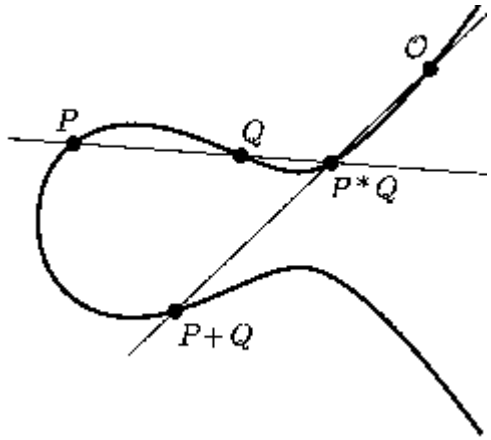


Elliptic Curves

To (too) many mathematicians

OTL

a puzzle

- **What is the number of balls that may be piled as a square pyramid and also re-arranged into a square array?**
- **Sol:** Let x be the height of the pyramid.

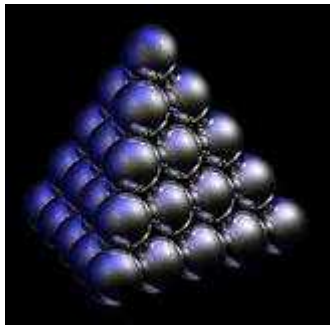
Thus, $$1^2 + 2^2 + 3^2 + \ldots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

We also want this to be a square:

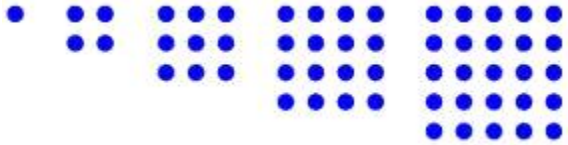
Hence, $$y^2 = \frac{x(x+1)(2x+1)}{6}$$

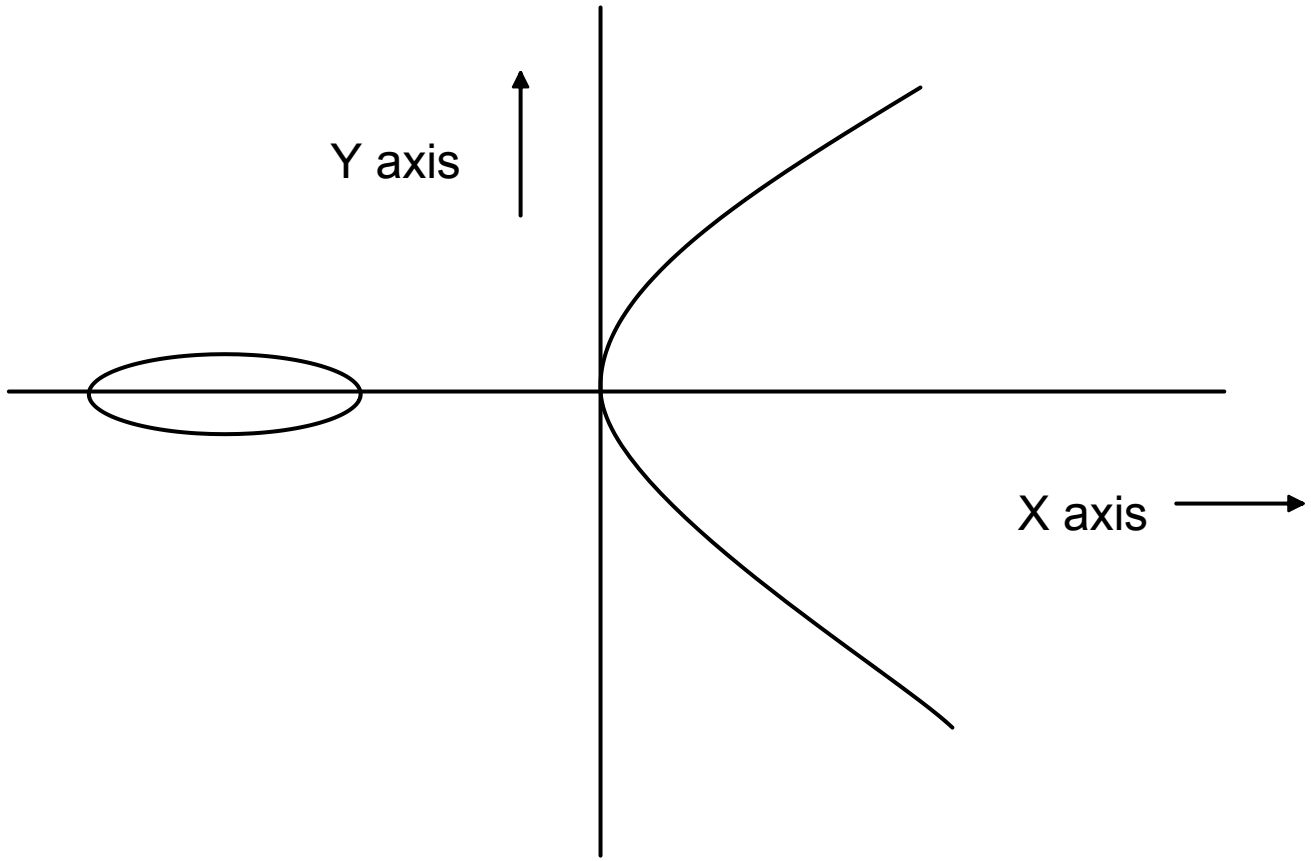
picture

from here



into these shape




Y axis
X axis

Diophantus

- Uses a set of known points to produce new points
- (0,0) and (1,1) are two trivial solutions
- Equation of line through these points is y=x.
- Intersecting with the curve and rearranging terms:

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

- We know that 1 + 0 + x = 3/2 =>

  x = ½ and y = ½

- Using symmetry of the curve we also have (1/2,-1/2) as another solution

Diophantus' Method

- Consider the line through (1/2,-1/2) and (1,1) => y=3x-2
- Intersecting with the curve we have:

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

- Thus ½ + 1 + x = 51/2 or x = 24 and y=70

Why is it called elliptic curve ?

- Originally developed to measure the circumference of an ellipse
- Recall that y = sin w means

$$w(y) = \sin^{-1} y = \int_0^y \frac{1}{\sqrt{1-t^2}}\, dt$$

*** Abel

- 그래서 $y = \sin w$
- Abel took the inverse functions of elliptic integrals and found the double periodicity.

$$F(w) = \int_0^w \frac{dz}{\sqrt{(1-z^2)(1-k^2z^2)}}$$

Ellipse

- $x^2/a^2 + y^2/b^2 = 1$

The Arc Length of an Ellipse

Let $k^2 = 1 - b^2/a^2$ and change variables $x \rightarrow ax$. Then the arc length of an ellipse is

$$a\int_{-1}^{1}\sqrt{\frac{1-k^2x^2}{1-x^2}}\,dx \qquad a\int_{-1}^{1}\frac{1-k^2x^2}{\sqrt{(1-x^2)(1-k^2x^2)}}\,dx$$

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

An Elliptic Curve!

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

An **elliptic integral** $\int R(x,y)\,dx$

*** Double Periodicity

Two linearly independent periods.

$$\wp(z+w_1)=\wp(z+w_2)=\wp(z)$$
$$\text{for} \quad all \quad complex \quad \nu mber \quad z.$$

