Curves, Conics and Cryptography, Oh My

Introduction

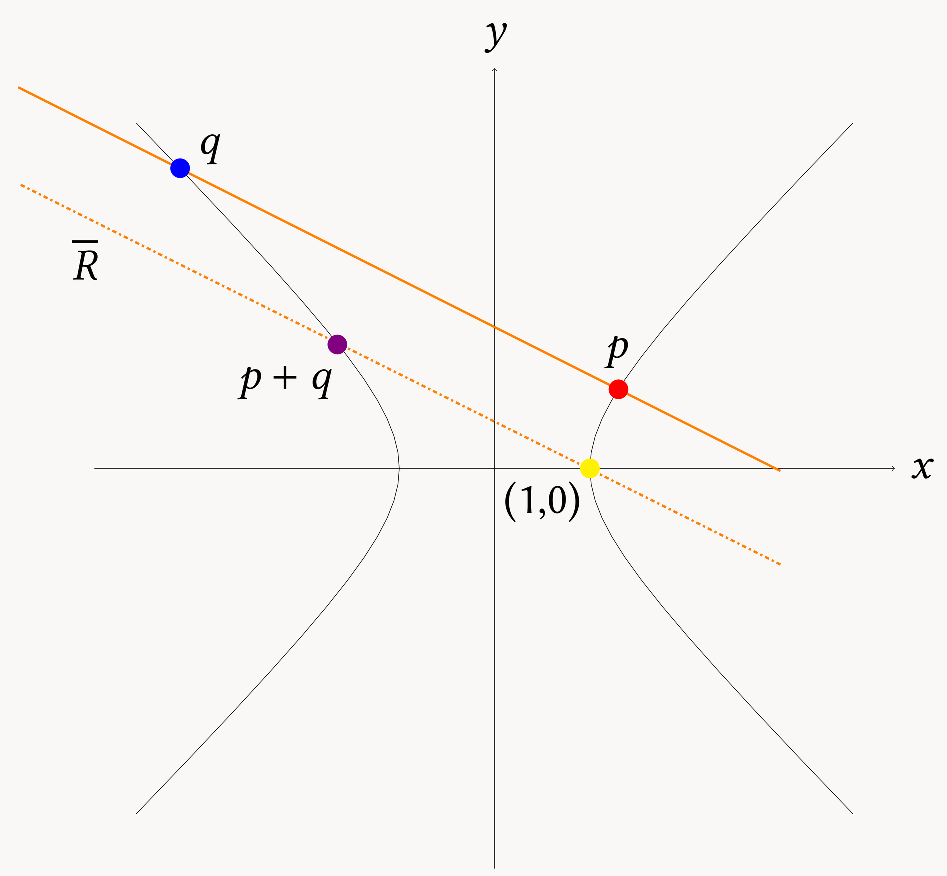
A conic is the curve in the xy-plane determined by the roots of a degree-two polynomial in x and y. They have been studied since antiquity. Our research team studied conics of the form C: $x^2 - dy^2 = 1$, $d \in \mathbb{Z}$, through a group law for adding points on the curve.
The goal of the project was two-fold:

1. To understand the group structure of conics
2. To use conics as a metaphor for understanding elliptic curves and their cryptographic applications

We treated C as a functor from commutative rings to groups and found the group structure of C when various common rings were inputted. Additionally, we studied the underlying theoretical reasons for the existences of such a nice geometric-algebraic relationship.

