Elliptic Curves on Finite Fields

Kumar Harsha, Anupam Saikia

***Abstract*—This paper explores the algebraic properties of elliptic curves over finite fields. Elliptic curves are being widely used in modern cryptographic techniques. The rational points on an elliptic curve obey group theoretic laws. As such, computing the order of these groups forms the basis of more complex computations. The first section of this paper deals with the basic group properties of rational points on elliptic curves and an introduction to projective geometry. In the second, algorithms for computing multiplication maps are explained. The later section has point counting algorithms followed by code snippets in SAGE. Also included, is a section on some unsolved problems in the domain.**

***Index Terms*—Elliptic curves, SAGE.**

I. ELLIPTIC CURVES

This section presents the basic theory of elliptic curves. Let

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

(Equation 1)

be the equation for a general cubic. The cubic is *rational* if the coefficients of its equation are rational numbers.

One of the basic theorems in the geometry of plane curves is the Bezout's theorem, stated below.

Bezout's Theorem: *A curve of degree m and a curve of degree n meet in mn points.*

In the case of cubic curves, we can state the following.

Theorem: Let C, C_1 and C_2 be three cubic curves. Suppose C goes through eight of the nine intersection points of C_1 and C_2, then C goes through the ninth intersection point.

A. Group law on a cubic

In order to define group operations on a cubic curve, we need a rational point on the cubic to begin with, the *zero element*. Let the zero element be $\mathcal{O}$. It is worth mentioning that the choice of $\mathcal{O}$ is not special. We may easily choose a different point to be the zero element of the group without changing the group structure.

If we have any two points on a rational cubic, say P and Q, and the zero element $\mathcal{O}$ exists as defined above, we may state the rule for the group operation as follows:

Definition: To add P and Q, take the third intersection point P $*$ Q, join it to $\mathcal{O}$, and then take the third intersection point to be P + Q. Thus, P + Q = $\mathcal{O}$ $*$ (P $*$ Q).

The commutatively, associatively and existence of negatives, with respect to the group operation defined, can be easily proved geometrically.

Revised Version Manuscript Received on April 11, 2016.

Kumar Harsha, Department of Mathematics, Indian Institute of Technology Guwahati, Guwahati, India.

Dr. Anupam Saikia, Department of Mathematics, Indian Institute of Technology Guwahati, Guwahati, India.

Mordell's Theorem: Let C be a nonsingular cubic curve with rational coefficients. Then the group Γ of rational points on C is finitely generated.

In light of the group operation defined earlier using the chord and tangent laws, we can outline a way to get all rational points starting from an initial set of rational points. We draw lines through the points in the set to get new points and then draw lines again through the new points obtained to get more points, and so on.

B. Projective geometry

An overview of projective geometry is required to express cubic curves in a normal form, discussed in the following section.

Definition: The projective plane is defined to be a set of triples $[a, b, c]$, with a, b, c not all zero, such that two triples $[a, b, c]$ and $[a', b', c']$ are considered to be the same point if there is a non-zero t such that $a = ta', b = tb', c = tc'$. The numbers a, b, c are called homogeneous coordinates for the point $[a, b, c]$. The projective plane is denoted by $\mathbb{P}^2$.

The projective plane can also be defined in purely geometric terms.

Definition: Let the *Euclidean (or affine) plane* be denoted by $\mathbb{A}^2 = \{(x, y) : x \text{ and } y \text{ any numbers}\}$. Then we define the projective plane to be

$$\mathbb{P}^2 = \mathbb{A}^2 \bigcup \{set of directions in \mathbb{A}^2\}$$

(Equation 2)

where direction is a non-oriented notion.

From an aesthetic and a practical viewpoint, a direction is an equivalence class of parallel lines and the points corresponding to directions are those points in $\mathbb{P}^2$ that are not in $\mathbb{A}^2$. These points are often called points at infinity and maybe viewed as the common intersection point of the parallel lines it is associated to. These points are good candidates for the zero element, as will be seen in the next section.

