Introduction to Elliptic Curves

What is an Elliptic Curve?

- An ***Elliptic Curve*** is a curve given by an equation

E : $y^2 = f(x)$

Where f(x) is a square-free (no double roots) cubic or a quartic polynomial

After a change of variables it takes a simpler form:

E : $y^2 = x^3 + Ax + B$

$$\boxed{4A^3 + 27B^2 \neq 0}$$

So $y^2 = x^3$ is not an elliptic curve but $y^2 = x^3 - 1$ is

Why is it called Elliptic?

Arc Length of an ellipse = $\boxed{\int_{-a}^{a}\sqrt{\frac{a^2-\left(1-b^2/a^2\right)x^2}{a^2-x^2}}\,dx}$

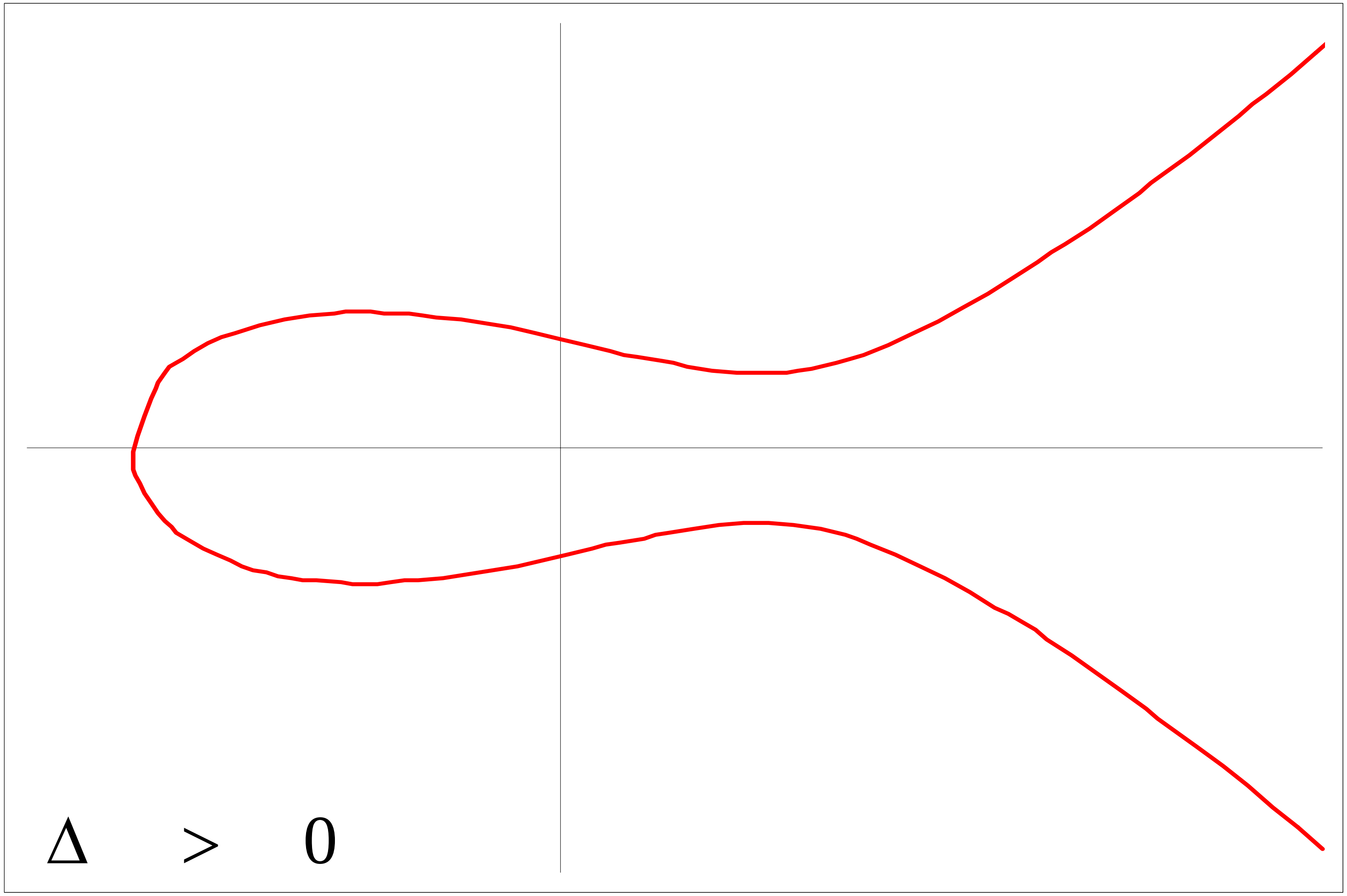
Let $k^2 = 1 - b^2/a^2$ and change variables $x \rightarrow ax$.