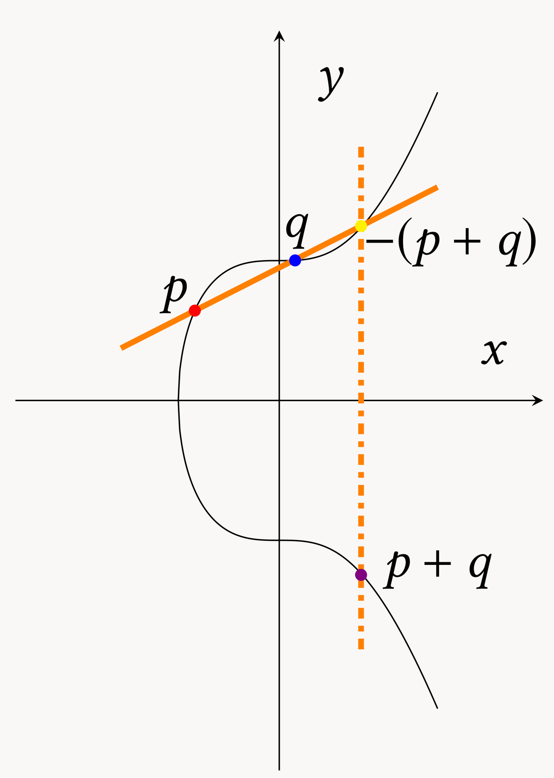
Conic Group Law

- Conics include **hyperbolas**, parabolas and circles
- There exists a natural group structure on the points of a conic:
  1. Given points p and q on C, draw a line through p and q, $\overline{pq}$
  2. Draw a line, $\overline{R}$, parallel to $\overline{pq}$ through the group identity (1,0)
  3. Mark as "$p+q$" the point of intersection between $\overline{R}$ and C besides (1,0).



Elliptic Curve Group Law

- Elliptic curves are cubics of the form E: $y^2 = x^3 + ax + b$
- Similar to conics, there exists a natural geometric group structure
- Elliptic curves live in projective space and thus ∞ is a point on the curve. In fact ∞ serves as the identity element.
- The natural group structure on the points of an elliptic curve:
  1. Given points p and q on E, draw a line through p and q, $\overline{pq}$.
  2. Mark as "$-(p+q)$" the third intersection of $\overline{pq}$ with E.
  3. Reflect $-(p+q)$ across the x-axis and mark the new point "$p+q$"

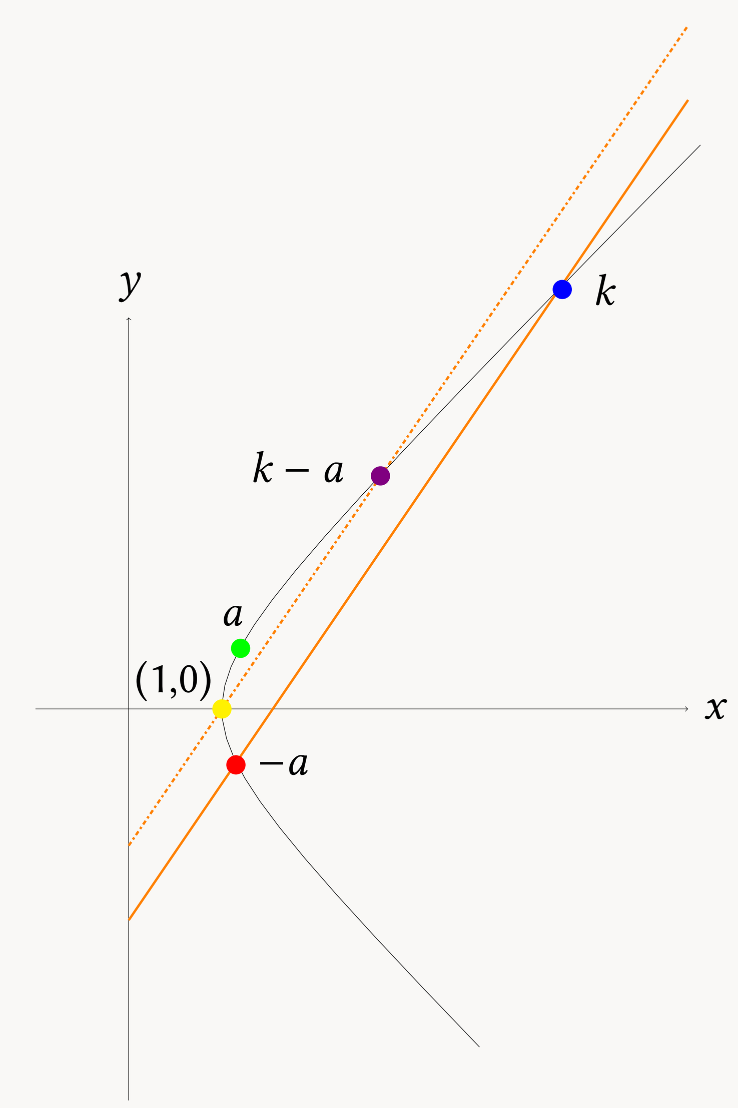


$C(\mathbb{Z})$ Points

The integer points of $C(Z)$, which are the points with integer coefficients, form an interesting subgroup of C. When $d > 0$, there is a group isomorphism,

$$C(\mathbb{Z}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

with the right branch of C isomorphic to $\mathbb{Z}$. The proof for the right branch is derived from a delightfully geometric contradiction.
Proof:
Let (a) be the least positive integer point on C.
Let (k) be the least positive integer point which is not a $\mathbb{Z}$-multiple of (a) on C
Consider (k) - (a):