An algebraic curve in the affine plane $\mathbb{A}^2$ is defined to be the set of solutions to a polynomial equation in two variables $f(x, y) = 0$. For curves in the projective plane, we will need to use polynomials in three variables. We have seen that $[a, b, c]$ and $[ta, tb, tc]$ are the same point in a projective plane. It is worthwhile, then, to look only at polynomials $F(X, Y, Z)$ for which $F(a, b, c) = 0$ implies that $F(ta, tb, tc) = 0$ for all t.

Definition: A polynomial $F(X, Y, Z)$ is called a *homogeneous polynomial* of degree d if it satisfies the identity $F(tX, tY, tZ) = t^d F(X, Y, Z)$.

In other words, we may say that F is a linear combination of monomials of the form $X^i Y^j Z^k$ where $i + j + k = d$.

Definition: A projective curve C in the projective plane $\mathbb{P}^2$ is defined as the set of solutions to a polynomial equation

$$C : F(X, Y, Z) = 0$$

(Equation 3)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

where F is a non-constant homogeneous polynomial. The degree of the curve C is the degree of the polynomial F.

C. *Weierstrass Normal Form*

We think of the cubic curve defined in *Equation 1* as being in the projective plane. By a suitable projective transformation $(x = X/Z, y = Y/Z)$, we can write the cubic equation in the form of $y^2 = cubic\ in\ x$.

Definition: A cubic curve in normal form looks like

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

(Equation 4)

Assuming that the (complex) roots of $f(x)$ are distinct, such a curve is called an *elliptic curve*.

D. *Explicit formulas for the Group Law*

In order to allow easy computation of $P + Q$, we set the zero element $\mathcal{O}$ as the point at infinity. The point $\mathcal{O}$ is counted as a rational point and follows the following conventions:

1. The line at infinity intersects the cubic thrice at the point $\mathcal{O}$.
2. A vertical line intersects the cubic at two points in the xy plane and also at $\mathcal{O}$.
3. All other lines intersect the cubic at three points, including complex points, in the xy plane.

Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_1 * P_2 = (x_3, y_3), P_1 + P_2 = (x_3, -y_3)$, where P_1 and P_2 are known and we need an expression for (x_3, y_3).

The line joining P_1 and P_2 has the equation

$$y = \lambda x + \nu$$

(Equation 5)

where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2\}$. Using *Equation 4* and *Equation 5*, we may write

$$y^2 = (\lambda x - \nu^2) = x^3 + ax^2 + bx + c$$

(Equation 6)

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2)$$

(Equation 7)

The line cuts the curve at three points. Let x_1, x_2, x_3 be the x-coordinates of these points. Then,

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3)$$

(Equation 8)

Equating the coefficients of x^2 on either side of the above equation, we get

$$x_3 = \lambda^2 - a - x_1 - x_2, y_3 = \lambda x_3 + \nu$$

(Equation 9)

II. GROUP PROPERTIES OF POINTS

In this section, we look at some important theorems and lemmas describing points on elliptic curves that have finite order.

A. *Points of order Two and Three*

Let C be the non-singular cubic curve

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c$$

(Equation 10)

This means that $f(x)$ and $f'(x)$ have no common roots.

1. A point $P \neq \mathcal{O}$ on the curve has order two if and only if $y = 0$.
2. The curve C has only four points of order dividing 2. The points form a group that is a product of two cyclic groups of order two.
3. A point $P \neq \mathcal{O}$ on C has order three if and only if x is a root of the polynomial

$$\psi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$$

(Equation 11)

4. C has exactly nine points of order dividing 3. These points form a group which is the product of two cyclic groups of order three.

The prrof of these properties is simple and is elaborated in Reference [1].

B. *Points of finite order*

The Nagell-Lutz theorem is an important result on points of finite order. It helps in computing such points efficiently in a finite number of steps. Before stating the theorem, the determinant of a cubic curve needs to be defined.

Definition: The *discriminant* of $f(x)$ is the quantity

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

(Equation 12)

where the curve C is expressed in its normal form and the coefficients hold their meaning.

