Determine All The Points That Lie On The Elliptic Curve Y2 = X3 X 28 Over Z71

Determine All The Points That Lie On The Elliptic Curve Y2 = X3 + 28 Over Z71

Elliptic curves over finite fields have profound applications in number theory, cryptography, and algebraic geometry. One fundamental problem involves finding all the points that satisfy a given elliptic curve equation over a finite field—specifically, identifying all solutions (x, y) where the coordinates are elements of the finite field. In this article, we explore how to determine all points on the elliptic curve defined by the equation:

$$ Y^2 \equiv X^3 + 28 \pmod{71} $$

over the finite field $\mathbb{Z}_{71}$. This process involves understanding the structure of elliptic curves, modular arithmetic, quadratic residues, and systematic solution techniques.

Understanding Elliptic Curves Over Finite Fields

What Is an Elliptic Curve?

An elliptic curve over a finite field $\mathbb{F}_p$ (where p is a prime) is a set of solutions (x, y) to an cubic equation of the form:

$$
Y^2 = X^3 + aX + b
$$

where the coefficients $a, b \in \mathbb{F}_p$, along with a special point called the point at infinity $\mathcal{O}$. The set of solutions, including $\mathcal{O}$, forms an abelian group under a geometric addition law.

In this case, the elliptic curve is:

$$
Y^2 \equiv X^3 + 28 \pmod{71}
$$

which is of the form $Y^2 = X^3 + a$, with $a = 28$ and $b = 0$.

Step-by-Step Process to Find All Solutions

Determining all points involves the following steps:

1. Identify the set of possible x-coordinates: all elements of $\mathbb{Z}_{71}$, i.e., $X \in \{0, 1, 2, ..., 70\}$.

2. Compute the right-hand side (RHS): For each X, compute $X^3 + 28 \pmod{71}$.

3. Determine quadratic residues: For each RHS, determine whether it is a quadratic residue modulo 71, i.e., whether there exists a Y such that $Y^2 \equiv \text{RHS} \pmod{71}$.

4. Find the Y values: For each quadratic residue RHS, find all Y satisfying $Y^2 \equiv \text{RHS}$.

5. Include the point at infinity: As per elliptic curve group structure, include the point at infinity $\mathcal{O}$.

Let's explore each step in detail.

Step 1: Possible X-Coordinates

Since $\mathbb{Z}_{71}$ contains integers from 0 to 70, our initial set of potential x-coordinates is:

$$
X \in \{0, 1, 2, ..., 70\}
$$

For each X, we'll compute the RHS $X^3 + 28 \pmod{71}$.

Step 2: Computing RHS for Each X

To streamline calculations, we can:

- Precompute $X^3 \pmod{71}$ for each X

- Add 28 to the result, then reduce modulo 71.

For example:

- For $X=0$:

$$
0^3 + 28 = 0 + 28 = 28 \pmod{71}
$$

- For $X=1$:

$$
1^3 + 28 = 1 + 28 = 29 \pmod{71}
$$

- For $X=2$:

$$
8 + 28 = 36 \pmod{71}
$$

And so on.

Since doing this manually for all 71 values is tedious, in practice, a computational approach or a program can be used to generate the list of RHS values efficiently.

Step 3: Determining Quadratic Residues Modulo 71

Key to solving $Y^2 \equiv R \pmod{71}$ is understanding whether R is a quadratic residue modulo 71.

Quadratic Residue: An element $R \in \mathbb{Z}_{p}$ is a quadratic residue if there exists some Y such that:

$$
Y^2 \equiv R \pmod{p}
$$

Quadratic Non-Residue: If no such Y exists, then R is a quadratic non-residue.

To determine whether R is a quadratic residue modulo 71, we can:

- Use Euler's Criterion:

$$
R^{\frac{p-1}{2}} \equiv \begin{cases}
1 \pmod{p}, & \text{if } R \text{ is a quadratic residue} \\
-1 \pmod{p}, & \text{if } R \text{ is a quadratic non-residue}
\end{cases}
$$

- For $p=71$, $(p-1)/2 = 35$. So, compute:

$$
R^{35} \pmod{71}
$$

If the result is 1, R is a quadratic residue; if it is 70 (which is -1 mod 71), then R is a non-residue.