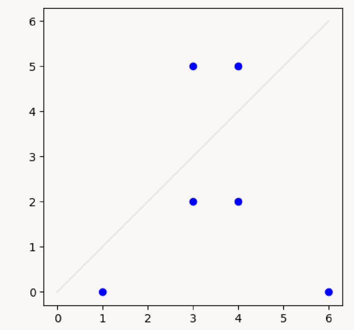
Notice that $(k-a)$ is less than (k) and so by assumption is a $\mathbb{Z}$-multiple of (a).
Thus $(k-a)$ = m(a) for some m$\in \mathbb{Z}$.
Thus (k) = [m+1](a) which is a contradiction. $\rightarrow\leftarrow$
Thus every integer point on the right branch is a $\mathbb{Z}$-multiple of (a). In other words, the right hand branch of our hyperbola is isomorphic to $\mathbb{Z}$. $\square$

$\mathbb{F}_p$ Points

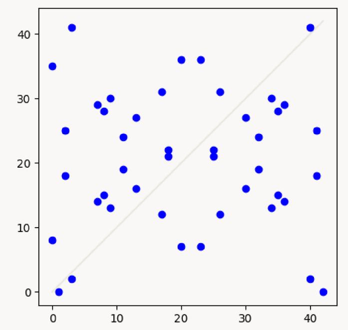
When we interpret the coorinates of $C(\mathbb{Z})$ modulo p, we find a subset of the points $C(\mathbb{F}_p)$, the $\mathbb{F}_p$ points. An understanding of $C(\mathbb{F}_p)$ is crucial to implementing effective cryptography. There is a group isomorphism,

$$C(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z}$$

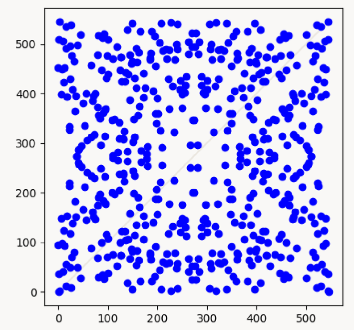
with $m = p$ - $(\frac{d}{p})$. Here are some examples of $C(\mathbb{F}_p)$ for a few primes p, with $C: x^2 - 2y^2 = 1$. Notice how quickly the complexity grows.



