ELLIPTIC CURVES AND CRYPTOGRAPHY

K. A. DRAZIOTIS

Abstract. Elliptic curves have many applications in many areas of mathematics. From number theory to complex analysis and from cryptography to physics. In this short note we present basic applications of Elliptic curves in mathematics and especially in cryptography.

Keywords: Elliptic Curves; Finite Fields; Cryptography;

1. Introduction

Elliptic curves have many applications in,

- *Number theory* : Fermat Last Theorem, BSD conjecture[1].
- *Cryptography* : Lenstra factorization, Primality test of Goldwasser, Killian and Atkin, Diffie-Hellman key exchange, Pairing cryptography, Post Quantum protocols (SIDH).
- *Physics* : Paths of strings looks like elliptic curves, see [4].
- *Analysis* : Computation of elliptic integrals $\int_a^b R(x,y)dx, y^2 =$ cubic, the inverse function $f(y)=\int_y^\infty \frac{1}{\sqrt{4t^3-g_2t-g_3}}dt$ is the Weierstrass function $\wp$. Weierstrass function $\wp$ is formally defined

$$\wp(z;\omega_1,\omega_2)=\frac{1}{z^2}+\sum_{n^2+m^2\neq 0}\Big(\frac{1}{(z+m\omega_1+n\omega_2)^2}-\frac{1}{(m\omega_1+m\omega_2)^2}\Big),\ \omega_1,\ \omega_2\in\mathbb{C}.$$

This function is doubly periodic, with periods $2\omega_1$ and $2\omega_2$. Then, the pair $(\wp(z),\wp'(z))$ satisfies the equation $y^2 = 4x^3 - g_2X - g_3$, for suitable g_2, g_3. That is $\wp$ parametrizes elliptic curves over $\mathbb{C}$.

We begin with the definition of the elliptic curve.

Definition 1. An elliptic curve over a field $\mathbf{K}$ is defined by an equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbf{K}$$

and has non zero discriminant Δ. Its discriminant is given by the formula,

$$\Delta = -d_2^2d_8 - 8d_4^2 - 27d_6^2 + 9d_2d_4d_6,$$

where

$$d_2 = a_1^2 + 4a_2,\ d_6 = a_3^2 + 4a_6,\ d_4 = 2a_4 + a_1a_3,$$

$$\text{and}\ \ d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

This is a short note based on a talk, presented in the two-day symposium celebrating the 90th anniversary of Department of Mathematics of Aristotle University of Thessaloniki.

[1] BSD : Birch and Swinnerton-Dyer Conjecture

This equation is called Weierstrass equation. The condition $\Delta \neq 0$, ensures that the curve does not have singular points, i.e. points where there are more than one distinct tangents. Sometimes we write $E/\mathbf{K}$ to denote that E is defined over $\mathbf{K}$, i.e. the coefficients are in the field $\mathbf{K}$. Also there is one point at infinity, $\infty = [0:1:0]$ (in projective coordinates).

If the characteristic of the field is not 2 or 3, then there is a change of variables that transforms E to $y^2 = x^3 + Ax + B$, with $A,\ B \in \mathbf{K}$ and $\Delta = -16(4A^3 + 27B^2)$.

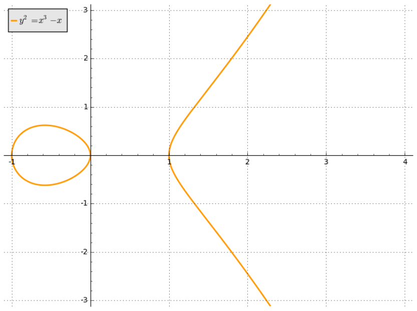


FIGURE 1. The curve $y^2 = x^3 - x$ over the reals. The discriminant is $\Delta = 64$.