Nagell-Lutz Theorem: Let $y^2 = f(x) = x^3 + ax^2 + bx + c$ be a non-singular cubic curve with integer coefficients a, b, c; and let D be the discriminant of the cubic polynomial $f(x)$ as in ((Equation 12).

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers; and either $y = 0$, in which case P has order two, or else y divides D.

A stronger form of the Nagell-Lutz theorem says that if $P = (x, y)$ is a rational point of finite order with $y \neq 0$, then y^2 divides D.

To compute subgroups using this theorem, we solve the cubic equation for $y = 0$ and each square divisor y^2 of D. The major disadvantages of this approach are

1. It requires factorization of D, which may be large and difficult to factor.
2. For every square divisor, a cubic equation has to be solved which is computationally slow.

An interesting thing to be noted here is that the Nagell-Lutz theorem is not an "if and only if" statement. This is important because the algorithm described above computes a set of points which includes all points of finite order. The Nagell-Lutz theorem cannot, however, be used to prove that a particular point has finite order. A point P can be proved to have finite order if we can find an integer $n \geq 1$ such that $nP = \mathcal{O}$.

The theorem, on the other hand, can often be used to prove that a point has infinite order. We compute $P, 2P, \ldots$ until we have a multiple nP that is not an integer. A faster method would be to compute only the x coordinates of $P, 2P, 4P, \ldots$ until some x has a non-integral value.

Darrin Doud has given a better procedure to compute subgroups of rational points on elliptic curves in his 1997 paper [3]. At this point it suffies to mention that the procedure depends on an analytic parameterization of the reduced normal form, $y\text{^}2 = x\text{^}3 + Ax + B$, by the Weierstrass $\wp$ function. We get a map

given explicitly by $z \mapsto (\wp(z), \wp'(z))$, which is in fact an isomorphism of groups.

Also noteworthy in the present context is Mazur's theorem.

Mazur's Theorem: Let C be a non-singular rational cubic curve, and suppose that $C(\mathbb{Q})$ contains a point of finite order m. Then either $1 \leq m \leq 10$ or $m = 12$ [1].

More precisely, the set of all points of finite order in $C(\mathbb{Q})$ forms a subgroup which has one of the following two forms:

1. A cyclic group of order N with $1 \leq N \leq 10$ or $N = 12$.
2. The product of a cyclic group of order two and a cyclic group of order $2N$ with $1 \leq N \leq 4$.

III. ISOGENIES

Elliptic curves have both an algebraic structure as an abelian group and a geometric structure as an algebraic curve. Homomorphism of abelian varieties are called isogenies, and they respect both the agebraic and geometric structures.

Definition: Let E_1 and E_2 be elliptic curves over a field k. An *isogeny* is a rational map $\alpha : E_1 \to E_2$ that induces a group homomorphism from $E_1(\bar{k})$ to $E_2(\bar{k})$ [5].

Definition: Let C_1 and C_2 be projective curves over k. A $rational\ map \phi : C_1 \to C_2$ has the form $(\phi_x : \phi_y : \phi_z)$ with $\phi_x, \phi_y, \phi_z \in \bar{k}(C_1)$, such that for every point $P \in C_1(\bar{k})$ where ϕ_x, ϕ_y, ϕ_z are defined, the point $(\phi_x(P) : \phi_y(P) : \phi_z(P))$ lies in $C_2(\bar{k})$ [5].

Definition:A rational map is *defined* (or *regular*) at a point $P \in C\_1(\bar{k})$ if there exists a function $g \in \bar{k}(C_1)$ such that $g\phi_x, g\phi_y, g\phi_z$ are all defined at P and at least one is nonzero at P. The map is denoted by $g\phi$ [5].

Definition:A rational map that is defined everywhere is called a *morphism* [5].

In the case of elliptic curves, every rational map is also a morphism. More generally, we have the following.

Theorem: If C_1 is a smooth projective curve then every rational map from C_1 to a projective curve C_2 is a morphism [1].