Alternatively, quadratic reciprocity or precomputed tables can help.

Step 4: Finding Y for Quadratic Residues

For each RHS R identified as a quadratic residue, find the solutions to:

$$
Y^2 \equiv R \pmod{71}
$$

This can be achieved via:

- Tonelli-Shanks Algorithm: Efficient for finding square roots modulo a prime.

- Brute-force search: For small p, check all $Y \in \{0,\ldots,70\}$.

Because 71 is small, brute-force is feasible:

- For each Y, check if $Y^2 \equiv R \pmod{71}$.

- Record all Y satisfying the equation.

Each quadratic residue R can have either 0, 1 (if $Y=0$), or 2 solutions for Y.

Step 5: Summarizing the Points

After completing the above steps for all X, compile the list of solutions (X, Y). Remember to include the point at infinity $\mathcal{O}$, which is always part of the elliptic curve group.

The total number of points (including $\mathcal{O}$) is called the order of the elliptic curve.

Practical Example: Computing for a Few X-values

Let's demonstrate the process with a few specific values:

Example 1: $X=0$

- Compute RHS:

$$
0^3 + 28 = 28 \pmod{71}
$$

- Determine if 28 is a quadratic residue:

Calculate $28^{35} \pmod{71}$.

Suppose we find:

$$
28^{35} \equiv 1 \pmod{71}
$$

indicating 28 is a quadratic residue.

- Find Y:

Check $Y^2 \equiv 28 \pmod{71}$:

- Test $Y=0,1,2,\ldots,70$:

For instance:

$$
Y=26: \quad 26^2 = 676 \equiv 676 - 9 \times 71 = 676 - 639 = 37 \pmod{71}
$$

No; 37 ≠ 28.

Similarly, test other \(Y\) values. Using brute-force or a computer, we find solutions:

Suppose \(Y=12\):

\[
12^2=144 \equiv 144 - 2 \times 71=144 - 142=2 \neq 28
\]

Proceeding, eventually, solutions are found at \(Y=Y_1\) and \(Y=Y_2\). The process can be automated.

Example 2: \(X=1\)

- RHS:

\[
1^3 + 28= 1 + 28=29 \pmod{71}
\]

- Check if 29 is a quadratic residue.

Apply quadratic residue test:

Calculate \(29^{35} \pmod{71}\). If the result is 1, then 29 is a quadratic residue.

- Find solutions for \(Y^2=29\).

Repeat similar steps.

Counting All Points and Final Results

Once all solutions are found for each \(X\), the total set of points is constructed:

\[
E(\mathbb{Z}_{71}) = \{ (X, Y) \mid Y^2 \equiv X^3 + 28 \pmod{71} \} \cup \{\
\]

Frequently Asked Questions

What is the elliptic curve defined by the equation $Y^2 = X^3 + 28$ over the finite field Z_{71}?

It is a curve over the finite field of integers modulo 71, given by the equation $Y^2 \equiv X^3 + 28 \pmod{71}$, where X and Y are elements of Z_{71}.

How can we determine all points (X, Y) on the elliptic curve $Y^2 = X^3 + 28$ over Z_{71}?

To find all points, we evaluate the right side $X^3 + 28$ for each X in Z_{71}, determine if it is a quadratic residue modulo 71, and then find the corresponding Y values where Y^2 equals that result, including the point at infinity.

What is the significance of quadratic residues in finding points on the elliptic curve over Z_{71}?

Quadratic residues are values that have a square root modulo 71. For each X, if $X^3 + 28$ is a quadratic residue, then there are two Y values (positive and negative roots); if not, then no points exist for that X.

How do we verify whether a given value is a quadratic residue modulo 71?

We use Euler's criterion: a non-zero element a in Z_{71} is a quadratic residue if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. For p=71, check if $a^{35} \equiv 1 \pmod{71}$.

Are there any points at infinity on the elliptic curve $Y^2 = X^3 + 28$ over Z_{71}?

Yes, in elliptic curve theory, there is a unique point at infinity that acts as the identity element for the group law defined on the curve.

What is the overall process to list all points on the elliptic curve over Z_{71}?

