On the Rational Cubic Curve Cryptosystems

Heather Henkel and X. Alex Wang
Department of Mathematics and Statistics
Texas Tech University
Lubbock, TX 79409-1042
USA

Abstract

In this paper, we study the group on $\mathbb{F}_q \cup \{\infty\}$ induced by rational cubic curves. We show that the group is isomorphic to either a subgroup of order $q+1$ of the multiplicative group of $\mathbb{F}_{q^2}$, or the additive group, or multiplicative group, of $\mathbb{F}_q$.

1 Introduction

It is well known that the points on an elliptic curve form an abelian group, and such a group structure has been used to implement the Diffie-Hellman key-passing scheme, and the ElGamal public-key cryptosystem and signature schemes. The elliptic curve cryptosystems have the potential to provide satisfied security with shorter key lengths [4, 5, 6].

An elliptic curve Γ is a nonsingular cubic curve in $\mathbb{P}^2$, and the group law is defined by the cord-and-tangent method [1]: Choose a point $O \in \Gamma$ as the identity of the group. For any two points $P, Q \in \Gamma$, let $\overline{PQ}$ be the line through P and Q. Then by Bézout's theorem [2], $\Gamma \cap \overline{PQ}$ contains 3 points counted with multiplicity. Let R be the third point in $\Gamma \cap \overline{PQ}$, Then $P * Q$ is defined to be the third point in $\Gamma \cap \overline{OR}$. The commutativity $P * Q = Q * P$ is obvious, and the associativity follows also from Bézout's theorem [1]. Such geometric construction can be applied to any irreducible cubic curves, including singular irreducible cubic curves. Note that a cubic curve is singular if and only if it is a rational curve, i.e. if and only if there is a polynomial mapping $\chi : \mathbb{P}^1 \to \mathbb{P}^2$ onto all but possible one point of the curve. The group law on a rational curve induces a pull-back group law on $\mathbb{P}^1$. In this paper, we investigate the group laws on $\mathbb{P}^1$ induced by rational cubic curves and the cryptosystems based on such group laws.

2 The Pullback Group on $\mathbb{P}^1$

Let $\mathbb{F}_q$ be a finite field of q elements, and $\mathbb{P}^n$ be the n dimensional projective space over the $\mathbb{F}_q$, i.e. the set of all lines through the origin in $\mathbb{F}_q^{n+1}$. Through any nonzero point $(x_0, x_1, \ldots, x_n) \in \mathbb{F}_q^{n+1}$ and the origin there is a unique line in $\mathbb{P}^n$. So the elements in $\mathbb{P}^n$ are represented by the equivalence classes of $\{(x_0, x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)\}$ where $(x_0, x_1, \ldots, x_n) \sim k(x_0, x_1, \ldots, x_n)$ for any nonzero $k \in \mathbb{F}_q$, and such equivalence classes are called the homogeneous coordinates of the elements in $\mathbb{P}^n$ [2].

Let Γ be a rational cubic curve in $\mathbb{P}^2$. Then there is a polynomial mapping $\chi : \mathbb{P}^1 \to \mathbb{P}^2$ of degree 3,

$$\chi(s,t) = (f(s,t), g(s,t), h(s,t)),$$

where f, g, h are homogeneous polynomials of degree 3, such that Γ is the closure of $\chi(\mathbb{P}^1)$. Write

$$\chi(s,t) = (s^3, s^2t, st^2, t^3)A$$

where A is an 4×3 full rank matrix over $\mathbb{F}_q$.

The projective space $\mathbb{P}^1$ can be considered as

$$\mathbb{P}^1 = \{(s,1)\} \cup \{(1,0)\} = \mathbb{F}_q \cup \{\infty\}.$$

Therefore for simplicity we write, $\chi(s,1) = \chi(s)$, and $\chi(1,0) = \chi(\infty)$, i.e.

$$\chi(s) = (s^3, s^2, s, 1)A$$

and

$$\chi(\infty) = (1,0,0,0)A$$

Let $\overline{\alpha\beta}$ be the line through the points α and β in $\mathbb{P}^2$. For any $a, b \in \mathbb{F}_q$, let the third point in

$$\Gamma \cap \overline{\chi(a)\chi(b)}$$

be $\chi(c)$. Then for $a \neq b$, c must be a solution of the equation

$$\det \begin{bmatrix} a^3 & a^2 & a & 1 \\ b^3 & b^2 & b & 1 \\ s^3 & s^2 & s & 1 \end{bmatrix} A = (b-a)(s-a)(s-b) \det \begin{bmatrix} a^3 & a^2 & a & 1 \\ a^2+ba+b^2 & a+b & 1 & 0 \\ s+a+b & 1 & 0 & 0 \end{bmatrix} A = 0,$$

and for $a = b$, a solution of

$$\det \begin{bmatrix} a^3 & a^2 & a & 1 \\ 3a^2 & 2a & 1 & 0 \\ s^3 & s^2 & s & 1 \end{bmatrix} A = (s-a)^2 \det \begin{bmatrix} a^3 & a^2 & a & 1 \\ 3a^2 & 2a & 1 & 0 \\ s+2a & 1 & 0 & 0 \end{bmatrix} A = 0.$$