Then the arc length of an ellipse is $\boxed{a\int_{-1}^{1}\frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\,dx}$

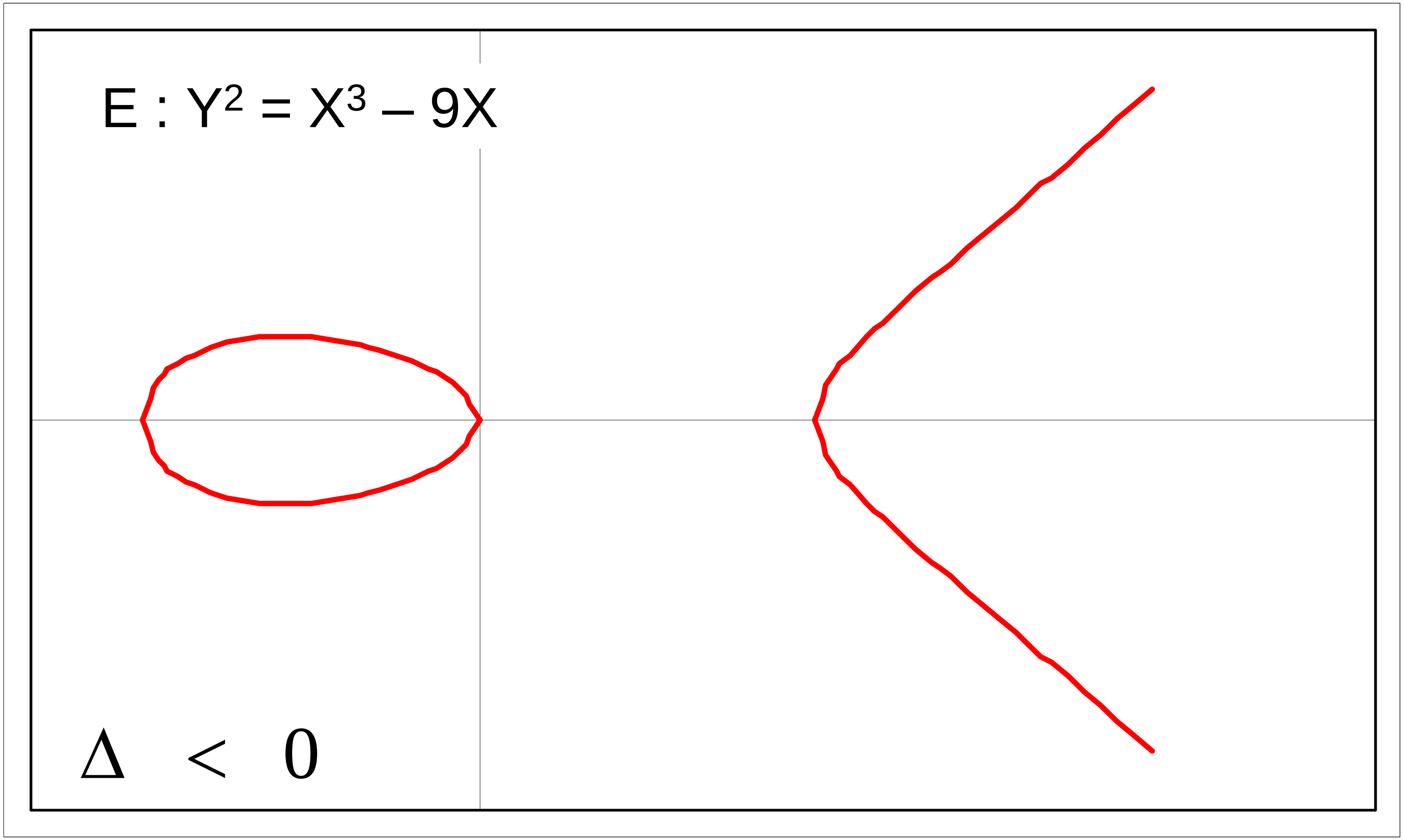
$$\text{Arc Length} = a\int_{-1}^{1}\frac{1-k^2x^2}{y}\,dx$$