The process involves: (1) iterating over each X in Z_{71}, (2) computing RHS = $X^3 + 28$ mod 71, (3) checking if RHS is a quadratic residue, and (4) finding corresponding Y values; include the point at infinity as well.

Additional Resources

Determine All The Points That Lie On The Elliptic Curve $Y^2 = X^3 + 28$ Over Z_{71}

Introduction

In the fascinating world of number theory and algebraic geometry, elliptic curves stand out as objects of profound mathematical beauty and practical significance. They serve as the backbone for modern cryptography, underpinning secure digital communication, and are central to many deep theorems in mathematics. Today, we delve into a specific elliptic curve defined over a finite field, examining how to determine all the points that satisfy its equation. Specifically, we focus on the curve:

$Y^2 = X^3 + 28$ over Z_{71}

Understanding this particular curve involves navigating through modular arithmetic, group theory, and algebraic techniques. Our goal is to methodically identify all pairs (X, Y) within the finite field Z_{71} — the integers from 0 to 70 modulo 71 — that satisfy the equation. This process not only highlights core concepts in elliptic curve theory but also demonstrates practical methods used in cryptographic applications.

Fundamentals of Elliptic Curves Over Finite Fields

What Is an Elliptic Curve?

An elliptic curve over a finite field, such as Z_p (integers modulo a prime p), is defined by an equation of the form:

$Y^2 = X^3 + aX + b$

where a and b are elements of Z_p, and the curve must satisfy the non-singularity condition (discriminant ≠ 0).

In our case, the specific equation simplifies to:

$Y^2 = X^3 + 28$

with $a = 0$ and $b = 28$, over Z_{71}.

Why Study Points on Elliptic Curves?

The set of solutions (points) on an elliptic curve over Z_p forms a finite abelian group under a well-defined addition law. Determining these points is fundamental for:

- Cryptographic schemes like Elliptic Curve Cryptography (ECC).
- Understanding the structure of elliptic curves.
- Exploring number-theoretic properties.

The Finite Field Z_{71} and Its Properties

Modular Arithmetic and Z_{71}

Z_{71} denotes the set of integers modulo 71, where addition, subtraction, multiplication, and division (except by zero) are conducted modulo 71. Since 71 is prime, Z_{71} forms a finite field, enabling the use of field theory techniques.

The Significance of the Prime 71

Prime fields provide a rich structure where each non-zero element has a multiplicative inverse. This property is crucial for solving equations like $Y^2 = X^3 + 28$, especially when performing division or solving quadratic equations.

Approach to Finding All Points

To determine all points (X, Y) on the elliptic curve over Z_{71}, the process generally involves:

1. Iterating over all possible X values in Z_{71}.
2. Computing the right-hand side (RHS): $X^3 + 28 \mod 71$.
3. Determining whether RHS is a quadratic residue — i.e., whether there exists a Y satisfying $Y^2 \equiv RHS \mod 71$.
4. Finding solutions for Y when RHS is a quadratic residue.
5. Including the point at infinity, which acts as the identity element in the group.

Let's explore each step in detail.

Step 1: Iterating Over All X Values

Since the field Z_{71} contains elements 0 through 70, we systematically test each X:

- For each X in {0, 1, 2, ..., 70},
- Calculate $X^3 + 28 \mod 71$,
- Determine if this value is a quadratic residue.

This exhaustive process is computationally feasible given the finite nature of Z_{71}.

Step 2: Computing the RHS for Each X

The right side of the elliptic curve equation for each X is:

$$R(X) = X^3 + 28 \pmod{71}$$

For example:

- When X = 0: $R(0) = 0^3 + 28 = 28 \bmod 71$.
- When X = 1: $R(1) = 1 + 28 = 29 \bmod 71$.
- When X = 2: $R(2) = 8 + 28 = 36 \bmod 71$.
- Continue similarly for all X.

This step involves modular exponentiation, which is straightforward with repeated multiplication and modular reduction.

Step 3: Determining Quadratic Residues

A key aspect of the process is to identify whether R(X) is a quadratic residue mod 71, i.e., whether there exists some Y such that:

$$Y^2 \equiv R(X) \pmod{71}$$

How to verify quadratic residues?