Definition: An *isomorphism* of elliptic curves is an invertible isogeny.

The special case of an isogeny $\alpha : E \to E$ from an elliptic curve to itself is called an endomorphism.

Two important examples of isogenies are the multiplication-by-n map and the Frobenius endomorphism.

A. *The multiplication-by-2 map*

Let E/k be the elliptic curve defined by $y^2 = x^3 + Ax + B$ and let α be the map that sends P to $2P$. The formulae for doubling an affine point are

$$\alpha_x(x,y) = \frac{9x^4 + 6Ax^2 + A^2x - 8xy^2}{4y^2}$$

$$\alpha_y(x,y) = \frac{(3x^2 + A)12xy^2 - (3x^2 + A)^3 - 8y^4}{8y^3}$$

(Equation 13)

The functions $\alpha_x(x,y)$ and $\alpha_y(x,y)$ are defined at all affine points $P = (x,y)$ except those with $y = 0$. When we switch to projective coordinates, we have

$$\alpha_x(x,y,z) = \frac{9x^4 + 6Ax^2z^2 + A^2xz^3 - 8xy^2z}{4y^2z^2}$$

$$\alpha_y(x,y,z) = \frac{(3x^2 + Az^2)12xy^2z - (3x^2 + Az^2)^3 - 8y^4z^2}{8y^3z^3}$$

$$\alpha_z(x,y,z) = 1$$

(Equation 14)

The points where α_x and α_y are undefined are the 2-torsion points of $E(\bar{k})$; three affine points $(x_i : 0 : 1)$ corresponding to the three distinct roots x_i of the cubic $x^3 + Ax + B$ and the point at infinity $(0 : 1 : 0)$.

B. *The Frobenius endomorphism*

Let $\mathbb{F}_p$ be a finite field of prime order p. The *Frobenius automorphism* $\pi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ is the map $\pi(x) = x^p$. If $f(x_1, \ldots, x_k)$ is any rational function with coefficients in $\mathbb{F}_p$, then

$$f(x_1, \ldots, x_k)^p = f(x_1^p, \ldots, x_k^p)$$

(Equation 15)

Definition: Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The Frobenius endomorphism of E sends the point (x,y,z) to (x^q, y^q, z^q).

If E is defined by $y^2 = x^3 + Ax + B$, then for any point $P = (x_0, y_0, z_0) \in E(\overline{\mathbb{F}}_q)$ we have

$$0 = (y_0^2 z_0 - x_0^3 - Ax_0 z_0^2 - Bz_0^3)^q = (y_0^q)^2 (z_0^q) - (x_0^q)^3 - Ax_0^q (z_0^q)^2 - B(z_0^q)^3$$

(Equation 16)

thus $\pi(P) \in E(\overline{\mathbb{F}}_p)$.

Even though Frobenius endomorphism is bijective on $\overline{\mathbb{F}}_q$, it is *not an isomorphism*; there is no inverse map.

C. *A standard form for isogenies*

Lemma: Let E_1 and E_2 be elliptic curves over k in short Weirstrass form, and let α be a nonzero isogeny from E_1 to E_2. Then α can be defined by an affine map of the form

$$\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)} y\right)$$

(Equation 17)

where $u, v, s, t \in \bar{k}[x]$ are polynomials in x with $u \perp v$ and $s \perp t$.

The notation $f \perp g$ means that f and g are relatively prime which is equivalent to saying that they have no common roots.

Lemma: Let $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)} y\right)$ be an isogeny from E_1 to E_2 in standard form. Then $v(x)$ and $t(x)$ have the same set of roots. Moreover, v^3 divides t^2.

We will see later that these properties are crucial for computing multiplication-by-n maps using division polynomials.

Definition: Let $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)} y\right)$ be an isogeny from E_1 toE_2 in standard form. The *degree* of α is $deg\ \alpha = \max\{ deg\ u, deg\ v \}$.