with $y^2 = (1 - x^2)(1 - k^2x^2)$ = quartic in x

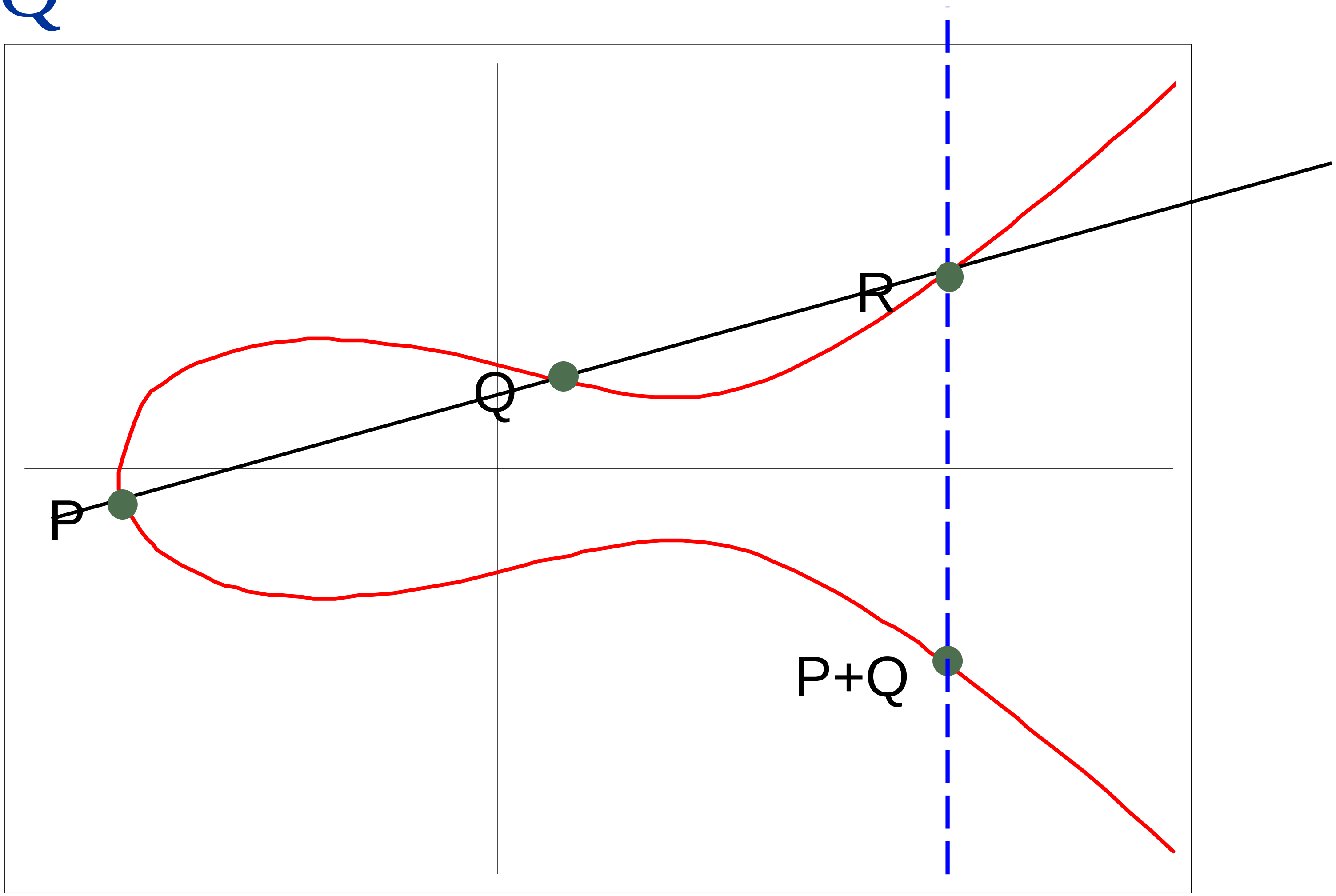
