Lenstra's Factorization Algorithm

W. Maleszewski
Lomza State University of Applied Sciences

17 September 2017

Introduction

This poster describes Lenstras Elliptic Curve Algorithm for factoring large numbers. The authors starts from the definition of elliptic curves over fields of characteristic different than 2 or 3. Then he introduces a construction of the abelian group over the K-rational points of an elliptic curve. Next he reminds Pollards p 1 algorithm and introduces Lenstra's Algorithm. This poster discusses how Lenstras improves upon Pollard and it gives a brief note on application.

Background

The name of elliptic curves is connected with the problem of determining the arc length of an ellipse using the so-called elliptic integral of the second kind. They cannot be expressed using elementary functions. Functions inverse to elliptic integrals are called *elliptic functions*

Example

One of the elliptic integrals is the function:

$$u = \int_y^\infty \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}}$$

The function inverse is the Weierstrass elliptical function $y = \wp(u)$, which satisfies the dependence:

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3.$$

The elliptic function satisfies the equation of a curve. As a result, this curve is called an elliptic curve *elliptic curve.*

Definitions

Let us call the elliptic curve in $\mathbb{R}^2$ as a set of solutions of the Weierstrass equation:

$$y^2 = x^3 + ax + b$$

together with a point at infinity O where the constants a,b meet the additional condition: $4a^3 + 27b^2 \neq 0$. We mark the set of solutions as $E(\mathbb{R})$. Thus, the elliptic curve is a set of:

$$E(\mathbb{R}) = \left\{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\right\} \cup \{O\}.$$

The condition

$$\Delta_E \neq 0$$

where $\Delta_E = -16 \cdot (4a^3 + 27b^2)$ means that the polynomial $x^3 + ax + b$ does not have multiple roots.

The algorithm of adding points on the elliptic curve

Let $E(\mathbb{R})$ be an elliptic curve, and $M_1, M_2 \in E(\mathbb{R})$, where

$$M_1 = (x_1, y_1),$$
$$M_2 = (x_2, y_2),$$

and $\mathcal{O}$ is "a point at infinity" [1], then:

- $\forall_{i,j\in\{1,2\}}(M_i \in \mathcal{O} \Rightarrow M_i + M_j = M_j)$
- $\forall_{i,j\in\{1,2\}}(M_i \notin \mathcal{O} \wedge M_j \notin \mathcal{O} \wedge x_i \neq x_j \Rightarrow M_i + M_j = (x_3, y_3))$, where:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = -y_1 + \lambda(x_1 - x_3) \end{cases}$$

and

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

- $\forall_{i,j\in\{1,2\}}(M_i \notin \mathcal{O} \wedge x_i = x_j \wedge y_i = -y_j \Rightarrow M_i + M_j = \mathcal{O})$
- $\forall_{i,j\in\{1,2\}}(M_i \notin \mathcal{O} \wedge M_i = M_j \Rightarrow M_i + M_j = (x_3, y_3))$, where:

$$\begin{cases} x_3 = \rho^2 - 2x_1 \\ y_3 = -y_1 + \rho \cdot (x_1 - x_3) \end{cases}$$

and

$$\rho = \frac{3x_1^2 + a}{2y_1}.$$

Theorem 1

$(E, +)$ is an abelian group with neutral element $\mathcal{O}$.

Elliptic Curve Groups

Let K be a field over which the curve is defined and denoted by E. Then the K-rational points of E are the points on E whose coordinates all lay in K, including the point at infinity. It forms a group too, because properties of polynomial equations show that if P is in $E(K)$, then P is also in $E(K)$, and if two of P, Q, and R are in $E(K)$, then so is the third. Additionally, if K is a subfield of L, then $E(K)$ is a subgroup of $E(L)$.

Trial Division

The simplest method of finding the prime factors of a given integer n is the well known Trial Division. We check for every prime p between 2 and $\sqrt{n}$ whether p divides n. This is fairly efficient if $n < 10^{20}$ but for larger n we need a more sophisticated approach.

Pollard's $p-1$ algorithm

Theorem 2 (Fermat)

If p is a prime and a is any number not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

If the assumptions of the theorem are true, then every multiple of k of $p-1$ has the property

$$a^k \equiv 1 \pmod{p}$$

$$p | a^k - 1$$

We are looking for a prime divisor p of the number n, it is also a divisor of n and $a^k - 1$, where k is a multiple a numbers $p-1$.
If we choose k such that the number $a^k - 1$ is divisible by n, ie

$$\gcd(a^L - 1; n) = n$$

we do not get new information. If we find k such number $a^k - 1$ is not divisible by n, that is

$$\gcd(a^L - 1; n) = p$$

then the calculation of $a^k - 1$ and $\gcd(a^L - 1; n)$ will lead to finding the divisor of n. [3, 5]

Algorithm

1. Choose a random integer such as $1 < a < n$.
2. If $\gcd(a; n) > 1$, then this gcd is a prime factor of n, so we are done.
3. For each $r = 2, 3, \ldots,$ compute $d = \gcd(a^{r!} - 1; n)$.
   a) If $d = n$, go back to step 1 and pick an integer a we haven't tried yet.
   b) If $d \neq n$ but $d > 1$, then d is a prime factor of n, so we are done.
   c) If $d = 1$, increment r and repeat this loop.

