Some Highlights along a Path to Elliptic Curves

Part 6: Rational Points on Elliptic Curves

Steven J. Wilson, Fall 2016

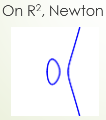
Outline of the Series

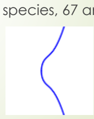
1. The World of Algebraic Curves
2. Conic Sections and Rational Points
3. Projective Geometry and Bezout's Theorem
4. Solving a Cubic Equation
5. Exploring Cubic Curves
6. **Rational Points on Elliptic Curves**

This 6-part series will highlight some of the mathematical topics needed to understand the basics of elliptic curves.

Elliptic Curve Prototypes

- With appropriate transformations, every elliptic curve can be transformed into $y^2 = x^3 + px + q$.
  - Unless the field on which it is graphed has characteristic 2 or 3, in which case the best result may be $y^2 + axy + by = x^3 + cx^2 + dx + e$.
- This is called **Weierstrass Normal Form**.
- On R^2, Newton gives 2 nonsingular species, 67 and 71:

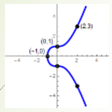




$y^2 = \text{(linear)(linear)(linear)}$ $y^2 = \text{(linear)(irreducible quadratic)}$

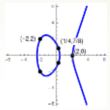
Rational Points (in R^2)

- Elliptic curves may or may not have rational points.



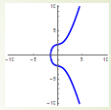
$y^2 = x^3 + 1$

Exactly 5 rational points



$y^2 = x^3 - 5x + 2$

Infinite number of rational points



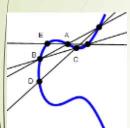
$y^2 = x^3 + x + 5$

No rational points

- If a line intersects an elliptic curve in 3 points, and 2 of them are rational points, then the third is also a rational point.

Combining Points

- **Chord Composition**

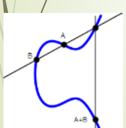


  - Draw line through 2 points,
  - The third point is the composition.
  - But it is not associative.

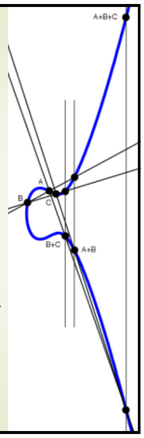
$(A*B)*C = D$

$A*(B*C) = E$

- **Group Addition**

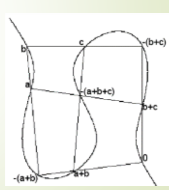


  - Use chord composition to obtain 3rd point.
  - Take its opposite.
  - This is associative.

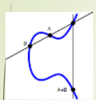


Cayley-Bacharach

- Bezout's Theorem says two cubics intersect in 9 points.
- **Cayley-Bacharach Theorem** (1886): Given the 9 intersection points of 2 cubics, if a third cubic passes through 8 of those points, it will also pass through the ninth point.
- In the figure at the right, think of:
  - First cubic as "horizontal" lines
  - Second cubic as "vertical" lines
  - Third cubic as "curve"
- We can use Cayley-Bacharach to prove associativity of our group addition.

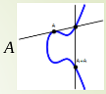


Some Special Cases



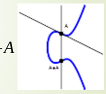
- Doubling a point
  - Use a tangent line to find 3rd point,
  - Then take the opposite.

$A+A$



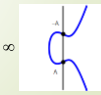
- Doubling an inflection point
  - The third point is itself,
  - Then take the opposite.

$A+A=-A$



- Adding the opposite:
  - The third point is at infinity,
  - Its opposite is at infinity.

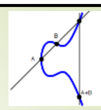
$A+(-A)=\infty$



- The point at infinity is the identity element.

$A+\infty=A$

Abelian Groups



Basic definition:

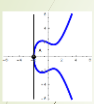
- **Closure**: For all $a,b\in G$, then $a+b\in G$.
- **Identity**: There exists $e\in G$ such that for all $a\in G$, $a+e=e+a=a$.
- **Inverses**: For all $a\in G$ there exists $a^{-1}\in G$ with $a+a^{-1}=a^{-1}+a=e$.
- **Associativity**: For all $a,b,c\in G$, then $(a+b)+c=a+(b+c)$.
- **Commutativity**: For all $a,b\in G$, $a+b=b+a$.

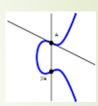
Adding rational points:

- The sum of 2 rational points is also a rational point.
- The point at infinity is the identity element, and it is a rational point.
- Reflecting a point across the x-axis produces the inverse, a rational point.
- The addition of rational points is associative. (Cayley-Bacharach)
- The 3rd point is not affected by the order of first 2 points.

