Factorization Algorithm Based on the Elliptic Curves Theory

George Vostrov
Ph. D. of Technical Sciences
Odessa national polytechnic university
Odessa, Ukraine
vostrov@gmail.com

Ivan Dermenzhy
Odessa national polytechnic university
Odessa, Ukraine
Ivandermenji97@gmail.com

Abstract—**In this article elliptic curve theory and its applications are considered. Much attention was paid to the possibility of composite numbers factorization problem solving by using the theory of elliptic curves. The Lenstra's method was analyzed and described in detail. The ways of its optimization were given. Algorithm's software implementation is developed.**

Index Terms—**elliptic curve, pseudo-curve, modular form, factoriazation.**

I.INTRODUCTION

Such structures as elliptic curves have been known for more than a century. Elliptic curves theory originally was used in classical analysis, in abstract and computational number theory, and occupied a fundamental position in these areas [1]. It is gaining increasing popularity in the applied fields of mathematical and information sciences nowadays. These objects are critically important in the cryptography, for the solving problem of the discrete logarithm and factorization, and also for the construction of cryptographic protocols. It also has a good perspective for use in the building of complex dynamic systems. The apparatus of the elliptic curves theory has many applications. Its significance is difficult to assess. Nevertheless, this direction is relatively "young" and has many gaps and unresolved problems.

The problem of factoring composite numbers into simple factors has a long and rich history, but despite this, it still does not have an effective solution. The surprising opportunity of using elliptical curves to solve this problem gives the hope for the creating more efficient factorization algorithm than those that already exist. The existing Lenstra's method, which is based on the theory of elliptic curves, provides subexponential computational complexity. Its efficiency is on the same level with the best modern methods. At the same time, it has a great space for optimization, this fact allows to believe that further research and development of the Lenstra's method will lead to a qualitative result.

II. CONCEPT OF THE ELLIPTIC CURVES METHOD

An important feature of the elliptic curves method is that its performance does not depend on the factoring number itself, but on its smallest divisor value [2]. This moment is significant for the method, since it opens up new possibilities for its use in combination with other factorization algorithms. Such as the method of a quadratic sieve, which is also subexponential, but it works faster for numbers whose dividers have a greater bit capacity. The Lenstra's method is the best algorithm for finding simple divisors of 20-25 characters' length [2].

The elliptic curve is the set of cubic equation solutions

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1)$$

where a_1, a_2, a_3, a_4, a_6 - coefficients from the field over which the curve is constructed [2]. This equation is presented in a general form, in the case of constructing a curve over a set of rational numbers, or over fields whose characteristic is different from 2 and 3, this equation can be simplified to $y^2 = x^3 + ax + b$, this kind of equation is called the Weierstrass form. This curve must be nonsingular and include point at infinity. The arithmetic of elliptic curves allows us to state that if n – is a prime number the point at infinity means a unique additional projective point on an elliptic curve that does not correspond to any affine point. If n is composite number, then there are other projective points, which do not correspond to any affine point. Nevertheless, we will allow only one additional point that corresponds to the projective solution [0;1;0]. Due to this limitation in the definition of the elliptic curve group, the pseudo-elliptic curve no longer forms a group with a composite n. It is easy to prove that there are pairs of points P and Q, for which the sum $P+Q$ – is undefined. This explains by the structure of the angular coefficient:

$$m=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, & if\ x_1\neq x_2\\ \dfrac{3x_1^2+a}{2y_1}, & if\ x_1=x_2\end{cases}, \qquad (2)$$

where $P=(x_1,y_1)$, $Q=(x_2,y_2)$.

The above results carry over to the elements of the set $E_{a,b}(Z_n)$, which differ from elliptic curves in the case when $n-$ is a composite number. [3]. In this case, the concept of elliptical pseudo-curve is used this curve defines by the conditions:

1. $a,b\in Z_n$
2. $G.C.D.(a,b)=1$
3. $G.C.D.(4a^3+27b^2,n)=1$
4. $E_{a,b}(Z_n)=\{(x,y)\in Z_n\times Z_n : y^2=x^3+ax+b\}\vee\{O\}$,

where O – infinitely corresponded point.