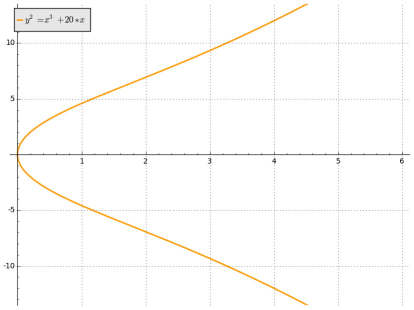


FIGURE 2. $y^2 = x^3 + 20x$, $\Delta = -512000$.

Other equivalent definitions are the following:

- A non singular projective genus 1 curve over $\mathbf{K}$ equipped with a $\mathbf{K}$-rational point O.
- A one dimensional group variety.

In figure 3 we define the addition over an elliptic curve. From the definition we see that is commutative. The neutral element is the point at infinity ∞. We usually denoted by O.

2. How the group $E(K)$ looks like?

The answer to this question depends on the field $\mathbf{K}$. If $\mathbf{K} = \mathbb{R}$ then the abelian group $E(\mathbb{R})$ has one or two connected components. Thus,

$$E(\mathbb{R}) \cong S^1 = \{z \in \mathbb{C} : |z| = 1\} \text{ or } S^1 \times C_2 \ (C_2 : \text{the cyclic group of two elements}).$$

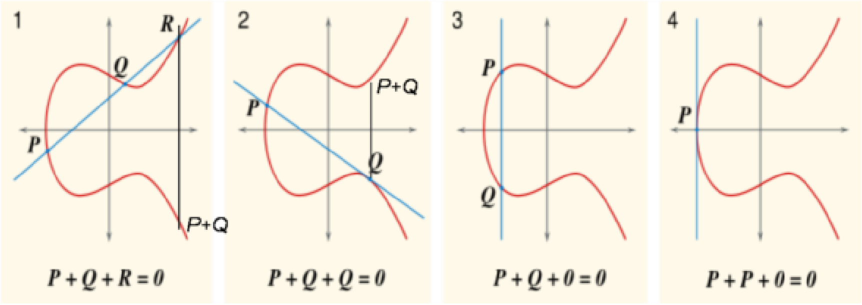


FIGURE 3. Group Addition in $\mathbb{R}$. We apply Chord tangent method to define the addition over an elliptic curve. Licence : Creative Commons.

The first case occurs if $x^3 + Ax + B$ has one real root and the second case if it has three real roots. If $\mathbf{K} = \mathbb{C}$, then $E(\mathbb{C}) \cong S^1 \times S^1$ (torus).

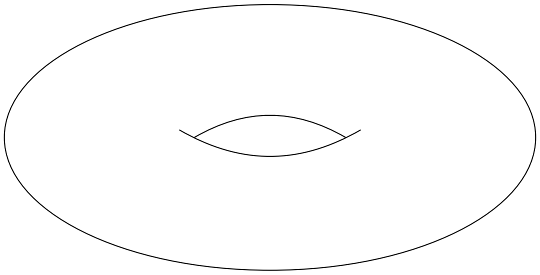


FIGURE 4. An elliptic curve over $\mathbb{C}$ is a torus.

The case $\mathbf{K} = \mathbb{Q}$ is more interesting. Mordell in 1922 proved the following,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_T \times \mathbb{Z}^r.$$

So a point $P \in E(\mathbb{Q})$ is written as

$$P = n_1P_1 + \cdots + n_rP_r + T, \ T \in E(\mathbb{Q})_T, \ n_i \in \mathbb{Z}.$$

The torsion part $E(\mathbb{Q})_T$ contains all the rational points of finite order. We have the following theorem.

Theorem 2.1 (Lutz-Nagell). *Let the elliptic curve $y^2 = x^3 + Ax + B$, with A, B integers. If $(x_0, y_0) \in E(\mathbb{Q})_T$ then $x_0, y_0 \in \mathbb{Z}$ and $y_0^2 | 4A^3 + 27B^2$.*

Mazur in 1977 proved the following landmark theorem.