IV. COMPUTING *n*P

Besides the projective coordinates, we can also represent elliptic curves in *Jacobian coordinates*. They give a speed benefit when the cost for field inversions are higher than field multiplications. Let $(x:y:z)$ represent the affine point $(\frac{x}{z^2},\frac{y}{z^3})$. The elliptic curve $y^2 = x^3 + Ax + B$ becomes

$$y^2 = x^3 + Axz^4 + Bz^6$$

(Equation 18)

The point at infinity then has the coordinates $\infty = (1:1:0)$.

A. *The group law in Jacobian coordinates*

Let $P_i = (x_i: y_i: z_i), i = 1,2$ be points on the elliptic curve *Equation 21*. Then

$$(x_1: y_1: z_1) + (x_2: y_2: z_2) = (x_3: y_3: z_3)$$

(Equation 19)

where x_3, y_3, z_3 are computed as follows:

I. When $P_1 \neq \pm P_2$,

$$r = x_1z_2^2, s = x_2z_1^2, t = y_1z_2^2$$
$$u = y_2z_1^3, v = s - r, w = u - t$$

(Equation 20)

$$x_3 = -v^3 - 2rv^2 + w^2$$

(Equation 21)

$$y_3 = -tv^3 + (rv^2 - x_3)w$$

(Equation 22)

$$z_3 = vz_1z_2$$

(Equation 23)

II. When $P_1 = P_2$,

$$v = 4x_1y_1^2, w = 3x_1^2 + Az_1^4$$

(Equation 24)

$$x_3 = -2v + w^2$$

(Equation 25)

$$y_3 = -8y_1^4 + (v - x_3)w$$

(Equation 26)

$$z_3 = 2y_1z_1$$

(Equation 27)

The elliptic curves in NIST's list of curves over $\mathbb{F}_q$ have $A = -3$ because it decreases the number of computations involved. When $A = -3$, we have $w = 3(x_1^2 - z_1^4) = 3(x_1 + z_1^2)(x_1 - z_1^2)$.

B. *Division polynomials*

Division polynomials help describe the map on an elliptic curve given by multiplication by an integer. This is an endomorphism and can be described by rational functions. The *division polynomials* $\psi_m \in \mathbb{Z}[x, y, A, B]$ are defined as [2]:

$$\psi_0 = 0$$

(Equation 28)

$$\psi_1 = 1$$

(Equation 29)

$$\psi_2 = 2y$$

(Equation 30)

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

(Equation 31)

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

(Equation 32)

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 form \geq 2$$

(Equation 33)

$$\psi_{2m} = \frac{1}{2y}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) form \geq 3$$

(Equation 34)

We now define ϕ_n and ω_n via

$$\phi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1}$$

(Equation 35)

$$\omega_n = \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$$

(Equation 36)

Lemma: For every integer n,

ψ_n lies in $\begin{cases} \mathbb{Z}[x, A, B], \text{n odd} \\ 2y\mathbb{Z}[x, A, B], \text{n even} \end{cases}$

ϕ_n lies in $\mathbb{Z}[x, A, B]$ $for\ all\ n$,

ω_n lies in $\begin{cases} \mathbb{Z}[x, A, B], \text{n even} \\ y\mathbb{Z}[x, A, B], \text{n odd} \end{cases}$

We now have sufficient tools to define the multiplication-by-n map.

Theorem: Let E/k be an elliptic curve defined by the equation $y^2 = x^3 + Ax + B$ and let n be a nonzero integer. The rational map

$$[n](x, y) = (\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)})$$

(Equation 37)

sends each point $P \in E(\bar{k})$ to nP [2].

V. POINT COUNTING

In this section are outlined algorithms for computing order of points and groups.

Definition: Let G be an additive abelian group. The *n-torsion subgroup* $G[n]$ is the kernel of the multiplication-by-n homomorphism $[n]$, the set $\{g \in G : ng = 0\}$.