In a strict mathematical formulation, this curve is not considered as an elliptic curve (such a curve is also called pseudo-curve), since F_p is not a field according to it the operations of finding the inverse element that are necessary to find the sum of the points of the curve are not always feasible in it. It goes from the impossibility of calculating the sum of two points $P(x_1,y_1)$ and $Q(x_2,y_2)$, it turns out that the difference between the first coordinates x_2-x_1 must be equal to zero modulo one of the divisors of n, thus, computing the greatest common divisor G.C.D. (n,x_2-x_1), there is a divisor of the given composite number [9]. Lenstra's algorithm is to select an arbitrary base point P_0 and pseudo curve $E_{a,b}(F_p)$ and to multiply it subsequent by various prime numbers and their degrees until get:

$$kP_0=\infty(\mathrm{mod}\ p), \qquad (3)$$

where p – is one of n divisors.

In addition, there is the possibility of the divisor obtaining as G.C.D. of the curve discriminant and factorized number. However, all the features of the discriminant that allow to receive the divisor in this way are unknown, this question is an extremely important for research.

Since, none of the divisors of a composite number is known, it is not possible to check whether condition (3) is fulfilled, on this basis, a sign of the algorithm successful completion is that the condition G.C.D. $(n,c)=d>1$ is fulfilled when calculating the angular coefficient [3].

The algorithm can be represented in the following form:

The input is a composite number n, which must be decomposed into prime factors.

1. The limit of the first stage b_1 is chosen.
2. A random curve $E_{a,b}(Z_n)$ and a point on it with coordinates (x,y) are generated. Moreover, $b=y^2-x^3-ax \bmod n$ and $g=G.C.D.(n,4a^3+27b^2)$. Further, if $g=n$, then we have to return to the curve generation and if $1<g<n$, then a divisor is found.
3. For every prime number $p<b_1$ the greatest degree is determined α_i such that $p_i^{\alpha_i}\le b_1$. Then a loop is executed for all $j=1:\alpha_i$, $P=p_iP$, as a result of which the point P multiplies by p^{α_i}. Each multiplication by p is performed using the elliptic multiplication algorithm: the addition-subtraction scheme [3].

III. METHOD ANALYSIS

The number of performed arithmetic operations is estimated by the value: $L_p\left[\frac{1}{2};\sqrt{2}\right]$ at L-notation, where p – is smallest divisor of n [3]. L-notation, is an asymptotic notation analogous to O-notation, that is used for the approximate estimation of computational complexity of the algorithm and is determined by the formula: $L_p[\alpha,c]=e^{(c+O(1))(\ln p)^{\alpha}(\ln\ln p)^{1-\alpha}}$, by $p\to\infty$, where, $\alpha=const$, $\alpha\in[0;1]$ [4].

The important result of the elliptic curves theory is the Hasse theorem. According to this theorem, the following assertion is true: the power of $E_{a,b}(F_{p^k})$ is satisfying the inequality: $p+1-2\sqrt{p}<\#E_{a,b}(F_{p^k})<p+1+2\sqrt{p}$, where $\#E_{a,b}(F_{p^k})-$ is the number of elliptic curve points, or in other words the power of a given curve, or the order of this curve [2].

In comparison of the three most effective subexponential methods: ECM (elliptic curve method), quadratic sieve method and numerical field sieve method, the decisive role is played by the dimension of the composite smallest divisor. In the case when the factorized number has a dimension exceeding the record for the remaining methods, the only way to find the divisor is the factorization by the Lenstra's method [3].

With the help of implemented in practice program by using the computer-programming language Java, the following results were achieved: with the smallest divisor 7 decimal digits long, the average work time is equal to – 8509.33 seconds, 6 decimal digits long – 498,3 seconds, 5 decimal digits long – 37.54 seconds, 4 decimal digits long – 6.985 seconds, 3 decimal digits long – 1.4 seconds, 2 decimal digits long – 0.166 seconds. In general, the results correspond to the subexponential estimation of the algorithm.

Until now, all calculations have been performed by modulo of factorized number. In case when the coordinates of the obtained points are calculated by modulo p, which is a

divisor of *n*, we get the following condition for the successful completion of the algorithm: $kP=\infty$, $k=\prod_{p_i^{\alpha_i}\le B_1} p_i^{\alpha_i}$ .In this case the curve $y^2=x^3+ax+b$ is constructed over the field F_p [3]. Let $l=\#E(F_p)$ is the number of curve points. Then according to Hasse theorem $l\in\left[p+1-2\sqrt{(p)},p+1+2\sqrt{(p)}\right]$. According to the fact that for every point *Q(x,y)* the condition $lQ=\infty$ is satisfied then, in order to ECM method to be successfully completed, it is necessary that factor *k* in equation (3) is divided by the order of the curve l. In the case when, all dividers of *l* do not exceed the boundary b_1, the last condition is satisfied. [3].