$C(\mathbb{F}_7)$



$C(\mathbb{F}_{43})$



$C(\mathbb{F}_{547})$

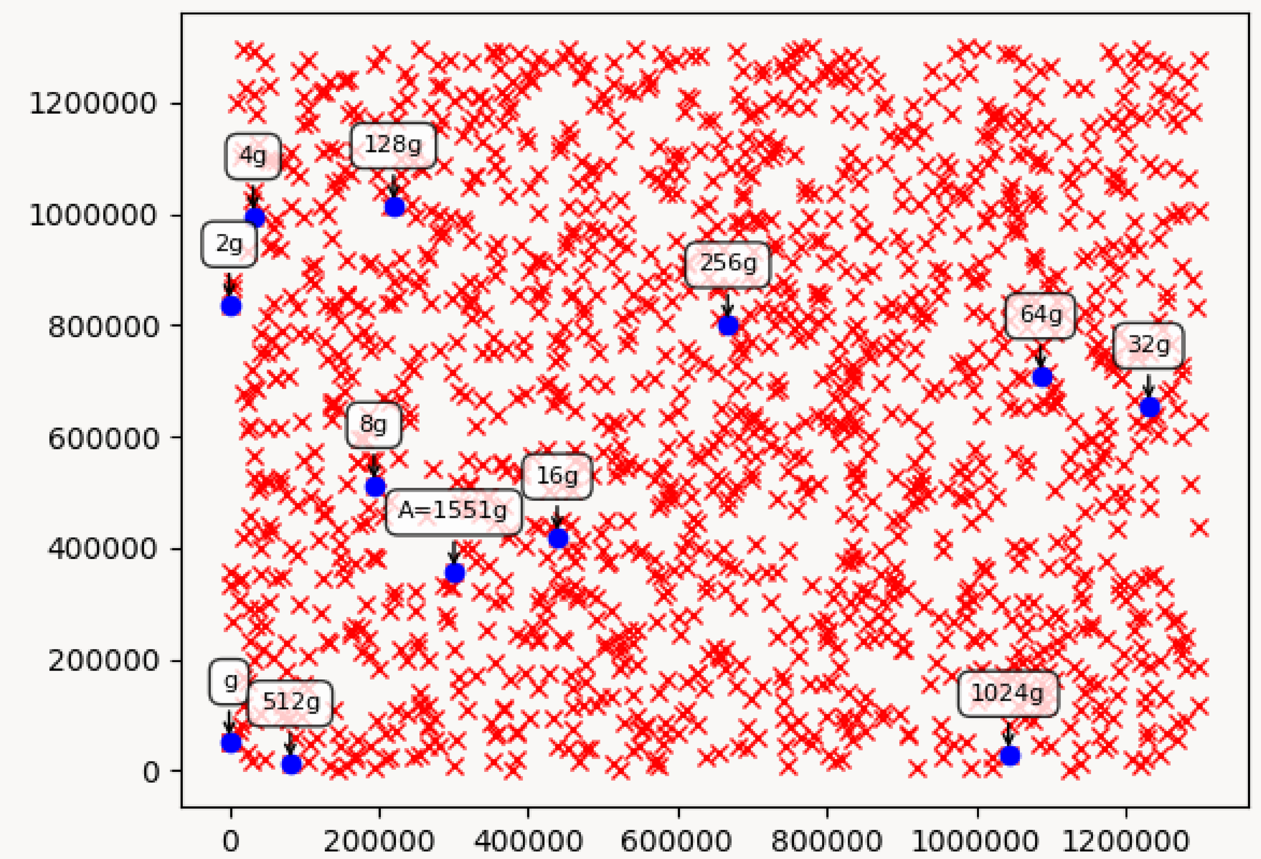
Cryptography Overview

The complexity of the groups determined by curves over finite fields makes them ideally suited for key exchanges, which allow two parties to securely share a private key. The key is used to securely encrypt and share data. In the table below, Alice and Bob are trying to agree on a key, which is a number, without telling Eve, the eavesdropper.

Alice	Eve	Bob
α	$y^2 = x^3 + ax + b$	β
$\alpha\beta$g	g = (a,b)	$\beta\alpha$g
	$\mathbb{F}_p$	
	αg	
	βg	

The items below Eve are public knowledge: Curve specification, finite field choice and a generating point, g. Alice and Bob will choose secret numbers α and β respectively. Using their secret number, they then compute and publicly share αg and βg. Alice and Bob can then easily compute $\alpha\beta$g, whereas Eve cannot as she does not know α or β. The problem of finding α, given that you only know αg and g, is called the discrete log problem.

To find $\alpha\beta g$ Eve needs to know α or β. Suppose Alice chooses $\alpha = 1551$. The plot below illustrates the intermediate points needed to compute $1551g$. The blue circles represent the points which must be computed to find $A = \alpha g$, given that you know $\alpha = 1551$. The red crosses represent the points which must be calculated in order to find α, given that you only know αg and g. The disparity between the two is what makes this key exchange so effective



The above example is using the conic $C: x^2 - 2y^2 = 1$ over $\mathbb{F}_{1299709}$ with generator $g = (8, 52374)$. This formulation of the discrete log problem is very difficult to solve without the secret information. In practice, an elliptic curve would be used rather than a conic, with much larger and more carefully chosen parameters, for increased security.

Further Questions and Related Topics

Lenstra's Algorithm and Pollard's $p-1$ Algorithm
The algebra-geometry connection
Can one project a conic onto a cubic?
When is the map $C(\mathbb{Z}) \longrightarrow C(\mathbb{F}_p)$ onto?

Frost Research Fellows Joel E. Pion & Ryan S. Zesch, advised by Dr. Eric Brussel.

We would like to thank The Bill and Linda Frost Fund for granting us the Frost Undergraduate Student Research Award.

California Polytechnic State University of San Luis Obispo. Contact: jpion@calpoly.edu