Theorem: Let E be an elliptic curve defined over a field of characteristic p. Then

$$E[n] \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} \bigoplus \mathbb{Z}/n\mathbb{Z}\ if p = 0\ or\ p \nmid n \\ \mathbb{Z}/n\mathbb{Z}\ or \{0\} if p > 0\ or\ is\ a\ power\ of\ p \end{cases}$$

(Equation 38)

Hasse's Theorem: Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field. Then

$$\#E(\mathbb{F}_q) = q + 1 - t$$

(Equation 39)

where t satisfies $|t| \leq \sqrt{q}$ [5].

The bound specified by the Hasse's theorem is the best possible and proves to be very valuable for computational purposes.

The most naïve approach we can take to count rational points on an elliptic curve is to evaluate the curve equation$y^2 = x^3 + Ax + B$ at every pair of points $(x, y) \in \mathbb{F}_q^2$. The cardinality would then be one more than the total number of solutions; the extra 1 for the point at infinity. The time complexity for this approach is $O(q^2 M(log\ q))$.

The advantage of the Hasse's theorem is that it tells us the interval where the quantity $\#E(\mathbb{F}_q)$ must lie

$$\mathcal{H}(q) = \left[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}\right] = \left[\left(\sqrt{q} - 1\right)^2, \left(\sqrt{q} + 1\right)^2\right]$$

(Equation 40)

which has width $4\sqrt{q}$.

A. Computing the order of a point

We first consider computing the order of a single point $P \in \#E(\mathbb{F}_q)$. Hasse's theorem tells us that $\mathcal{H}(q)$ contains at least one integer M such that $MP = 0$ and such M is a multiple of $|P|$.

Algorithm: Order of a point

1. $M_0 = \left(\sqrt{q} - 1\right)^2$
2. Compute $M_0 P$
3. Generate the sequence of points $(M_0 + 1)P, (M_0 + 2)P, \ldots, MP = 0$
4. Let $m = M$
5. Compute the prime factorization $m = M = p_1^{e_1} \ldots p_w^{e_w}$
6. For each prime p_i, while $p_i \mid m$ and $(m/p_i)P = 0$, replace m by m/p_i
7. Output m

The time complexity for this approach is dominated by the time taken to find a multiple of $|P|$ in $\mathcal{H}(q)$. This involves $O(\sqrt{q})$ operations, leading to a complexity of $O(\sqrt{q} M(log\ q))$.

We can apply this algorithm and find a combination of points such that the least common multiple of their orders has a multiple in $\mathcal{H}(q)$. Then, we may compute the group order.

B. Computing the group order

Definition: For a finite group G, the *exponent* of G, denoted by $\lambda(G)$, is defined by $\lambda(G) = lcm\{\ |\alpha| : \alpha \in G\ \}$.

It is worth noting that $\lambda(G)$ is a divisor of $|G|$ and will be divisible by the order of every element of G. Thus, if we compute the least common multiple of a sufficiently large subset of a finite abelian group G, we will eventually obtain $\lambda(G)$.

Theorem: Let G be a finite abelian group with exponent $\lambda(G)$. Let α, β be uniformly distributed random elements of G. Then

$$Pr[lcm(|\alpha|, |\beta|) = \lambda(G)] > 6/\pi^2$$

(Equation 41)

Reference [5] has a beautiful proof of this. The theorem implies that if we generate random points $P \in E(\mathbb{F}_q)$ and accumulate the least common multiple N of their orders, we should expect to obtain the group exponent $\lambda(E(\mathbb{F}_q))$ in $O(1)$ time. If $\lambda(E(\mathbb{F}_q))$, however, is smaller than $4\sqrt{q}$, then it might have more than one multiples in $\mathcal{H}(q)$. To overcome this problem, we consider the quadratic twist of E.

Definition: An integer q is called a *quadratic residue modulo n* if it is congruent to a perfect square modulo n; i.e., if there exists an integer x such that $x^2 \equiv q\ (mod\ n)$. Otherwise, q is called a *quadratic no residue modulo n*.

Definition: For a quadratic nonresidue $d \in \mathbb{F}_q$, the elliptic curve $\tilde{E}$ defined by $dy^2 = x^3 + Ax + B$ is called the quadratic twist of the elliptic curve E defined by $y^2 = x^3 + Ax + B$.