Order of a Point

- If $A+A+...+A=nA=\infty$, then the **order** of point A is n.
  - The order of the point at infinity is 1.
  - The order of an x-intercept is 2.
  - The order of an inflection point is 3.
  - Some points may have infinite order.



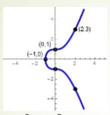


- **Nagell-Lutz Theorem** (1935). If $A=(x,y)$ is a rational point of finite order on the elliptic curve $y^2=x^3+px+q$ having integer coefficients, then:
  - Both coordinates are integers.
  - If the point is not an x-intercept, then y is a factor of the discriminant $\Delta=-4p^3-27q^2$.
- Corollary: A non-integer rational point has infinite order.

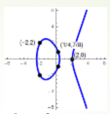
More Theorems

- **Mordell's Theorem** (1922). The group of rational points on an elliptic curve with rational coefficients is a finitely generated abelian group.
- **Mazur's Theorem** (1982).
  - Suppose a rational point on an elliptic curve has finite order n. Then $1 \le n \le 12$, but $n \ne 11$.
  - The subgroup of rational points of finite order is isomorphic to either Z_n or to $Z_2 \oplus Z_k$, with $k = 2,4,6,8$. It is called the **torsion subgroup**.
- Therefore: every group of rational points on an elliptic curve is isomorphic to $Z^r \oplus (\text{torsion subgroup})$, where r is the **rank**.

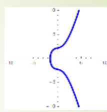
Examples



$y^2 = x^3 + 1$



$y^2 = x^3 - 5x + 2$



$y^2 = x^3 + x + 5$

- By Nagell-Lutz Theorem, integer points are easy to find.

$\Delta = -27 = -3^3$ $\qquad \Delta = 392 = 2^3 \cdot 7^2$ $\qquad \Delta = -679 = -7 \cdot 97$

- By Mazur's Theorem, there is an isomorphism.

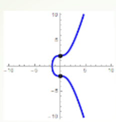
Z_6 $\qquad Z \oplus Z_2$ $\qquad Z_1$

- By Mordell's Theorem, there are finitely many generators.

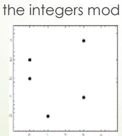
$(2,3)$ $\qquad (2,0),(-2,2)$ $\qquad \infty$

Graphing on a Finite Field

- Over the real numbers: $y^2 = x^3 + 4$



- Over the integers mod 5: $y^2 = (x^3 + 4) \bmod 5$



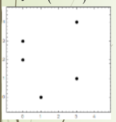
$4^2 = (3^3 + 4) \bmod 5$

$16 = 31 \bmod 5$

- If every point is nonsingular, then with the addition of points defined as before, these rational points will also form an abelian group.

Bezout on a Finite Field?

$y^2 = (x^3+4) \bmod 5$



- Bezout's Theorem requires that the field be algebraically closed (so every number has a root).
  - But finite fields are never algebraically closed.
  - For integers mod 5, the square roots of 2 and 3 do not exist.
- But all is not lost. If a line intersects the curve with
  - Multiplicity 3, the "third" point is itself.
  - Multiplicity 2, the remaining linear factor has a solution.
  - Multiplicity 1, the remaining quadratic factor may or may not have a solution. Some lines intersect in only one point.
- However, if a line intersects in 2 points, then it will intersect in a third point. The remaining linear factor has a solution.
- Still required for group addition:
  - Each point has an "opposite".
  - The point at infinity is the identity.

"Slopes" on a Finite Field?

- Can we compute "slopes" on a finite field? Yes, use the same "formulas".
  - The slope of the curve at any point can be found with implicit differentiation.

$$y^2 = (x^3+4) \bmod 5 \qquad \frac{dy}{dx} = \frac{3x^2}{2y} \Rightarrow m = \frac{3x^2}{2y} \bmod 5$$

- Since only integers are permitted, all non-vertical tangent lines must have integer slopes.

