbb{F}_p)$. $P \in C(\mathbb{Q})$ P has infinite order

$kP = \left(\frac{m_k}{d_k^2}, \frac{n_k}{d_k^3}\right)$.

What happens when $\overline{P} \in C(\mathbb{F}_p)$ is of order b?

$$\begin{array}{lcl} P \in C(\mathbb{Q}). & & P, 2P, 3P, \ldots bP. \\ V_p \downarrow & & \downarrow \quad \downarrow \quad \downarrow \\ \overline{P} \in C(\mathbb{F}_p) & & \overline{P}, 2\overline{P}, 3\overline{P} \ldots b\overline{P} = O \end{array}$$

$$bP = \left(\frac{m_b}{d_b^2}, \frac{n_b}{d_b^3}\right)$$

$\Rightarrow p \mid d_b$.

So $\overline{P}$ ~~has~~ $\in C(\mathbb{F}_p)$ has order b $\Leftrightarrow$ $p \mid d_b$.

Given n

Step 1: We will choose an curve C and point $P \in C(\mathbb{Q})$.
Pick $k = \mathrm{LCM}[1, \ldots, K]$

Step 2. We will compute $kP = \left(\frac{m_k}{d_k^2}, \frac{n_k}{d_k^3}\right)$.

Step 3. We find $\gcd(d_k, n)$.

Step 1 - ① Check $\gcd(n, 6) \neq 1$

② Choose $P = (x_1, y_1)$, Choose b

$C: \; y^2 = x^3 + bx + c$ s.t. $P \in C$.

③ Check $\gcd(27c^3 + 4b^2, n) = 1$.

④ $k = \mathrm{LCM}(1, ---, K)$.

Step 2 - $k = \sum_n a_n 2^n \quad a_n \in \{0, 1\}$

Compute $P, 2P, 4P, 8P, ---$ (doubling formula.

How do we add points?

$P = (x_1, y_1)$

$$x(2P) = \frac{(x_1^2 - b)^2 - 8cx_1}{4y_1^2} \mod n.$$

inverse $4y_1^2 \pmod n$

$\gcd(4y_1^2, n) = a_1 4y_1^2 + a_2 n$.

$\gcd = 1 \Rightarrow a_1$ inverse $4y_1^2 \bmod n$

$x(2p) = a_1 \cdot ((x_1^2 - b)^2 - 4cx) \mod n$

if not $\gcd(4y_1^2, n) \mid n$.

Example

$n = 35$

$P = (2,6) \in C: \; y^2 = x^3 + 14x.$

$k = LCM(1,2,3,4) = 12.$

$12 = 8 + 4.$

need $2P, 4P, 8P \pmod{n}$.

$P = (2,6)$

$$x(2P) = \frac{(2^2 - 14)^2}{4 \cdot 6^2} = \frac{100}{4 \cdot 36} \pmod{35}$$

$$\equiv \frac{100}{4} = 25 \mod (35).$$

$$x(4P) = \frac{(25^2 - 14)^2}{4(25^3 + 14 \cdot 25)}$$

$\gcd(4 \cdot 25^3 + 14 \cdot 25, 35)$

$= 5$

so we find factor of n.

$35 = 5 \cdot 7.$