Quadratic twists are interesting because of the following property

$$\#E(\mathbb{F}_q) + \#\tilde{E}(\mathbb{F}_q) = 2q + 2$$

(Equation 42)

We need to state one more theorem before we design the algorithm to compute group order.

Mestre's Theorem: Let $p > 229$ be a prime, and let $E(\mathbb{F}_p)$ be an elliptic curve with quadratic twist $\tilde{E}(\mathbb{F}_p)$. Then either $\lambda(E(\mathbb{F}_p))$ or $\lambda(\tilde{E}(\mathbb{F}_p))$ has a unique multiple in $\mathcal{H}(p)$.

Mestre's theorem comes of use when the group exponent we are computing is smaller than $4\sqrt{q}$. The Las Vegas algorithm computes the group order $\#E(\mathbb{F}_p)$ using Mestre's theorem, where p is a prime greater than 229.

Algorithm: Las Vegas algorithm to compute group order

1. Compute the quadratic twist $\tilde{E}$ of $\tilde{E}$ using a randomly generated non-residue $d \in \mathbb{F}_p$
2. Let $E_0 = E$ and $E_1 = \tilde{E}$; let $N_0 = N_1 = 1$ and $i = 0$
3. *While* (neither N_0 nor N_1 has a unique multiple in $\mathcal{H}(p)$)
4. Generate a random point $P \in E_i(\mathbb{F}_p)$
5. Find $M \in \mathcal{H}(p)$ such that $MP = 0$
6. Factor M and compute $|P|$
7. Replace N_i by $lcm(N_i, |P|)$ and I by $1 - i$
8. *EndWhile*
9. *If* ($N\_0 \mid M$ and $M \in \mathcal{H}(p)$)
10. Output M
11. *Else*
12. Output $2p + 2 - M$, where $N_1 \mid M$
13. *EndIf*

By the properties of the group exponent discussed earlier, it is certain that the while loop runs in O(1) time. The time complexity for this algorithm is dominated by the time to find M in step 5. We get an expected complexity of $O(\sqrt{p}\, M(log\ p))$.

The process of finding M can be improved using the *baby-steps giant-steps* method. This is a generic group algorithm introduced by Dan Shanks [5]. It searches $\mathcal{H}(q) = [a, b]$ for an integer M such that $MP = 0$. The main idea is to compute multiples of P at intervals, rather than all of them. It works as outlined.

Algorithm: Baby-steps Giant-steps

1. Pick integers r and s such that $rs \geq b - a$
2. Compute the set $S_{baby} = \{0, P, 2P, \ldots, (r-1)P\}$
3. Compute the set $S_{giant} = \{aP, (a + r)P, (a + 2r)P, \ldots, (a + (s-1)r)P\}$
4. *ForEach* giant step $P_{giant} = (a + ir)P \in S_{giant}$
5. Check whether $P_{giant} + P_{baby} = 0$ for some baby step $P_{baby} = jP \in S_{baby}$

6. If so, output $M = a + ri + j$
7. *End For*

VI. OPEN PROBLEMS

In this section, we summarize some unsolved problems in the domain of elliptic curves.

A. Rank of Elliptic curves

Definition: The *rank of an elliptic curve* is the measure of the size of the set of rational points lying on it.

There is no effective algorithm for computing the rank. The elliptic curve with the biggest exactly known rank, 19, is

$$y^2 + xy + y = x^3 - x^2 + 31368015812338065133318565 29220659079282035345x + 30203880269856608733564318842954349862452204168387449355518606256815984 7$$

(Equation 43)

The curve with rank atleast 24 is

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x + 50422499248491067001080179916808272 675944375622291141511 6$$

(Equation 44)

B. The Birch and Swinnerton-Dyer conjecture

The proof of this conjecture is one of Millennium Prize Problems stated by the Clay Mathematics Institute. The conjecture, associated with the names of B.J.Birch and H.P.F. Swinnerton-Dyer, has evolved gradually.