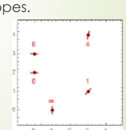
$$m_{(1,0)} = \frac{3(1^2)}{2(0)} = DNE$$

$$m_{(3,1)} = \frac{3(3^2)}{2(1)} = \frac{27}{2} \bmod 5 = \frac{2}{2} = 1$$

$$m_{(0,2)} = \frac{3(0^2)}{2(2)} = 0$$

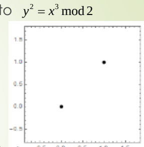
$$m_{(0,3)} = \frac{3(0^2)}{2(3)} = 0$$

$$m_{(3,4)} = \frac{3(3^2)}{2(4)} = \frac{27}{8} \bmod 5 = \frac{32}{8} \bmod 5 = 4$$



A Simple Case of a Singularity

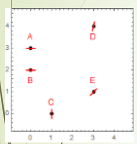
- The curve $y^2 = (x^3+4) \bmod 2$ is equivalent to $y^2 = x^3 \bmod 2$
- Easy to confirm 2 points.
- Slope: $\frac{dy}{dx} = \frac{3x^2}{2y} \Rightarrow m = \frac{3x^2}{2y} = \frac{x^2}{0} \bmod 2$
- At $(1,1)$ there is a vertical tangent.
- But $(0,0)$ is singular: $\frac{\partial}{\partial x}(y^2 - x^3) = \frac{\partial}{\partial y}(y^2 - x^3) = 0$



- If curve C is nonsingular on R², and it is graphed on a finite field, then it has:
  - **Bad reduction** if it is singular on that finite field.
  - **Good reduction** if it is nonsingular on that finite field.
- If $p \geq 3$ does not divide the discriminant, then curve C has good reduction.

Group Structure

- Since $y^2 = (x^3 + 4) \bmod 5$ had good reduction, the set of rational points form a group.
- The addition table for the points:



	A = (0,3)	B = (0,2)	C = (1,0)	D = (3,4)	E = (3,1)	∞
A = (0,3)	B	∞	E	C	D	A
B = (0,2)	∞	A	D	E	C	B
C = (1,0)	E	D	∞	B	A	C
D = (3,4)	C	E	B	A	∞	D
E = (3,1)	D	C	A	∞	B	E
∞	A	B	C	D	E	∞

- Multiples of each point: $\{P, 2P, 3P, ...\}$

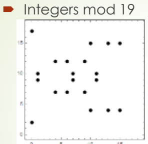
$$nA = \{A, B, \infty\}$$
$$nB = \{B, A, \infty\}$$
$$nC = \{C, \infty\}$$
$$nD = \{D, A, C, B, E, \infty\}$$
$$nE = \{E, B, C, A, D, \infty\}$$
$$n\infty = \{\infty\}$$

- This group is isomorphic to Z_6, and D is a generator.
- For this group, given any generator G, the equation $nG = P$ can be solved for n.

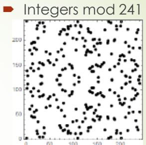
Larger Finite Fields

$y^2 = x^3 + 4$

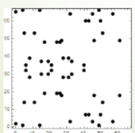
- Integers mod 19



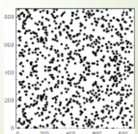
- Integers mod 241



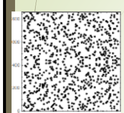
- Integers mod 67



- Integers mod 863



The ECDLP



- The **elliptic curve discrete logarithmic problem** (ECDLP) is to find the value n in the equation $nG = P$, where G and P are points on an elliptic curve over a finite field.
- "Logarithmic", because if the group operation was written multiplicatively, the equation would be $G^n = P$.
- The ECDLP is considered to be a very hard problem (even harder than factoring very large integers).

- **Elliptic curve cryptography** is an approach to public key cryptography that uses the ECDLP.
- Bitcoin uses elliptic curve cryptography, specifically $y^2 = x^3 + 7$ over the integers mod

115792089237316195423570985008687907853269984665640564039457584007908834671663

A Finite Field Theorem

- **Hasse's Theorem** (1933). If p is a prime number, the number of points $\#C(Z_p)$ on the elliptic curve C over the finite field Z_p satisfies the inequality

$$\left|\#C(Z_p) - p - 1\right| \le 2\sqrt{p}$$

  - Or equivalently: $\left(\sqrt{p}-1\right)^2 \le \#C(Z_p) \le \left(\sqrt{p}+1\right)^2$
- Some results:

Prime	Max Difference	Percent Difference	Actual
5	5	100 %	6
19	9	47.4 %	21
67	17	25.4 %	57
241	32	13.3 %	
863	59	6.84 %	
1.158×10^{77}	6.806×10^{38}	5.877×10^{-37} %	1.158×10^{77}

Fermat and Modularity

- **Fermat's Last Theorem** (conjectured 1637): There are no nontrivial solutions of $a^n + b^n = c^n$, when $n \ge 3$.
- Andrew Wiles proved (1995) that every semistable elliptic curve is **modular** (which was enough to imply Fermat's Last Theorem is true).