Graph of $y^2 = x^3 - 5x + 8$



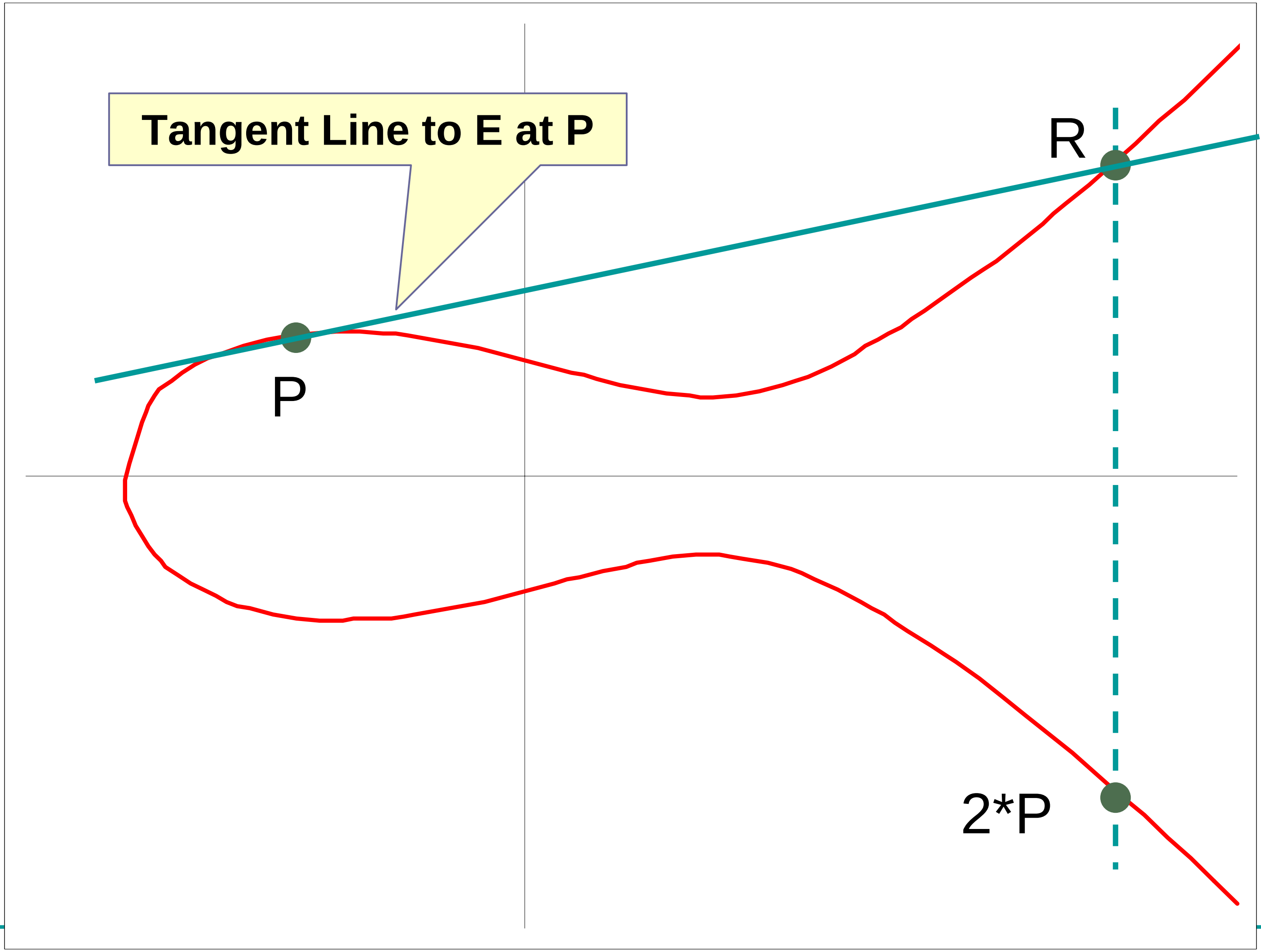
Elliptic curves can have separate components



