Choosing $E$ and $P$

**Method 1:** Random selection ($F = \mathbb{F}_q$ fixed).

1) Choose $x, y, a \in \mathbb{F}_q$ at random, and put $b = y^2 - (x^3 + ax)$.
2) Check that $4a^3 + 27b^2 \neq 0$. If true, then $E = E_{a,b}$ is an elliptic curve over $F$ and $P = (x, y) \in E(F)$. If not, then go back to step 1.

**Problem:** Is $(E, P)$ cryptographically good? For this, need: ord$(P)$ has a large prime divisor. This can be checked in polynomial time provided that we have solved:

**Subproblem:** Determine $|E(F)|$. (Use Schoof/Elkies/Atkin.)

**Method 2:** Choose $P \in E(\mathbb{Q})$ and reduce mod $p$.

1) Use random selection method (with $x, y, a \in \mathbb{Z}$) to find $E/\mathbb{Q}$ and $P \in E(\mathbb{Q})$. (Thus, $E : y^2 = f(x)$, $f(x) \in \mathbb{Z}[x]$).
2) Use the Nagell/Lutz criterion (or Mazur’s Theorem) to check that ord$(P) = \infty$. If false, go back to step 1.
3) Choose a large prime $p \nmid \Delta_E$ and consider $\overline{E} = E \pmod{p}$. (Thus, $\overline{E}/\mathbb{F}_p : y^2 \equiv f(x) \pmod{p}$.) Put $\overline{P} := (x, y) \pmod{p}$. Then $\overline{P} \in \overline{E}(\mathbb{F}_p)$.
4) If $(\overline{E}, \overline{P})$ is not cryptographically safe, choose a new prime $p$ and repeat step 3.

**Remarks:**
1) The check of step 4 leads to similar problems as in Method 1. However, for certain elliptic curves $E/\mathbb{Q}$ (the CM-curves) there exists a formula for $|\overline{E}(\mathbb{F}_p)|$ in terms of $p$.
2) It is conjectured (and proven under (GRH)) that there exist infinitely many primes $p$ such that $\overline{P}$ is a generator of $\overline{E}(\mathbb{F}_p)$. (Analogue of Artin’s Conjecture.)
Method 3: Koblitz curves.

1) Let $p$ be a small prime and choose $E/\mathbb{F}_p$. Compute $N = |E(\mathbb{F}_p)|$ by the naive method.

2) Take $r$ such that $q = p^r$ is large enough. Then we can compute $|E(\mathbb{F}_q)|$ by the Artin/Schmidt/Hasse formula:

\begin{equation}
|E(\mathbb{F}_q)| = |\alpha^r - 1|^2,
\end{equation}

where $1/\alpha$ is a root of $pT^2 - aT + 1$, and $a = p + 1 - N$. Alternately, we could use the following second order recursion formula for $a_n := a_{E/\mathbb{F}_{p^n}} = 1 + p^n - |E(\mathbb{F}_{p^n})|$:

\begin{equation}
a_{n+2} = aa_{n+1} - qa_n, \quad \text{with } a_0 = 2, \ a_1 = a.
\end{equation}

Remark: The formula (1) uses Hasse’s result that

\[ pT^2 - aT + 1 = (\alpha T - 1)(\alpha T - 1). \]

(Recall that this implies the Hasse bound: $|a| \leq 2\sqrt{p}$.)

Difficulties: 1) It is not so easy to find a suitable point $P \in E(\mathbb{F}_q)$. (Use Koblitz’s idea of message embedding.)

2) The Weil descent attack (due to Frey (∼2000)) forces us to chose $r$ carefully ($r$ prime is best).