Theorem 2.2 (Mazur, 1977). $E(\mathbb{Q})_T \cong C_N, \ N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ *or* $E(\mathbb{Q})_T \cong C_N \times C_{2N}, \ 1 \leq N \leq 4$.

The non negative integer r is called rank. If $r = 0$ the set $E(\mathbb{Q})$ has finitely many rational points else it has infinitely many.

Conjecture 2.3. *There are elliptic curves (over $\mathbb{Q}$) that have arbitrary large rank.*

Elkies found an elliptic curve with rank at least 28. Is not easy to compute the rank. This number is very useful in the case we want to compute the integer points of an elliptic curve. Also is related with a famous conjecture.
Birch and Swinnerton-Dyer Conjecture (BSD). BSD predicts the value of the rank in terms of the $L-$function attached to E. The $L-$function is defined as follows,

$$L(E,s)=\prod_{p\nmid N_E}(1-a_pp^{-s}+p^{1-2s})^{-1}\prod_{p\mid N_E}(1-a_pp^{-s})^{-1},$$

where $a_p=1+p-|E(\mathbb{F}_p)|$ and N_E is the conductor of E. This series converges, if $\Re(s)>3/2$. Hasse conjectured that this series can be defined in $\mathbb{C}$ and later this was proved. So it makes sense to define $L(E,s=1)$. Now, BSD conjecture asserts that $r=\text{ord}_{s=1}L(E,s)$. The quantity $\text{ord}_{s=1}L(E,s)$ is called analytic rank.

Conjecture 2.4 (BSD, 1960-1965)**.** $L(E,s)=c(s-1)^r+\sum_{j\geq 1}c_j(s-1)^{j+r},\ c\neq 0.$

In 2015 Bhargava & Shankar, proved that a positive proportion of elliptic curves over $\mathbb{Q}$ have analytic rank zero and (from a theorem of Kolyvagin) satisfy BSD conjecture.

For the set $E(\mathbb{Z})$ we have Siegel's result.

Theorem 2.5 (Siegel, 1928)**.** $|E(\mathbb{Z})|<\infty$.

Also, there are effective methods that allow us to compute exactly the set $E(\mathbb{Z})$.

2.1. The case $\mathbf{K}=\mathbb{F}_q$.

Here with q we denote a prime power and with p a prime number. In the case where the field $\mathbf{K}$ is finite, then the set $E(\mathbb{F}_q)$ is finite, but the computation of $|E(\mathbb{F}_q)|$ is not an easy task. Knowing this number is very important in the development of Elliptic Curve Cryptography (ECC).

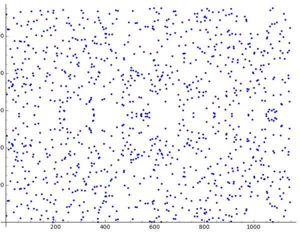


FIGURE 5. $p=1151$ and $E:y^2=x^3-x-1$. $E(\mathbb{F}_p)\cong\mathbb{Z}/560\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$

Hasse in 1936 proved the following basic theorem.

Theorem 2.6 (Hasse, 1936)**.**

$$\big|q+1-|E(\mathbb{F}_q)|\big|\leq 2\sqrt{q}.$$

A result of Waterhouse tell us that for every β with $|\beta|<2\sqrt{q}$ there is an Elliptic curve with $|E(\mathbb{F}_q)|=q+1-\beta$. A naive way to compute $|E(\mathbb{F}_q)|$ is by using brute force. This is only applicable for small q, say $q=O(2^{30})$. In 1995 Schoof managed to find a polynomial (bit complexity) algorithm for the computation of $|E(\mathbb{F}_q)|$ with bit complexity $O((\log_2 q)^6)$. Elkies and Atkin further improved this.