Example

Let $n = 10001$. Let's start with $a = 2$. Then clearly $\gcd(2; 10001) = 1$, so we proceed into the loop. We first compute $a^{2!} = 2^2 = 4$. Then

$$\gcd(a^{2!} - 1, n) = \gcd(3, 10001) = 1$$

so we continue. Now $a^{3!} = (a^{2!})^3 = 4^3 = 64$, and

$$\gcd(a^{3!} - 1, n) = \gcd(63, 10001) = 1$$

Next $a^{4!} = (a^{3!})^4 = 64^4 \equiv 5539 \pmod{10001}$, and

$$\gcd(a^{4!} - 1, n) = \gcd(5538, 10001) = 1$$

Next $a^{5!} = (a^{4!})^5 = 55395 \equiv 7746 \pmod{10001}$, and

$$\gcd(a^{5!} - 1, n) = \gcd(7745, 10001) = 1$$

Next $a^{6!} = (a^{5!})^6 = 77466 \equiv 1169 \pmod{10001}$, and

$$\gcd(a^{6!} - 1, n) = gcd(1168, 10001) = 73.$$

We've run into a gcd that is bigger than 1 and not equal to $n = 10001$, so jackpot! 73 must be a prime factor of n. Then we can compute quickly that $10001/73 = 137$, so $10001/73 = 137$ and we are done.

Lenstras Elliptic Curve Method

Given an integer n, we use the following steps to find factors of n. [2]

1. Check that n isn't divisible by 2 or 3, and that n isn't a perfect power.
2. Choose random integers a, x, y between 1 and n.
3. Let $b = y^2 - x^3 - ax \pmod{n}$.
4. Calculate $D = \gcd(4a^3 + 27b^2; n)$.
   - If $1 < D < n$, we are done.
   - If $D = 1$, proceed to Step 5.
   - If $D = n$, go back to Step 2 and choose a different a.
5. Let E be the elliptic curve $E : y^2 = x^3 + ax + b$, and let $P = (x, y) \in E$.
6. Choose a number k which is a product of small primes raised to small powers. For example, a good choice is $k = \mathrm{lcm}(2, 3, \ldots, B)$ for some integer $B \approx 100$.
7. Compute $kP \pmod{n}$.
8. If kP lies on E, go back to Step 2 and choose different values for a, x, y. Otherwise, Step 7 yields a factor of n.

Example

Consider $n = 455839$. Let $E : y^2 = x^3 + 5x - 5$, $P = (1, 1)$, $k = 10!$ We begin by finding

$$2!P = 2P \pmod{n}$$

by using the algorithm of adding points on the elliptic curve

$$2P = (14, -53) \pmod{455839}$$

$$4P = (259851, 116255) \pmod{455839}$$

$$6P = (179685, 28708) \pmod{455839}$$

Similarly, we find that $4!P, 5!P, \ldots 7!P$ all lie on E, but computing $8!P$ requires inverting $599 \pmod{n}$ which isn't possible. This is because 599 is a factor of n, and we conclude that $n = 599 \cdot 761$.

Summary

Lenstra's ECM is known to reliably find factors with up to 25 digits, and there has even been found a prime factor with 83 digits using ECM [6]. The algorithm is, however, much more difficult to implement as the point addition is a more complicated procedure and it isn't quite clear which elliptic curve should be chosen. It is not obvious when we should stop sing Lenstra's ECM to find factors. In fact, the success of Lenstra's ECM is somewhat random (if we choose random curves), but even so its average success rate is so high that in practice one typically uses Lenstra's ECM after using Trial Division to "filter out" more small factors before moving on to more general purpose factoring algorithms.

References

[1] N. Koblitz, *A course in number theory and cryptography*, Springer Science & Business Media vol.114, 1994
[2] T. Browning, *Lenstra Elliptic Curve Factorization*, 2016
[3] A. Chrzszczyk, *Algorytmy teorii liczb i kryptografii w przykadach* Wydawnictwo BTC, 2010.
[4] L. Zeller *Improving Lenstra's Elliptic Curve Method*, Oregon State University, 2010
[5] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of computation 48.177 (1987): 243-264.
[6] http://www.loria.fr/ zimmerma/records/top50.html.

Contact: Lomza State University of Applied Sciences, email: wmaleszewski@pwsip.edu.pl