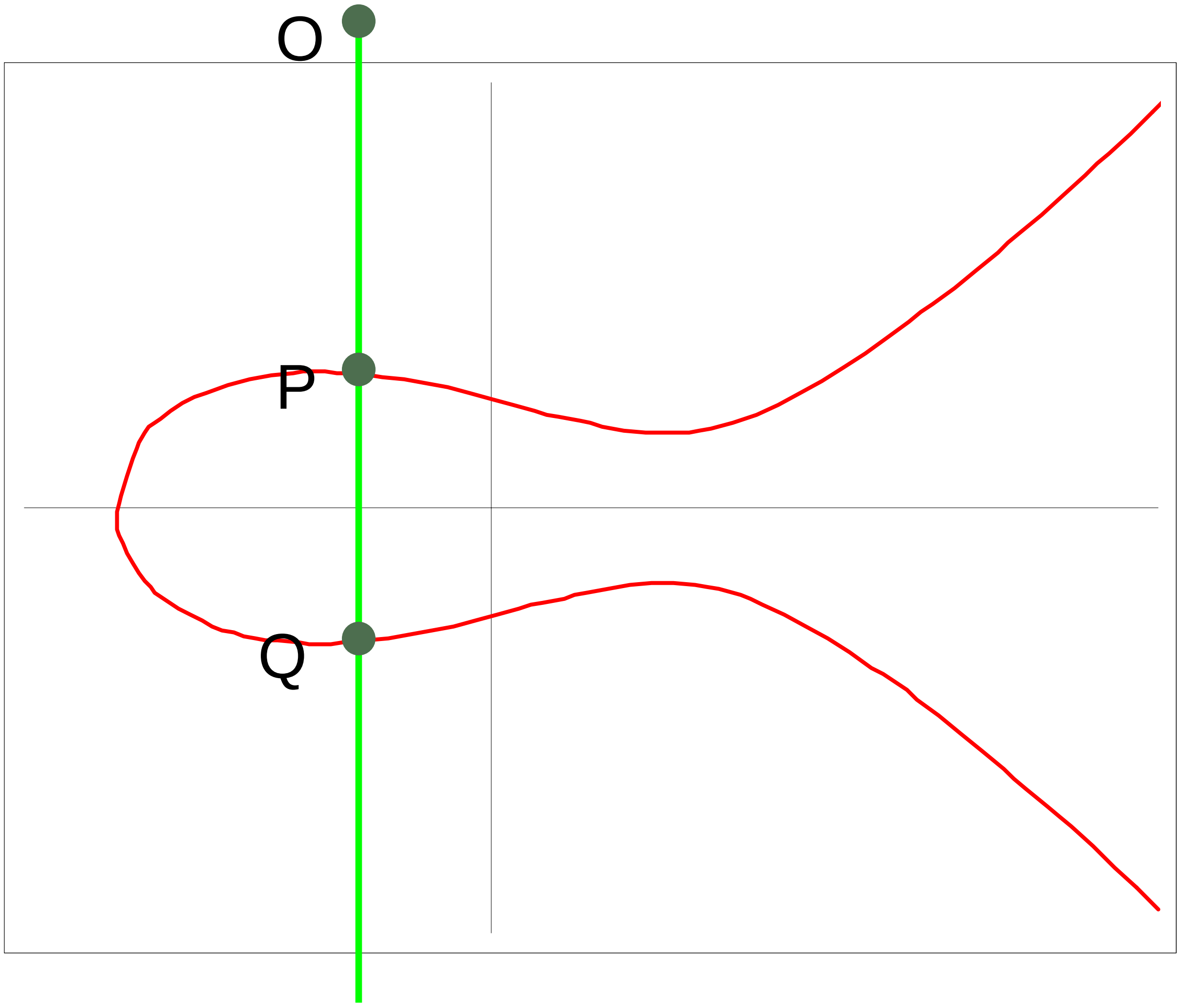
Addition of two Points P+Q



Doubling of Point P



Point at Infinity



Addition of Points on E

1. Commutativity. $P_1+P_2 = P_2+P_1$

2.Existence of identity. $P + O = P$

3. Existence of inverses. $P + (-P) = O$

4. Associativity. $(P_1+P_2) + P_3 = P_1+(P_2+P_3)$

Addition Formula

Suppose that we want to add the points

$$P_1 = (x_1,y_1) \quad \text{and} \quad P_2 = (x_2,y_2)$$

on the elliptic curve

$$E : y^2 = x^3 + Ax + B.$$

If $x_1 \neq x_2$

$$\boxed{m = \frac{y_2 - y_1}{x_2 - x_1}}$$

If $x_1 = x_2$

$$\boxed{m = \frac{3x_1{}^2 + A}{2y_1}}$$

$$\boxed{x_3 = m^2 - x_1 - x_2}$$

$$\boxed{y_3 = m(x_1 - x_3) - y_1}$$

Note that when P1, P2 have rational coordinates and A and B are rational, then P_1+P_2 and 2P also have rational coordinates

Important Result

Theorem (Poincaré, ≈1900): *Suppose that an elliptic curve* E *is given by an equation of the form*

$$y^2 = x^3 + A\,x + B \qquad \textit{with} \quad A,B \textit{ rational numbers.}$$

Let E**(Q)** *be the set of points of* E *with rational coordinates,*

$$E(\mathbf{Q}) = \{\, (x,y) \in E \;:\; x,y \textit{ are rational numbers} \,\} \cup \{\, O \,\}.$$

Then sums of points in E**(Q)** *remain in* E(**Q**).