Definition 2. Let P be a point of an elliptic curve over a field $\mathbf{K}$, we define the order of the point P to be the cardinality of the subgroup generated by the point P. That is,

$$ord(P) = |\langle P\rangle|.$$

Definition 3. $E[m]$ is the set of all points of order m of an elliptic curve $E/\mathbf{K}$.

$$E[m] = \{P \in E(\overline{\mathbf{K}}) : mP = O\}.$$

$\overline{\mathbf{K}}$ is an algebraic closure of $\mathbf{K}$.

Theorem 2.7. *Let q be a prime p or a power of p.*
If $\gcd(p, m) = 1$, *then* $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$.
If $m = p^r m'$, $\gcd(p, m') = 1$, *then* $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_{m'}$, *or* $E[m] \cong \mathbb{Z}_{m'} \times \mathbb{Z}_{m'}$.

Furthermore the following holds.

Theorem 2.8. $E(\mathbb{F}_q) \cong \mathbb{Z}_n \times \mathbb{Z}_{cn}$, *where* $c \geq 0$. *If* $c > 0$ *then* $n|q - 1$.

Example 2.9. Let $E : y^2 = x^3 + 7$, and $p = 13$. Then $E(\mathbb{F}_7) \cong C_7$.

3. Discrete Logarithm Problem (DLP)

Let G be a multiplicative group. We define DLP over G.

Input: Let $g \in G$ and $a \in \langle g\rangle$.
Output: Find k such that $g^k = a$.

If $\mathrm{ord}(g) = n$, then k is uniquely determined mod n. The first key exchange protocol is due to Diffie and Hellman and is based on DLP over $\mathbb{Z}_p^*$.

Alice and Bob agree to a common prime field $\mathbb{Z}_p$ and a number g in $\mathbb{Z}_p^*$. Alice picks a random number a in $\mathbb{Z}_p$ and keeps it private. Also, Bob picks a random number b. Then, they exchange the following numbers.

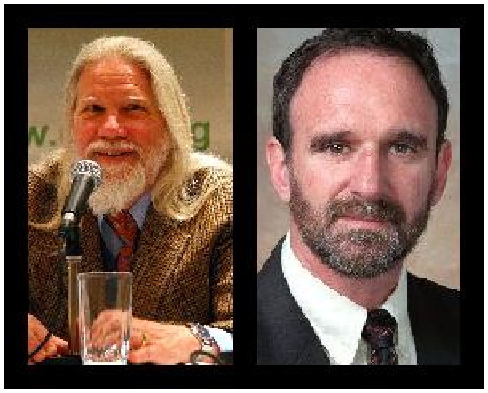
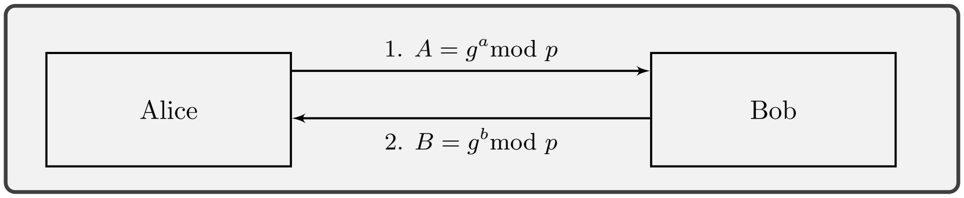


Figure 6. Whit Diffie and Martin Hellman (the photos have CC licence, see https://commons.wikimedia.org/wiki/File:Whit_Diffie_at_CFP_2007.jpg and https://commons.wikimedia.org/wiki/File:Martin-Hellman.jpg).



Alice computes,

$$B^a \bmod p = (g^b)^a \bmod p = g^{ba} \text{mod } p.$$

and Bob

$$A^b \bmod p = (g^a)^b \bmod p = g^{ab} \text{mod } p.$$

But $g^{ba} = g^{ab} \text{mod } p$, so they end up with a common number (their secret key).

An eavesdropper, say Eve, having the pair (g^a, g^b) tries to compute $g^{ab} \pmod p$. This problem that Eve has to solve is called *Diffie-Hellman problem.* One way to solve this is to compute the discrete logarithm over $\mathbb{Z}_p^*$. The inverse, is an open problem.

