The Goldwasser/Kilian Elliptic Curve Primality Test

**Given:** A positive integer \( n \) (known to be “probably prime”).

**Aim:** Prove that \( n \) is prime, or else find a proper factor \( d|n \).

**Idea:** Analogue of Pocklington’s Primality Test.

**Procedure:**

**Step 1:** Select random integers \( a, x_0, y_0 \) (mod \( n \)) and put
\[
E : y^2 = x^3 + ax + b, \quad P = (x_0, y_0) \text{ with } b = y_0^2 - (x_0^3 + ax_0).
\]

**Step 2:** Check that \( g:=\gcd(\Delta_E, n) = 1 \), where \( \Delta_E = 4a^3 + 27b^2 \):
- If \( g = 1 \), then go to the next step.
- If \( g = n \), then repeat step 1 with new values.
- If \( g \neq 1, n \), then done: we’ve found a proper factor!

**Step 3:** Pretend that \( n \) is prime and use the Schoof Algorithm to compute \( m = \#E(\mathbb{F}_n) \).

**Note:** If Schoof’s algorithm breaks down, then we can easily find a factor of \( n \); then done.

**Step 4:** If we cannot write \( m = kq \), where \( k \geq 2 \) is small and \( q \) is “probably prime” (by a suitable primality test), then start over with step 1.

**Step 5:** Thus \( m = kq \) with \( k \) small and \( q \) (probably) prime, \( q > (n^{1/4} + 1) \). Compute \( mP \) and \( kP \).
- If \( mP \neq \mathcal{O}(= P_\infty) \), then \( n \) is composite (by Lagrange).
- If \( kP = \mathcal{O} \), then start over with step 1.
Step 6: Thus $m = kq$, $mP = \emptyset$ and $kP \neq \mathcal{P}$. By the Proposition, we can conclude that $n$ is prime provided we know that $q$ is prime.

For this: restart the algorithm for $q = q_1$ in place of $n$. We then get a new $m = k_2q_2$, where $k_2$ is small and $q_2$ is probably prime. Restart with $q_2$, etc.

Note that since $q_{i+1} \leq \frac{q_i - 1}{2}$, we have at most $t = \log_2 n$ such (probable) primes $q_1 = q, \ldots, q_t$ to consider, and that if any $q_i$ is proven to be prime, then the Proposition guarantees that $q_{i-1}, \ldots, q_1 = q$ and hence also $n$ are all prime.