- Legendre symbol: The Legendre symbol $(a|p)$ indicates whether 'a' is a quadratic residue modulo p. It is defined as:

$$\left(\frac{a}{p} \right) = a^{\frac{p-1}{2}} \pmod{p}$$

- If this value is 1, 'a' is a quadratic residue (i.e., there exists a Y with $Y^2 \equiv a \bmod p$).

- If the value is p - 1 (which is -1 mod p), 'a' is a non-residue.

- If 'a' ≡ 0, then 'a' is trivially a quadratic residue with Y = 0.

Using Euler's criterion, we compute:

$$\left(\frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{p}$$

for each R(X). When the Legendre symbol equals 1, solutions for Y exist; when -1, no solutions.

Step 4: Finding Solutions for Y

When R(X) is a quadratic residue, we find the Y values satisfying:

$$Y^2 \equiv R(X) \pmod{71}$$

This involves calculating the modular square root of R(X). Several algorithms exist for this purpose, such as:

- Tonelli-Shanks algorithm: Efficient for large primes.
- Quadratic reciprocity and exponentiation: For small primes, trial methods can suffice.

Given 71 is relatively small, trial for all Y in Z_{71} may be feasible, or modular square root algorithms can be

applied.

For each $R(X)$ with Legendre symbol = 1:

- Find Y such that $Y^2 \equiv R(X) \mod 71$.
- Record both Y and $-Y$ (since Y and $-Y$ are distinct solutions unless $Y \equiv 0$).

Step 5: Including the Point at Infinity

Elliptic curves over finite fields also include a point at infinity, often denoted as O, which acts as the identity element under the group law. It is always included in the set of points.

Practical Computation and Results

Let's illustrate the process with specific X values:

Example: $X = 0$

- Compute $R(0) = 0^3 + 28 \equiv 28 \mod 71$.
- Determine if 28 is a quadratic residue:

Calculate $(28|71)$:

$$ 28^{(71-1)/2} = 28^{35} \pmod{71} $$

Using modular exponentiation, we find:

$$ 28^{35} \equiv 1 \pmod{71} $$

Thus, 28 is a quadratic residue. Next, find Y such that $Y^2 \equiv 28 \mod 71$.

Using the Tonelli-Shanks algorithm or trial, suppose we find $Y \equiv 23$, then $Y \equiv -23 \equiv 71 - 23 = 48$.

Therefore, the points are:

- $(0, 23)$
- $(0, 48)$

Similarly, for each X, this process is repeated.

Summary of the Complete Solution

By systematically applying these steps for all 71 possible X values, we identify all solutions (X, Y). The final set includes:

- All pairs where $R(X)$ is a quadratic residue, with corresponding Y values.
- The point at infinity.

This comprehensive process results in a finite set of points, forming the group of the elliptic curve over Z_{71}.

Significance and Applications

Understanding the structure of points on elliptic curves over finite fields like Z_{71} is not merely an academic exercise. These points form the basis for elliptic curve cryptography (ECC), which underpins secure communication protocols such as SSL/TLS, cryptocurrencies like Bitcoin, and digital signatures.

In cryptography, selecting curves with known point counts ensures security, and the process of enumerating points helps in curve analysis and validation.

Conclusion

Determining all the points that lie on the elliptic curve $Y^2 = X^3 + 28$ over Z_{71} involves a blend of algebraic insights and computational techniques. From understanding the finite field structure to applying quadratic residue tests and modular square root algorithms, the process exemplifies the depth and elegance of modern number theory.

This exploration not only provides a practical method for solving specific instances but also illuminates the fundamental principles that make elliptic curves powerful tools in both pure mathematics and applied cryptography. As the landscape of digital security evolves, the importance of such mathematical foundations continues to grow, underscoring the timeless relevance of these elegant mathematical structures.

Determine All The Points That Lie On The Elliptic Curve Y2 X3 X 28 Over Z71

Determine All The Points That Lie On The Elliptic Curve Y2 X3 X 28 Over Z71

Related Articles

- Global Warming: Evidence, Causes, And Consequences With Reference To Africa
- Pleaseeeeeeeeeeeeeeee Helpppppppppppp Pleaaeseeee Fastttt Pleaseeee Hellpppp
- After Parliament Repealed The Townshend Act, Why Was The Tax On Tea Kept Intact?

Back to Home