If we substitute the group of integers modulo p, with a group of an elliptic curve over a finite field, we get the Elliptic Curve variant of Diffie-Hellman (ECDH). This protocol is used by many TLS - servers. Also, Bitcoin protocol uses Elliptic curves for the signing procedure. The *bitcoin curve* is $y^2 = x^3 - 7$ over the prime field $\mathbb{F}_p$ with $p = 2^{256} - 2^{32} - 977$.

3.1. **Elliptic Curve Cryptography (ECC).** In 1985, Koblitz and Miller independently discover ECC. Although, the first application of elliptic curves in cryptography presented by H.Lenstra in 1984, by providing a factorization algorithm based on elliptic curves. Further, S. Goldwasser and J. Kilian in 1986, and Atkin (the same year) provided a primality test using elliptic curves.

The problem of elliptic curves that we use in cryptography is the Discrete Logarithm Problem (ECDLP). Let P be a point of an elliptic curve over a finite field and $G = \langle P \rangle = \{nP : n \in \mathbb{Z}\}$, be the subgroup generated by this point. Let Q be in G. Then, we want to find an integer k, such that $Q = kP$, $(k = \log_P(Q))$. The morphism $\log_P : G \to \mathbb{Z}/N\mathbb{Z}$ where $N = |G|$ is isomorphism. The inverse map $\phi : \mathbb{Z}/N\mathbb{Z} \to G$, is $\phi(k) = kP$. As we saw we can use elliptic curves to exchange keys using the DH protocol. Also, using El Gamal protocol we can use elliptic curves to send encrypted messages and finally, using DSA[2] with elliptic curves, we can sign messages. So, elliptic curves are used on all the fundamental cryptographic primitives.

3.2. **Attacks to DLP in a group** G**.** For a generic group G we have, Shank's Algorithm (baby steps-giant steps), Pollard Rho and Pohlig-Hellman (applied, when the order of the group is a smooth integer). All these algorithms are exponential. Although, we have better algorithms if the group $G = \mathbb{F}_p^*$. In this case we have the Index calculus method which has subexponential complexity (best algorithm today). First developed in 1920 by Kraitchik (for prime fields). The index calculus method does not seem to work for Elliptic curves. So, ECDLP provides smaller keys than RSA or classical DH for the same level of security.

[2] DSA, is the Digital Signature Algorithm.

4. Pairing based cryptography

In 2001 was proposed by D. Boneh, M. Franklin and others. They answered an old question of Adi Shamir :
Find an efficient public key cryptosystem, where the public key's of Alice are her identity.
Pairing based cryptography was also used to construct short signatures schemes (e.g. Boneh, Lynn and Shacham). Also, Joux using pairings managed to solve the tripartite DH problem. That is, three persons exchange a secret key in one round. A pairing is a map,

$$e_N : E[N] \times E[N] \to \mu_N = \{x \in \overline{\mathbb{F}}_q : x^N = 1\}$$

such that, $\gcd(N, p) = 1$, where $p = char(\mathbb{F}_q)$. It has the following properties,
Bilinearity

$$e_N(S_1 + S_2, T) = e_N(S_1, T)e_N(S_2, T),$$
$$e_N(S, T_1 + T_2) = e_N(S, T_1)e_N(S, T_2).$$

Non-degeneracy

$$e_N(T, T) \neq 1.$$

Computability
e_N can be efficiently computed.

Miller's algorithm allows us to compute in linear time the values of a Weil pairing. This is a basic reason for applying pairings in cryptography. In many pairing based protocols we use the following assumption.

Bilinear Diffie-Hellman Problem. Given P, aP, bP, cP compute $e_N(P, P)^{abc}$.

