Topological Interpretation of Elliptic Curves

Topological Interpretation of Finite Cyclic Groups

Avneet Singh
Interplanetary Company UG
sshmatrix@proton.me

ABSTRACT

Elliptic curves form the backbone of most cryptography today and are expected to feature in the post-quantum world through Zero-Knowlege algorithms. Most literature on Elliptic curves starts from the definition of a cubic symmetric polynomial and builds upon the group theoretic interpretation of finite fields. This may be sufficient to grasp the mere necessary details for implementing Elliptic curves in practise, but not necessarily ideal if one wants to understand why Elliptic curve geometry is unique and useful. To most readers, it can appear that Elliptic curves were drawn from a magic hat. In paper will illustrate that this is clearly not the case and there exists a very legitimate reason for how and why the humanity ended up using Elliptic curves for cryptography.

INTRODUCTION

This paper is intended as a standalone appendix to the main paper titled 'Intuitive Interpretation of Non-Interactive Zero-Knowledge Cryptography' [1]. The main paper deals with pretty much the entire field of cryptography starting from basic RSA to advanced Zero-Knowledge algorithms. In interest of conciseness, several important aspects of Elliptic curves couldn't be discussed in detail in the main paper; this document is an attempt to address those shortcomings for the overtly inclined reader. We'll also touch some peripheral topics that have tied number theory and elliptic curves at the hip. Having said that, we'll follow the same theme as the main paper and avoid jargon like plague.

INCHING TOWARD ELLIPTIC CURVES

The hint is in the name. Elliptic curves are related to ellipses and their discovery was 'accidental' so to speak; most of the initial work toward elliptic curves was done by Newton, Legendre, Fermat, Euler, Abel and Jacobi. In simple terms, an elliptic curve is a paramterisation of an ellipse's circumference or arc length and it easily derivable. To begin with, consider an ellipse described by its semi-major and -minor axis lengths of α and γ $(=1)$, i.e. eccentricity $e^2 = 1 - 1/\alpha^2$. Such an ellipse is described by: $(1 - e^2)\,x^2 + y^2 = 1$. We can simplify it further by safely[1] replacing the constant $1 - e^2$ with k^2, yielding $y^2 = 1 - k^2\,x^2$. Let's try to calculate the circumference C(k) of this ellipse; this will equivalent to integrating $(\delta x^2 + \delta y^2)^{1/2}$ along the curve in one of the four cartesian quarters and then multiplying it by 4. This results in

$$C(e) = 4\sum(\delta x^2 + \delta y^2)^{1/2},\ \text{for}\ x = [0,\ \alpha], \tag{1}$$

[1] such that the values of both e and k lie between 0 and 1, aka [0, 1]

$$C(e) = 4\sum_0^{\alpha}(\delta x^2 + \delta y^2)^{1/2} = 4\alpha\sum_0^1\left[\frac{1 - e^2x^2}{1 - x^2}\right]^{1/2}\delta x. \tag{2}$$

This is already the **elliptic integral** of the second kind[2] and it is particularly difficult to evaluate analytically. When e = 1 (k = 0), it is straightforward and evaluates to 4α as expected. When e = 0 (i.e. circles; k = 1), it is also relatively straightforward and evaluates naturally to

$$C(e)_{k=1} = 4\alpha\sum_0^1\frac{1}{(1 - x^2)^{1/2}}\delta x = 4\alpha\sum_0^1\sin^{-1}(x) = 2\pi\alpha. \tag{2a}$$

In conjunction with the well-known trigonometric parameterisation of ellipse with $(x, y) \to (\alpha\sin\theta, \gamma\cos\theta)$, the general elliptic intergal reduces to,

$$C(e) = \sum_0^{\pi/2}(1 - e^2\sin^2\theta)^{1/2}\delta\theta. \tag{3}$$

In strict sense, the inverse of the integrand in the elliptic integral (2)–(3) is already the elliptic curve, but it is not straightforward to interpret in this form. In order to arrive at a more intuitive and interpretive form of elliptic curve, we perform a paramterisation of the form $\theta^n = 1 - e^2x^2$. Let's consider in particular the parametrisation for n = 1, such that $\theta = 1 - e^2x^2$. This leads to

$$C(k) = \frac{1}{2}\sum_{k^2}^1\frac{\theta}{[\theta(\theta - k^2)(\theta - 1)]^{1/2}}\delta\theta = -\frac{\mathbf{i}}{2}\sum_{k^2}^1\frac{\theta}{E(\theta)}\delta\theta, \tag{4}$$

where **i** is the usual complex unit, i.e. $\mathbf{i} = \sqrt{-1}$. The 3-order polynomial term in the denominator is of the form