For the successful completion of an algorithm with two stages, it is required that all dividers of l, except the greatest one, were less than the boundary of the first stage, and the greatest divisor had degree $\alpha=1$ and was less than the boundary of the second stage. This condition is less strict, but it is characterized by all the same problems as in the case of one stage algorithm. Besides, this optimization, in addition to increasing the method convergence, leads to increasing in computational costs for each new generation of the curve [2].

Thus, the necessary boundary for the degrees of *l* divisors strongly depends on the value of $\#E_{a,b}(F_p)$, which is determinates by coefficients of elliptic curve *a* and *b*. At the moment the reliable algorithm for choosing a curve with the order divisor maximum degree smallest value is unknown [2].

It is important to research the probability of finding a certain *b*-smooth number in the Hasse interval. At the moment, it is not known whether there is always a smooth number in the interval [3]. The L-notation that based on the heuristic probabilistic methods of the Canfield-Erdoes-Pomerance theorem, gives an estimate that in order to obtain a smooth order of the group it is sufficient to take $L_p[\frac{\sqrt{2}}{2};\sqrt{2}]$ curves [5].

On the other hand, there is a need to evaluate the order of the generated curve, to change curves until we get smooth one. The algorithm could be greatly speed up with an efficient curve order evaluation method. Since the generation of a curve is a low cost operation, all the computational complexity is related to the search for prime numbers at the given interval and then multiplying the points of the curve by the given primes and their degrees. The problem is that there is no algorithm for the pseudo-curve's order calculating. The existing Schoof's algorithm for the curve order calculating, in addition to its laboriousness and complexity in implementation, is intended for curves constructed over finite fields. Knowing the divisor of the factorizable number, it is possible to compute the order of such pseudo-curve by using Schoof's algorithm. However, none of the divisors is known, moreover, the search for divisors is the goal of the Lenstra's method. Thus, the only way to solve this problem is a theoretical research of the elliptic curves structures and their various classes.

According to the empirical results, there is a certain ratio between the values of the curve parameters at which the summary required value of the first and second boundaries reaches its minimum [2]. Since the theoretical apparatus for the selection of these parameters has not been developed at the moment, the only way out is random generation of an elliptical curve by random selection of its parameters, and the most effective way of optimization is the parallel use of several curves. Because the value of the factor *p* is unknown, then the choice of boundary performed empirically that definitely degrades the reliability of the method practical convergence assessment.

Table I shows experimentally obtained results, which describes the recommended value of the first stage boundary and the number of parallel curves used for different values of the smallest divisor factorization [6].

TABLE I. THE OPTIMAL BOUNDARY AND THE NUMBER OF CURVES USED FOR DIFFERENT NUMBERS

Number of characters	Value of boundary	Estimation of the parallel used curves number
15	2000	25
20	11000	90
25	50000	300
30	25000	700
40	3000000	5100
45	11000000	10600
50	43000000	19300
55	11000000	49000
60	260000000	124000
65	850000000	210000
70	2900000000	340000

In the modular forms and elliptic curves theories, various areas of mathematical science are synthesized, such as: algebraic geometry, number theory, complex analysis, the theory of finite groups and fields, and many others [1]. Many successes in the solution of the number congruence determining problem has been achieved by sharing and development of this two directions [1]. The natural number is congruence if there exist a rectangular triangle with rational sides whose area is equal to a given number. In particular, the main breakthrough in this area is the Tunnel theorem [1], which is the result of the two this theories fusion.

Despite great efforts focused on the research of these areas, one fundamental and extremely complex issue has not been solved for them yet. Which are the similarities and differences of the given structures? Without a doubt, they have a huge number of similarities, but it is impossible to assert a complete analogy of these objects. The most significant achievement in this area is the modularity theorem, the authorship of Taniyama, Simura and Weyl [7]. This theorem establishes the relation between elliptic curves constructed over the field of rational numbers and modular forms that represent definite

analytic functions of a complex variable. According to this theorem, an elliptic curve over the field of rational numbers is a modulus.