In either case, c is the solution of

$$\det \begin{bmatrix} a^3 & a^2 & a & 1 \\ 3a^2 & 2a & 1 & 0 \\ s+2a & 1 & 0 & 0 \end{bmatrix} A = 0.$$

Therfore

$$c = -\frac{A_1 + (a+b)A_2 + abA_3}{A_2 + (a+b)A_3 + abA_4} \tag{2.1}$$

where A_i is the 3×3 minor of A obtained by removing the ith rows.

Fix a $\sigma \in \mathbb{F}_q$ to be the identity element of the group. Then $\chi(a*b)$ is the third point in

$$\Gamma \cap \overline{\chi(c)\chi(\sigma)},$$

and therefore the group operation is given by

$$a*b = -\frac{A_1 + (\sigma + c)A_2 + \sigma c A_3}{A_2 + (\sigma + c)A_3 + \sigma c A_4} \tag{2.2}$$

$$= \frac{(a+b)\alpha + ab\beta + \sigma(-\alpha + ab\gamma)}{\alpha - ab\gamma + \sigma(\beta + (a+b)\gamma)}, \tag{2.3}$$

where

$$\alpha = A_2^2 - A_1A_3, \quad \beta = A_2A_3 - A_1A_4, \quad \gamma = A_3^2 - A_2A_4.$$

The formula (2.3) can be simplified further. Note that any linear transformation on the homogeneous coordinates of $\mathbb{P}^1$ results in a new form of χ, which induces an isomorphic pull-back group on $\mathbb{P}^1$. Therefore we can assume

1. $\sigma = \infty$,

2. The inverse element of a is $-a$.

Applying these conditions to (2.3), we then have

$$\beta = 0$$

and corresponding group operation becomes

$$a*b = \frac{ab - \kappa}{a+b} \tag{2.4}$$

where $\kappa = \alpha/\gamma$.

Theorem 2.1. *If $\kappa = 0$, then the group operation is not defined for $0*0$, and the group $((\mathbb{F}_q - \{0\}) \cup \{\infty\}, *)$ is isomorphic to the additive group of $\mathbb{F}_q$.*

If $\sqrt{-\kappa} \in \mathbb{F}_q$, then the group operation is not defined for $\sqrt{-\kappa} * (-\sqrt{-\kappa})$, and the group $((\mathbb{F}_q - \{\pm\sqrt{-\kappa}\}) \cup \{\infty\}, *)$ is isomorphic to the multiplicative group of $\mathbb{F}_q$.

If $\sqrt{-\kappa} \notin \mathbb{F}_q$, then the group operation is defined for every points in $\mathbb{F}_q \cup \{\infty\}$, and the group $(\mathbb{F}_q \cup \{\infty\}, *)$ is isomorphic to a subgroup of the multiplicative group of $\mathbb{F}_{q^2}$. Therefore it is a cyclic group.

Proof. The operation is not defined if the homogeneous coordinates of $a*b$ becomes $(0,0)$, or equivalently, the numerator and denominator of $a*b$ are both zero. So the operation is not defined for $\sqrt{-\kappa} * (-\sqrt{-\kappa})$.

If $\kappa = 0$, then the operation can be written as

$$\frac{1}{a*b} = \frac{1}{a} + \frac{1}{b}.$$

Therefore the mapping $a \mapsto 1/a$ ($\infty \mapsto 0$) defines an isomorphism of $((\mathbb{F}_q - \{0\}) \cup \{\infty\}, *)$ and $(\mathbb{F}_q, +)$.

If $\kappa \neq 0$, then

$$\left(\frac{a^2-\kappa}{a^2+\kappa} - \frac{2a}{a^2+\kappa}\sqrt{-\kappa}\right)\left(\frac{b^2-\kappa}{b^2+\kappa} - \frac{2b}{b^2+\kappa}\sqrt{-\kappa}\right) = \frac{\left(\frac{ab-\kappa}{a+b}\right)^2 - \kappa}{\left(\frac{ab-\kappa}{a+b}\right)^2 + \kappa} - 2\frac{\frac{ab-\kappa}{a+b}}{\left(\frac{ab-\kappa}{a+b}\right)^2 + \kappa}\sqrt{-\kappa}$$

for $a, b \neq \pm\sqrt{-\kappa}$. Therefore if $\sqrt{-\kappa} \in \mathbb{F}_q$, the map

$$a \mapsto \frac{a^2-\kappa}{a^2+\kappa} - \frac{2a}{a^2+\kappa}\sqrt{-\kappa}, \quad \infty \mapsto 1$$

defines an isomorphism of $((\mathbb{F}_q - \{\pm\sqrt{-\kappa}\}) \cup \{\infty\}, *)$ and $(\mathbb{F}_q - \{0\}, \cdot)$.