- Given the elliptic curve E, then for each prime number p, we can define $\varepsilon_p = \#E(\mathbb{Z}_p) - p - 1$, a quantity whose values were considered in Hasse's Theorem.
- We then define the **L-function** $L(E,s)$ of the elliptic curve E through an infinite product, specifically $L(E,s) = \prod_{p \text{ prime}} \left(1 - \frac{\varepsilon_p}{p^s} + \frac{1}{p^{2s-1}}\right)$.
- The infinite product form of the L-function can be rewritten as an infinite sum, and we obtain the **L-series** $L(E,s) = \sum_{n=1}^{\infty} \frac{\varepsilon_n}{n^s}$. Note that this also defines ε_n when n is not prime.
- The coefficients ε_n of $L(E,s)$ are then used to define the function $f_E(z) = \sum_{n=1}^{\infty} \varepsilon_n e^{2\pi i n z}$.
- Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix of integers, with $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$. (This collection of matrices forms a group called the **modular group**.)
- Let H be the subset of $\mathbb{C}$ for which the imaginary part is positive. This is often referred to as the **upper half-plane**.
- If there exists a number N that is a factor of c, and for which the function $f_E(z)$ has the property that $f_E\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f_E(z)$ for every $z \in H$, then the elliptic curve E is said to be **modular**, and the number N is called the **conductor** of E.

BSD Conjecture

- **Birch and Swinnerton-Dyer Conjecture** (1965): Let E be a rational elliptic curve, and $L(E,s)$ its L-function. The multiplicity of the zero of the function $L(E,s)$ at $s=1$ is equal to the rank of the group of rational points on E.
- In 2000, the Clay Mathematics Institute identified seven **Millennium Problems** as "important classic problems that have resisted solution for many years", and for each of the seven is offering a $1,000,000 prize for its solution. The BSD conjecture is one of these problems.

Postscript: Why the Name?

- **Ellipses** are conic sections, or algebraic curves of degree 2.
- **Elliptic integrals** originally arose when solving for the arc length of an ellipse. Now, they describe any integral of the form $f(x) = \int_c^x R\left(t, \sqrt{P(t)}\right) dt$, where R is a rational function, P is a polynomial of degree 3 or 4.
- **Elliptic functions** were originally defined as inverse functions of elliptic integrals. They are periodic in 2 directions on the complex plane, and satisfy the differential equation $(y'(z))^2 = P(y(z))$, where P is a cubic polynomial with no repeated roots.
- **Elliptic curves** use elliptic functions when parametrized.

For Further Reading

About Elliptic Curves:

- Ash, Avner, & Robert Gross, *Elliptic Tales*, 2012.
- Silverman, Joseph H., & John T. Tate, *Rational Points on Elliptic Curves*, 2nd edition, 2015.

About Elliptic Curve Cryptography

- Corbellini, Andrea, "Elliptic Curve Cryptography: A Gentle Introduction", andrea.corbellini.name, May 17-June 8, 2015.
- Sullivan, Nick, "A (Relatively Easy to Understand) Primer on Elliptic Curve Cryptography", ArsTechnica.com, Oct. 24, 2013.

About the Millennium Problems and the BSD Conjecture:

- Devlin, Keith, *The Millennium Problems*, 2002.
- Johnson, Brent A., "An Introduction to the Birch and Swinnerton-Dyer Conjecture", Rose-Hulman Undergraduate Mathematics Journal, 16:1 (Spring 2015), p. 270-281.
- Stewart, Ian, *Visions of Infinity*, 2013.

More Reading

About the Proof of Fermat's Last Theorem:

- Faltings, Gerd, "The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles", *Notices of the American Mathematical Society*, 42:7 (July 1995), p. 743-746.
- Hellegouarch, Yves, *Invitation to the Mathematics of Fermat-Wiles*, 2002.
- Ribenboim, Paulo, *Fermat's Last Theorem for Amateurs*, 1999.

About the Connection with Ellipses:

- Rice, Adrian, and Ezra Brown, "Why Ellipses are Not Elliptic Curves", *Mathematics Magazine*, 85 (2012), p. 163-176.
- Brown, Ezra, "Three Fermat Trails to Elliptic Curves", *College Mathematics Journal*, 31:3 (May 2000), p. 162-172.