The significance of this theorem is difficult to underestimate, since it is in some way a generalization of Fermat's Great Theorem, because any counterexample to Fermat's theorem is eventually reduced to a nonmodular elliptic curve [8]. Fermat's grand theorem was solved by joint theoretical apparatus of the theory of elliptic curves and modular forms.

Since the Lenstra's method is a direct descendant of the *(p-1)*-Pollard method, it also has an extension in the form of a second stage [2]. The point of which consists in the using of the points obtained at the first stage with further multiplication by prime numbers that have values over the first stage boundary [2].

In addition to this optimization and its variations, there are a lot of other ways to optimize the method, in particular, Crandall and Pomerance suggest [3] the following:

1. Special parameterization, in order to quickly obtain random curves.

2. Selection curves which orders are divided by 12 or 16 [3].

3. Optimizing elliptic algebras by using a fast Fourier transform (FFT) and others.

The most effective way to optimize the elliptic curves method is to use parallel implementation with distributed memory [9], when the same number is attempted to decompose by using many different randomly generated curves at the same time. Thus, it is possible to obtain almost linear acceleration [9]. It becomes possible to use large amount of computing power with the help of cloud computing provided by a many services, such as Amazon, in order to speed up the factorization process.

Also, the right choice of boundaries is important, its allows to get a significant reduction in the use of time resources during the algorithm performance. For the correct choice of such boundaries, the Brent's table [10] is used. In this table the recommended boundary values for close numbers of a certain digit are indicated.

CONCLUSIONS

The work shows the relevance of elliptical curves and their research. The importance of their use in the factorization of composite numbers is established. This is substantiated by the fact that the problem is fundamental for a number of theoretical and applied areas, and its solution based on the elliptic curves theory is an extremely effective. A great perspective of this method development has been established. This is evidenced by the existence of a large number of optimizations among which parallel implementation of the algorithm is most effective. This work shows that the using of these optimizations, leads to significantly improvement of results. Lenstra's method on the basis of the elliptic curves theory is described and analyzed in detail. Its program realization is carried out, the results of its work are shown. The ECM algorithm, due to its subexponential nature, is well applicable in practice and it should be investigated in more detail, due to its prospects in terms of optimization.

Despite all the advantages of this method it is not devoid of disadvantages and complexities. A lot of attention is paid to these moments in this work. The problem of the heuristic method character, which is expressed in the random generation of curves, is analyzed in detail. Empirical results of the boundary choosing problem solving are described. Fundamental problems of the elliptic curves theory are considered, in particular, the question of these structures and modular forms analogy. Also, it is important to research the features of the curve discriminant that makes possible to obtain the factorized number divisor.

REFERENCES

[1] Koblitz N. Introduction to Elliptic Curves and Modular Forms– Graduate Texts in Mathematics. 97 (2nd ed.). Springer-Verlag. – 320 p. — ISBN 0-387-97966-2/

[2] Ишмухаметов Ш. Т. Методы факторизации натуральных чисел. — Казань: Казан. ун.. — 2011. — 190 с.

[3] Crandall R. E., Pomerance C. B. Prime numbers: A Computational Perspective. — New York: Springer-Verlag, 2001. — 545 p. — ISBN 0-387-94777.

[4] Carl Pomerance, Analysis and comparison of some integer factoring algorithms, In Mathematisch Centrum Computational Methods in Number Theory, Part 1, — 139 p. — , 1982.

[5] Canfield E. R., Erdős P., Pomerance C. On a Problem of Oppenheim concerning "Factorisatio Numerorum" (англ.) // Journal of number theory. — 1983. — Вып. 17.

[6] Dario Alpern's Web site: Factorization using the Elliptic Curve Method (ECM) [Electronic resource] URL: https://alpertron.com.ar/ECM.HTM.

[7] Conrad, Brian, Fred Diamond, Richard Taylor. Modularity of certain potentially Barsotti-Tate Galois representations, Journal of the American Mathematical Society 12 (1999), 567 p.

[8] Соловьев Ю.П. (2 1998). «Гипотеза Таниямы и последняя теорема Ферма». Соросовский Образовательный Журнал: 138 — с.

[9] Ефимов С.С., Макаренко А.В., Пыхтеев А.В. Параллельная реализация и сравнительный анализ алгоритмов факторизации с распределенной памятью, 2012, Омский государственный университет им. Ф. М. Достоевского.

[10] Brent R. (1999). "Factorization of the tenth Fermat number". Mathematics of Computation 68 (225): — 451p.