**Lenstra’s Factorization Method**

**Given:** A positive integer $n$ (known to be composite).

**Find:** A proper factor $d|n$, $1 < d < n$.

**Idea:** Use Pollard’s $p−1$ method, but replace $\mathbb{F}_p^\times$ by $E(\mathbb{F}_p)$ for a suitable elliptic curve $E/\mathbb{Q}$.

More precisely: given $P \in E(\mathbb{Q})$, compute $kP$ in $E(\mathbb{Q})$. If there is a $j$ with $1 \leq j \leq k$ such that the denominator of $jP$ is not prime to $n$, then we get a factor.

**Step 0:** Check that $(n, 6) = 1$ and that $n \neq m^r$, for any $r \geq 2$. Choose parameters $B, C$ and put

$$k = \prod_{q \leq B} q^{\alpha_q} \quad \text{where } \alpha_q = \left[ \frac{\log C}{\log q} \right], \text{ q prime}$$

**Step 1:** Choose random integers $a, x_0, y_0$ in $[0, n − 1]$ 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:** Compute $kP(\text{mod } n)$ (see details below):

- If this can be done successfully, go back to step 1.
- Otherwise, we get a proper factor: done!
**Step 3 (details):** Compute \( k_j P \pmod{n} \), for a suitable sequence \( k_1, \ldots, k_r = k \). (See Methods 1 and 2 below.) Write

\[
P_j = k_j P = \left( \frac{x_j}{z_j}, \frac{y_j}{z_j} \right) \quad \text{in} \quad E(\mathbb{Q}),
\]

where \( \gcd(x_j, y_j, z_j) = 1 \). If

\[
d_j := \gcd(z_j, n) = 1,
\]

then there exist \( x_j \equiv \frac{x_j}{z_j} \pmod{n} \) and \( y_j \equiv \frac{y_j}{z_j} \pmod{n} \), and so

\[
\overline{P}_j = (\overline{x}_j, \overline{y}_j) \equiv k_j P \pmod{n}
\]

can be computed directly from \( \overline{P}_{j-1} \). Otherwise:
- either \( d_j = n \): then go back to step 1;
- or \( d_j \neq 1, n \): then we have a proper divisor: done!

**Method 1 (for choosing the \( k_j \)'s):** Binary power method (cf. Silverman/Tate): Write

\[
k = 2^r + 2^{r-1}c_1 + \ldots + 2c_{r-1} + c_r, \quad \text{with} \quad c_i \in 0, 1
\]

and put \( k_0 = 1, \; k_j = 2k_{j-1} + c_j \).

**Method 2:** Use the factorization of \( k \) (cf. Koblitz):

Let \( q_1 = 2, q_2 = 3, \ldots, q_r \) denote the primes \( \leq B \) and put \( k_0 = 1 \) and

\[
k_{j+1} = q_i k_j \quad \text{for} \quad A_{i-1} \leq j < A_i, \; 1 \leq i \leq r,
\]

where \( A_0 = 1, \; A_i = \alpha_{q_1} \cdots \alpha_{q_i} \). Thus we get the sequence:

\[
1, 2, 2^2, \ldots, 2^{\alpha_2}, 3(2^{\alpha_2}), 3^2(2^{\alpha_2}) \ldots, 3^{\alpha_3}2^{\alpha_2}, \ldots, k.
\]