Further, pairings were used to attack ECDLP (MOV attack to ECDLP). Menezes, Okamoto and Vanstone, in 1993 showed that one can reduce the ECDLP for supersingular elliptic curves over a finite field $\mathbb{F}_q$ to a classical DLP in $\mathbb{F}^*_{q^d}$ with $d \leq 6$. Supersingular elliptic curves are defined by the property, $|E(\mathbb{E}_q)| \equiv 1 \pmod{p}$.

5. Quantum Attacks to DLP

Peter Shor in 1994, discovered a polynomial time (probabilistic) algorithm that solves DLP (and factorization problem, too) in a generic group G. So, if a quantum computer with large enough memory constructed in the future, ECDLP will not be secure (and all the modern Public Key crypto, too). This algorithm needs

$$O\big(\log_2 r(\log_2 \log_2 r)(\log_2 \log_2 \log_2 r)\big)$$

quantum gates, where r is the order of the group G. In other words, if $d = \log_2 r$ then the bit complexity is $O(d^3)$. For memory we need $\approx 10d$ qubits. We remark that this algorithm has polynomial bit complexity and is generic. Works, both in $\mathbb{F}_q^*$ and for elliptic curves. The Shor's algorithms proves that FACTOR problem and DLP is in BQP complexity class : **B**ounded-error **Q**uantum **P**olynomial complexity class. Today (2019) IBM-Q, the quantum computer of IBM has 20 qubits memory.

Shor's algorithm reduces the problem of factorization/DLP to a specific class of a general problem called HSP : **H**idden **S**ubgroup **P**roblem.

Definition 4. HSP : Given a description of a finite group G and a function f on G that is promised to be strictly $H-$periodic for some subgroup H, find a generating set for H.

Simon, Shor and Kitaev proved that, if G is Abelian then we can solve HSP in polynomial time with a bounded error in a quantum computer. That is, we can efficiently find a subset X of G that generates the subgroup H, with probability $2/3$. Ettinger, Hoyer and Knill in 2004, improved the probability to be exponentially small. Regev in 2008 provided a subexponential quantum algorithm for the Dihedral group $\mathbb{D}_N$ (is non-Abelian for $N > 2$). Also in 2004 showed that an efficient solution to HSP implies a solution to the SVP[3] (a hard lattice based problem).

If a quantum computer with large memory ever constructed, then the most well known public key cryptosystem, RSA, and the digital signature (EC)DSA, shall break and all the current security in Internet will be comprised.

5.1. **Quantum resistant ECC.** Elliptic curves again provide a solution. The problem of finding isogenies over superelliptic curves is (believed to be) quantum resistant. Based on the previous problem we can define a Supersingular Isogeny Diffie - Hellman key exchange (SIDH) protocol. The proposed protocol uses $2688-$bits public keys for $128-$bits security. Further, provides forward secrecy, i.e. protects past sessions against future compromises of secret keys or passwords.

This protocol is based on the following problem.

Isogeny Walk Problem.
Input : Two isogenous elliptic curves E, E'.
Output : An isogeny $\phi : E \to E'$ of *smooth* degree.
This problem is considered computationally hard. Note that, if we are looking for isogenies of specific degree say ℓ, then Elkies (1992) provided an algorithm $O(\ell^2)$.

References

[1] Andrea Enge, *Elliptic curves and their application to cryptography,* Springer 1999.

[2] S. Galbraith, *Mathematics of public key cryptography.* Cambridge University Press, Cambridge, 2012.

[3] A.H. Koblitz, N. Koblitz, and Menezes, *Elliptic curve cryptography : The serpentine course of a paradigm shift.*

[4] Linh Thi Dieu Pham, *From String Theory to Elliptic Curves over Finite Field* $\mathbb{F}_p$, Bard University, 2014.

[5] J.H. Silverman, *The arithmetic of Elliptic curves*, 2009, Springer.

[6] J.H. Silverman, Talk, *The Ubiquity of Elliptic Curves.*

[3] SVP, is the Shortest Vector Problem. Is proved to be NP-hard under randomized reductions. See [2].