Pollards Faktorisierungsalgorithmus

1. Wähle eine Zahl k, welche das Produkt kleiner Primzahlen mit kleinen Potenzen ist, z.B. $k = \text{kgV}(1, ..., K)$ mit $K \in \mathbb{N}$.
2. Wähle ein $a \in \mathbb{N}$ mit $1 < a < n$.
3. Bestimme $\text{ggT}(a, n)$.

   Wenn $\text{ggT}(a, n) \notin \{1, n\}$ gilt, erhalten wir einen nicht-trivialen Teiler von n.
4. Berechne $D = \text{ggT}(a^k - 1, n)$.

   Gilt $D = 1$, so wähle im Schritt 1 ein größeres k.

   Wenn $D = n$ gilt, so wähle im Schritt 2 eine anderes a.

   Im Fall $1 < D < n$ ist D ein nicht-trivialer Teiler von n.

Faktorisierungsalgorithmus für Elliptische Kurven

1. Überprüfe, ob $\text{ggT}(n, 6) = 1$ und $\forall m, r \in \mathbb{N}, r \geq 2 : n \neq m^r$ gilt.
2. Wähle zufällige Zahlen $b, x_1, x_2 \in \mathbb{N}$ mit $1 < b, x_1, x_2 < n$.
3. Berechne $c = y_1^3 - x_1^3 - bx_1 \mod c$. Dann verwende E als die durch $y^2 = x^3 + bx + c$ definierte Elliptische Kurve und setze $P = (x_1, y_1) \in E$.
4. Überprüfe, ob $\text{ggT}(4b^3 + 27c^2, n) = 1$ gilt.

   Wenn $\text{ggT}(4b^3 + 27c^2, n) = n$ gilt, dann weiter bei Schritt 2 mit einem neuen b.
5. Wähle $k \in \mathbb{N}$ als Produkt von kleinen Primzahlen mit kleinen Potenzen, zum Beispiel $k = \text{kgV}(1, ..., K)$.
6. Berechne $kP = \left(\frac{a_k}{d_k^2}, \frac{b_k}{d_k^3}\right)$. Hierfür muss $\text{ggT}(d_k, n) = 1$ gelten, damit das Inverse von d_k bestimmt werden kann. Wenn $\text{ggT}(d_k, n) = n$ gilt, so gehe zurück zu Schritt 5 und wähle ein kleineres k.