The many uses of elliptic curves.

Really Complicated first…

Elliptic curves were used to prove Fermat's Last Theorem

$$E_{a,b,c} \;:\; y^2 = x\,(x - a^p)\,(x + b^p)$$

Suppose that $a^p + b^p = c^p$ with $abc \neq 0$.

Ribet proved that $E_{a,b,c}$ <u>is</u> <u>not</u> modular

Wiles proved that $E_{a,b,c}$ <u>is</u> modular.

Conclusion: The equation $a^p + b^p = c^p$ has no solutions.

Elliptic Curves and String Theory

In *string theory*, the notion of a point-like particle is replaced by a curve-like string.

As a string moves through space-time, it traces out a surface.

For example, a single string that moves around and returns to its starting position will trace a torus.

So the path traced by a string looks like an elliptic curve!

Points of E with coordinates in the complex numbers **C** form a *torus*, that is, the surface of a donut.

Congruent Number Problem

- Which positive rational n can occur as areas of right triangles with rational sides?

This question appears in 900A.D. in Arab manuscripts

A theorem exists to test the numbers but it relies on an unproven conjecture.

- Ex: ***5*** is a congruent number because it is the area of 20/3, 3/2, 41/6 triangle

Congruent Number Problem cont….

Suppose a, b and c satisfy $\boxed{a^2 + b^2 = c^2}$ $\boxed{\frac{ab}{2} = n}$

Then set $\boxed{x = \frac{n(a+c)}{b}}$ $\boxed{y = \frac{2n^2(a+c)}{b^2}}$

A Calculation shows that $\boxed{y^2 = x^3 - n^2 x}$

Conversely: $\boxed{a = (x^2 - n^2)/y}$ $\boxed{c = \frac{x^2 + n^2}{y}}$ $\boxed{b = \frac{2nx}{y}}$

A positive rational number n is congruent if and only if the elliptic curve has a rational point with y not equal to 0

Congruent Number Problem cont…

Continuing with n = 5

$$\boxed{y^2 = x^3 - 25x}$$

We have Point (-4,6) on the curve

$$We \quad find\ -2P \quad is\ x = \frac{1681}{144} \qquad y = \frac{62279}{1728}$$

We can now find a, b and c

Factoring Using Elliptic Curves

Ex: We want to factor 4453

Step 1. Generate an elliptic curve with point P mod n

$$y^2 = x^3 + 10x - 2 \pmod{4453} \ let\ P = (1,3)$$

Step 2. Compute BP for some integer B.

$$Lets \quad compute \quad 2P \quad first \quad \frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}$$

$$We \ used \ the \ fact \ that \ \gcd(6, 4453) = 1 \ to \ find \ 6^{-1} \equiv 3711 \pmod{4453}$$

$$we \ find \ that \ 2P = (x, y) \ with \ x \equiv 3713^2 - 2 \quad y \equiv -3713(x-1) - 3 \equiv 3230$$

$$2P \ is \ (4332, 3230)$$

Factoring Continued..

Step 3. If step 2 fails because some slope does not exist mod n, the we have found a factor of n.

$$To\ \ compute\ \ \ 3P\ \ we\ \ add\ \ \ P\ \ and\ \ \ 2P$$

$$The\ slope\ is\ \frac{3230-3}{4332-1}=\frac{3227}{4331}$$

$$But\quad \gcd(4331,4453)=61\neq 1\ \ we\ can\ not\ \ find\ \ 4331^{-1}(\mathrm{mod}\ 4453)$$

$$However,\ \ we\ have\ \ found\ the\ \ factor\ 61\ of\ \ 4453$$

Cryptography

Suppose that you are given two points $\boldsymbol{P}$ and $\boldsymbol{Q}$ in $E(\mathbf{F}_p)$.