If $\sqrt{-\kappa} \notin \mathbb{F}_q$, then the map defines an imbedding of $\mathbb{F}_q \cup \{\infty\}$ into the multiplicative group of $\mathbb{F}_q(\sqrt{-\kappa}) = \mathbb{F}_{q^2}$, and therefore $(\mathbb{F}_q \cup \{\infty\}, *)$ is a cyclic group of order $q+1$ (see [3, Theorem 5.3]). □

Remark 2.2. There is a very simple geometric interpretation of the group when $\sqrt{-\kappa} \notin \mathbb{F}_q$, but $\sqrt{\kappa} \in \mathbb{F}_q$. Consider the line defined by $y = \sqrt{\kappa}$ in $\mathbb{F}_q \times \mathbb{F}_q$. For any two non-horizontal lines through the origin (i.e. two points in $\mathbb{P}^1$), let α, β be the angles inclination of the lines, and $(a, \sqrt{\kappa}), (b, \sqrt{\kappa})$ be the points of intersections of the lines with the line $y = \sqrt{\kappa}$. Then

$$\cot\alpha = a/\sqrt{\kappa}, \quad \cot\beta = b/\sqrt{\kappa}$$

and

$$\cot(\alpha+\beta) = \frac{\cot\alpha\cot\beta - 1}{\cot\alpha + \cot\beta} = \frac{\frac{ab-\kappa}{a+b}}{\sqrt{\kappa}},$$

i.e. if we consider $(a, \sqrt{\kappa})$ as homogeneous coordinates of lines through origin in $\mathbb{F}_q^2$. Then the angle of inclination of $(a * b, \sqrt{\kappa})$ is the sum of the angles of inclinations of $(a, \sqrt{\kappa})$ and $(b, \sqrt{\kappa})$.

3 Examples and Final Remark

Example 3.1. Consider $\mathbb{Z}_{11}$ and let $\kappa = 1$. We have

$$\begin{array}{llllll} 3^0 = \infty & 3^1 = 3 & 3^2 = 5 & 3^3 = 10 & 3^4 = 9 & 3^5 = 4 \\ 3^6 = 0 & 3^7 = 7 & 3^8 = 2 & 3^9 = 1 & 3^{10} = 6 & 3^{11} = 8. \end{array}$$

Example 3.2. Consider $\mathbb{Z}_3(x)/(x^2+1) = \mathbb{F}_9$ and let $\kappa = 1 + x$. We have

$$\begin{array}{lllll} 2^0 = \infty & 2^1 = 2 & 2^2 = 2x & 2^3 = 2 + x & 2^4 = 2 + 2x \\ 2^5 = 0 & 2^6 = 1 + x & 2^7 = 1 + 2x & 2^8 = x & 2^9 = 1. \end{array}$$

It seems that when $\kappa \notin \mathbb{F}_q$, the discrete log problem over $(\mathbb{F}_q \cup \{\infty\}, *)$ is harder to solve than the problem over $\mathbb{F}_q$, and therefore the cryptosystem defined over $(\mathbb{F}_q \cup \{\infty\}, *)$ might be more secure than the cryptosystem defined over the multiplicative group of $\mathbb{F}_q$. The drawback is that more calculations are involved. The group operation can also be written in terms of homogeneous coordinates:

$$(a_1, a_2) * (b_1, b_2) = (a_1 b_1 - \kappa a_2 b_2, a_1 b_2 + b_1 a_2). \tag{3.1}$$

So the division in the calculation of a^n can be avoided until the last step.

References

[1] I. F. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[2] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[3] T. W. Hungerford, *Algebra*, Holt, Rinehart and Winston, New York, 1974.

[4] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of computation* 48, 1987, 203–209.

[5] N. Koblitz, A. Menezes, and S. A. Vanstone, "The State of Elliptic Curve Cryptography," *Designs, Codes and Cryptography* 19, 2000, 173–193.

[6] A. Menezes and S. A. Vanstone, "Elliptic Curve Cryptosystems and Their Implementation," *J. Cryptology* 6, 1993, 209–224.

[7] A. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," *IEEE Trans. Information Theory* 39, 1993, 1639–1646.

[8] N.P. Smart, "The Discrete Logarithm Problem of Elliptic Curves of Trace One," *J. Cryptology* 12, 1999, 193–196.