Conjecture: [Birch and Swinnerton-Dyer]

The Taylor expansion of $L(C, s)$ at $s = 1$ has the form

$$L(C, s) = c(s-1)^r + higher\ order\ terms$$

(Equation 45)

with $c \neq 0$ and $r = rank(C(\mathbb{Q}))$ [4].

In particular this conjecture asserts that $L(C, 1) = 0 \Rightarrow C(\mathbb{Q})$ is infinite. $L(C, s)$ stands for the L-series of the cubic curve C and s denotes the genus of the curve. In layman terms, the value of a surface's genus is equal to the number of *holes* it has.

A crude statement summarizing the conjecture is that an elliptic curve has infinitely many rational points if and only if $L(E, s) = 0$ at $s = 0$.

C. Congruent number problem

Definition: A *congruent number* is a positive integer that is the area of a right-angled triangle with rational sides.

The question of determining whether a given integer is a congruent number is the congruent number problem. This problem has not, as of 2012, been successfully resolved. Tunnell's theorem provides a criterion but his result relies on the Birch and Swinnerton-Dyer conjecture, which is still unproven [6].

We shall see how this is related to elliptic curves. Suppose a, b, c are numbers that satisfy the following conditions:

$$a^2 + b^2 = c^2$$
$$\frac{1}{2}ab = n$$

(Equation 46)

We set $x = n(a + c)/b$ and $y = 2n^2(a + c)/b^2$. Some simple calculations lead us to the following:

$$y^2 = x^3 - n^2x.$$

(Equation 47)

We may also express a, b, c in terms of x, y as follows:

$$a = (x^2 - n^2)/y$$
$$b = 2nx/y$$
$$c = (x^2 + n^2)/y$$

(Equation 48)

The correspondence between (a, b, c) and (x, y) is that they are inverses of each other for cases when y is nonzero. We can safely say that a, b, c are rational and positive if and only if x, y are rational and positive.

The congruent number problem then boils down to checking if the curve

$$y^2 = x^3 - n^2x$$

(Equation 49)

has a rational point for $y \neq 0$. In other words, a number n can be said to be congruent if the curve (Equation 49) has positive rank.

ACKNOWLEDGMENT

F. A. Author thanks his mentor for the undergraduate thesis project, who is the second author of this paper, for constant motivation and guidance throughout. The author also thanks his family and friends for their support.

REFERENCES

1. Joseph H. Silverman &John Tate, Rational Points on Elliptic Curves, Springer-Verlag New York, 1992, pp. 15–64.
2. Lawrence C. Washington, Elliptic Curves - Number theory and Cryptography.Chapman and Hall/CRC, 2008, pp. 77-102.
3. Darrin Doud, "A procedure to calculate torsion of Elliptic Curves over.ℚ"Manuscripta Mathematica, November1997.
4. Celine Maistret, "Computations on the Birch and Swinnerton-Dyer conjecture for elliptic curves over pure cubic extensions" [Master's Thesis/Online], Concordia University, Canada, August 2012, Available: https://www2.warwick.ac.uk/fac/sci/maths/people/staff/maistret/maistret_msc_f2012.pdf
5. Andrew Sutherland, 18.783 Elliptic Curves, Spring 2013, Massachusetts Institute of Technology: MIT Open Course Ware.[Online], 2013, Available: http://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2013/index.htm
6. Wikipedia Contributors, Elliptic curve[Online], October 11, 2014, Available: http://en.wikipedia.org/w/index.php?title=Elliptic_curve&oldid=629180339

AUTHORS PROFILE

Kumar Harsha, Undergraduate degree in Mathematics and Computing, Indian Institute of Technology Guwahati, Batch of 2015. Currently working as Product Engineer at Aspiring Minds Assessment Pvt Ltd.

Dr. Anupam Saikia, PhD (University of Cambridge, UK). Currently Professor, Department of Mathematics and Associate Dean of Academic Affairs at Indian Institute of Technology Guwahati.