The **<u>Elliptic Curve Discrete Logarithm Problem</u>** (ECDLP) is to find an integer $\boldsymbol{m}$ satisfying

$$Q = \overbrace{P + P + \cdots + P}^{m \text{ summands}} = mP.$$

- If the prime p is large, it is very very difficult to find m.
- The extreme difficulty of the ECDLP yields highly efficient cryptosystems that are in widespread use protecting everything from your bank account to your government's secrets.

Elliptic Curve Diffie-Hellman Key Exchange

Public Knowledge: A group **$E(F_p)$** and a point **P** of order n.

BOB		ALICE
Choose secret $0 < \mathbf{b} < n$		Choose secret $0 < \mathbf{a} < n$
Compute $\mathbf{Q}_{Bob} = \mathbf{bP}$		Compute $\mathbf{Q}_{Alice} = \mathbf{aP}$
Send $\mathbf{Q}_{Bob}$	$\longrightarrow$	to Alice
to Bob	$\longleftarrow$	Send $\mathbf{Q}_{Alice}$
Compute $\mathbf{bQ}_{Alice}$		Compute $\mathbf{aQ}_{Bob}$

Bob and Alice have the shared value $\mathbf{bQ}_{Alice} = \mathbf{abP} = \mathbf{aQ}_{Bob}$

Can you solve this?

Suppose a collection of cannonballs is piled in a square pyramid with one ball on the top layer, four on the second layer, nine on the third layer, etc.. If the pile collapses, is it possible to rearrange the balls into a square array (how many layers)?

Hint: P_1 *and* P_2 *are trivial solutions*

Find $P_2 + P_3$

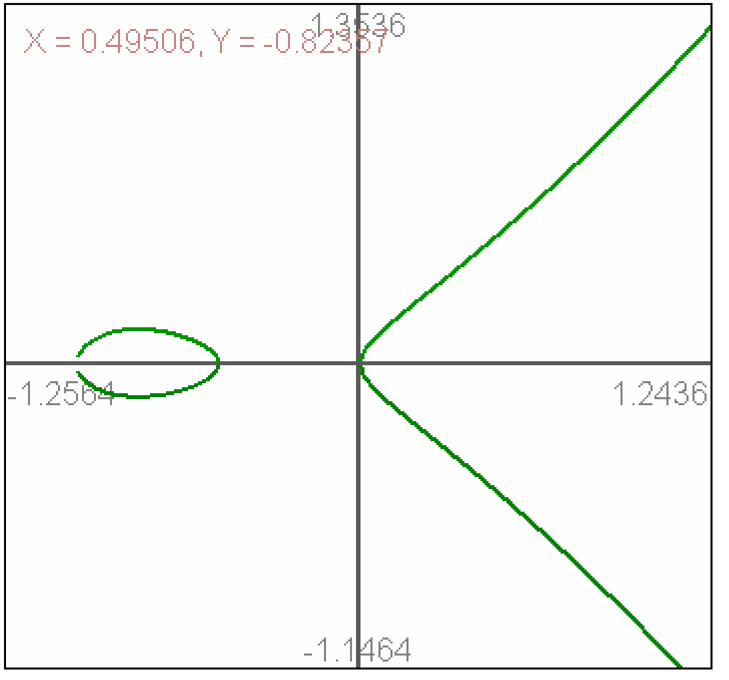
$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + \ldots$$

Solution

$$1^2 + 2^2 + 3^3 + \ldots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

$$y^2 = \frac{x(x+1)(2x+1)}{6}$$

This is an elliptic curve



We know two points $P_1(0,0)$ $P_2(1,1)$

The line through these points is y = x

$$x^2 = \frac{x(x+1)(2x+1)}{6} = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6}$$

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0$$

Solution cont…

$$0+1+x=\frac{3}{2} \quad therefore \quad P_3 \ \ is \ \ (\frac{1}{2},-\frac{1}{2})$$

$$The\ line\ through\ P_2\ and\ P_3\ is\ y=3x-2$$

$$(3x-2)^2=\frac{x(x+1)(2x+1)}{6}$$

$$x^3-\frac{51}{2}x^2+\ldots=0$$

$$\frac{1}{2}+1+x=\frac{51}{2}$$

$$\boxed{x=24} \quad \boxed{y=70}$$

$$\boxed{1^2+2^2+3^2+\ldots+24^2=70^2}$$

References

- Elliptic Curves Number Theory and Cryptography

Lawrence C. Washington

- http://www.math.vt.edu/people/brown/doc.html
- http://www.math.brown.edu/~jhs/