$$E^2(\theta) = \theta^3 + r\cdot\theta^2 + p\cdot\theta + q,$$

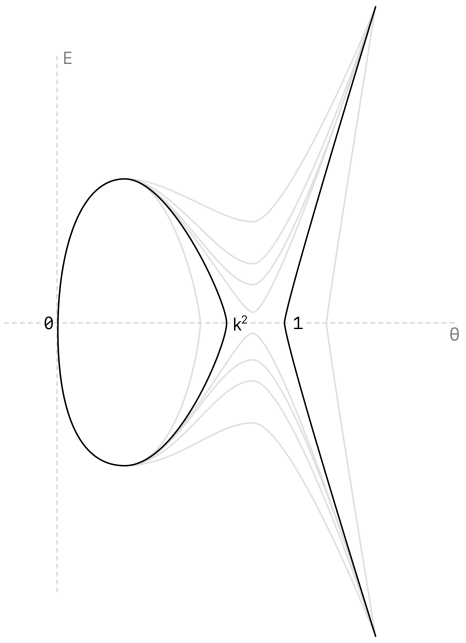

Figure 1: Family of Elliptic curves

and this is precisely the more recognisable form of the **elliptic curve**! Note that the form of $E(\theta)$ in the above example asserts three roots of $E(\theta)$, i.e. 0, k^2, 1. This is however not true for generic elliptic curves which may have only one real root depending on the values of p, q and r, all of which are functions of k in return. In our particular example, $r = -(1 + k^2)$, $p = k^2$ and $q = 0$. Some readers may feel cheated at this point since we have just said that an elliptic curve is simply the square root of a cubic polynomial! This is indeed correct but not every cubic polynomial is an elliptic curve; the coefficients of the cubic polynomial must be such that there are no repeated roots, i.e. they represent a legitimate ellipse with legal values of e^2 and k^2.

[2] 'second kind' due to the presence of θ in the numerator in its parameterised form; 'first kind' has 1 in the numerator

INITIATION BY JACOBI

It was Abel who first understood that the inverse of the intergal in (2a) is periodic and more relevant than the intergal itself, i.e.

$$F^{-1}(\bar{x}) = 1/\sum_{0}^{\bar{x}} \frac{1}{(1 - x^2)^{1/2}}\,\delta x = \sin^{-1^{-1}}(\bar{x}) = \sin(\bar{x}), \tag{5}$$

Legendre in the past had re-arranged equation (2) in another form which turned out to be more useful for Jacobi. Legendre's form of (2) simply reads

$$C(e) = 4\alpha\sum_{0}^{1} \frac{1 - e^2x^2}{[(1 - x^2)(1 - e^2x^2)]^{1/2}}\,\delta x, \tag{6}$$

Legendre noted that integrating the elliptic integral of second kind is easier if one knows the integral evaluation of the first kind[2], i.e. the same equation as above but with the numerator set to 1,

$$C(\bar{x}) = 4\alpha\sum_{0}^{\bar{x}} \frac{1}{[(1 - x^2)(1 - e^2x^2)]^{1/2}}\,\delta x. \tag{7}$$

In parameterised form, elliptic integral of the first kind reads,

$$C(e) = \sum_{0}^{\pi/2} \frac{1}{(1 - e^2\sin^2\theta)^{1/2}}\,\delta\theta, \tag{8}$$

which is eerily innocent-looking and quite similar to (3) except that the integrand is inverted. This particular form of the elliptic integral of the first kind circle is where Jacobi made the first meaningful step toward parameterising generic elliptic curves. While generalising the integral $F(x)$ to $F(e, x)$ for non-zero e, Jacobi concluded that he didn't in fact need to solve the integral but instead simply attempt to gauge its properties (e.g. periodicity) by analysing the integrant. Jacobi's playtime revealed that the symmetric appearance of the terms e^2 and x^2 in the general elliptic integral equates to a bi-periodic function with complex periods! In simpler words, equation (7) is double-periodic with both periods ($\hat{\omega}_1, \hat{\omega}_2 \in \mathbb{C}$) being complex numbers, such that $C(\bar{x}) = C(\bar{x} + n_1\cdot\hat{\omega}_1) = C(\bar{x} + n_2\cdot\hat{\omega}_2)$, where $\hat{\omega}_1$ and $\hat{\omega}_2$ must necessarily be linearly-independent in $\mathbb{R}$, aka they are not mutually related by $\hat{\omega}_1 \neq \mathbb{R}\cdot\hat{\omega}_2$. Jacobi had arrived at this result after he fucked around with $C(\bar{x})$ and assumed it to be a sine-inverse-like function[2] (denoted $\sin_L^{-1}\bar{x}$), and found out that it did in fact have properties similar to a sinusoid such as periodicity. This however wasn't the most important assertion; Jacobi further found that no single-variable function has more than two independent periods, and all except elliptic integrals of the first and second (and third) kind have at most one period only. This was arguably the first solid proof that elliptic integrals were a special class of functions.

EISENSTEIN'S ENGINEERING

_

REFERENCES

[1] Intuitive Interpretation of Non-Interactive Zero-Knowledge Cryptography

[2] one can observe this by integrating (6) using the elementary 'by parts' formalism
[2] due to the said integral being literally $\sin^{-1}(\bar{x})$ for $e = 0$

METADATA

Github:
Contracts:
Source:
SHA-1 Checksum:
Date: August 12, 2023