It satisfies

$$[\wp'(z)]^2=4\wp(z)^3-60\,G_4\wp(z)-140\,G_6$$

*** Double Periodicity

- So for x = $\wp(z)$ and y = $\wp'(z)$
- $y^2 = 4x^3 - 60G_3 x - 140G_6$

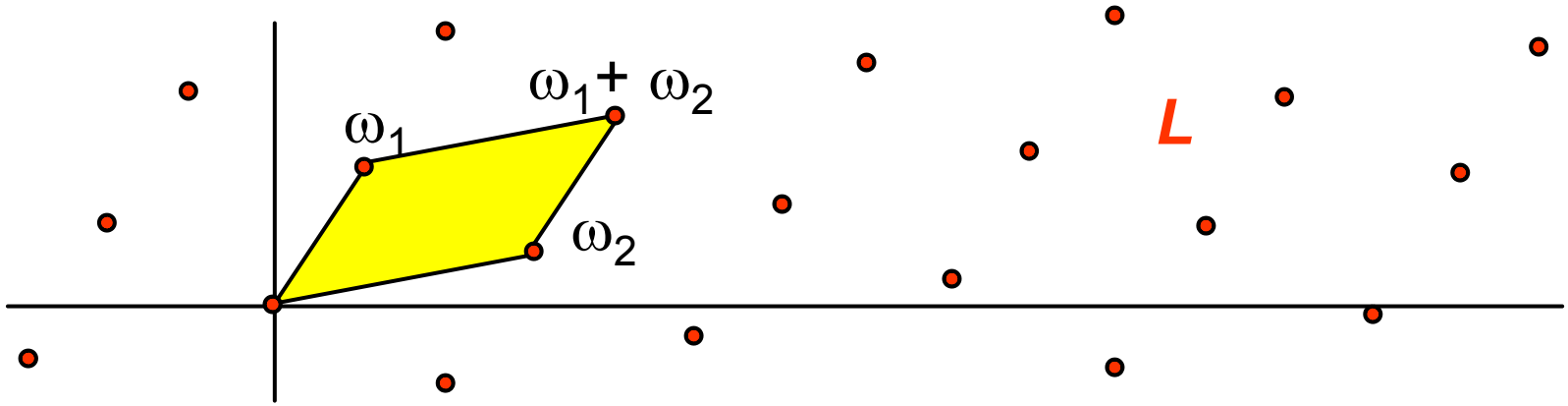
Elliptic Functions and Elliptic Curves

The $\wp$-function and its derivative satisfy an algebraic relation

$$\wp'(z)^2 = \wp(z)^3 + A\,\wp(z) + B$$

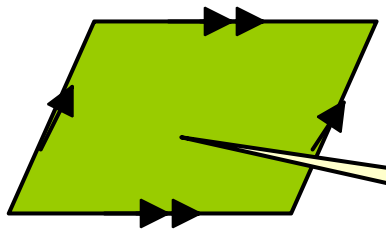
The double periodicity means that it is a function on the quotient space $\mathbb{C}/L$, where L is the lattice

$$L = \{\, n_1\omega_1 + n_2\omega_2 \;:\; n_1, n_2 \text{ are integers} \,\}.$$



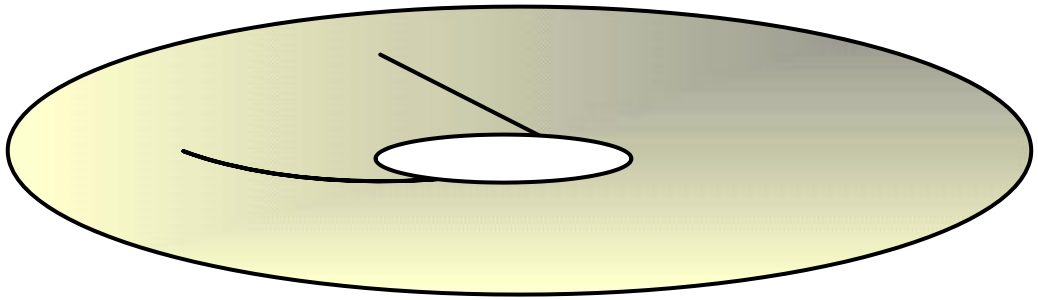
The Complex Points on an Elliptic Curve

The $\wp$-function gives a complex analytic isomorphism

$$\frac{\mathbb{C}}{L} = \text{  } \xrightarrow{(\wp(z),\wp'(z))} E(\mathbb{C})$$

Parallelogram with opposite sides identified = a torus

Thus the points of E with coordinates in the complex numbers $\mathbb{C}$ form a *torus*, that is, the surface of a donut.

$E(\mathbb{C}) =$ 

*** $X^2 + Y^2 = C$

- Let $x = a + b\sqrt{-1}$, $y = c + d\sqrt{-1}$.
- The solution over complex numbers is a surface, in fact topologically sphere.
- If unbelievable, check out level curves.

- Furthermore it has group structure.
- $(a + b\sqrt{-1})(c + d\sqrt{-1})$
  becomes $= ac-bd + (ad+bc)\sqrt{-1}$

Why is it called Torus?

- Complex Tori

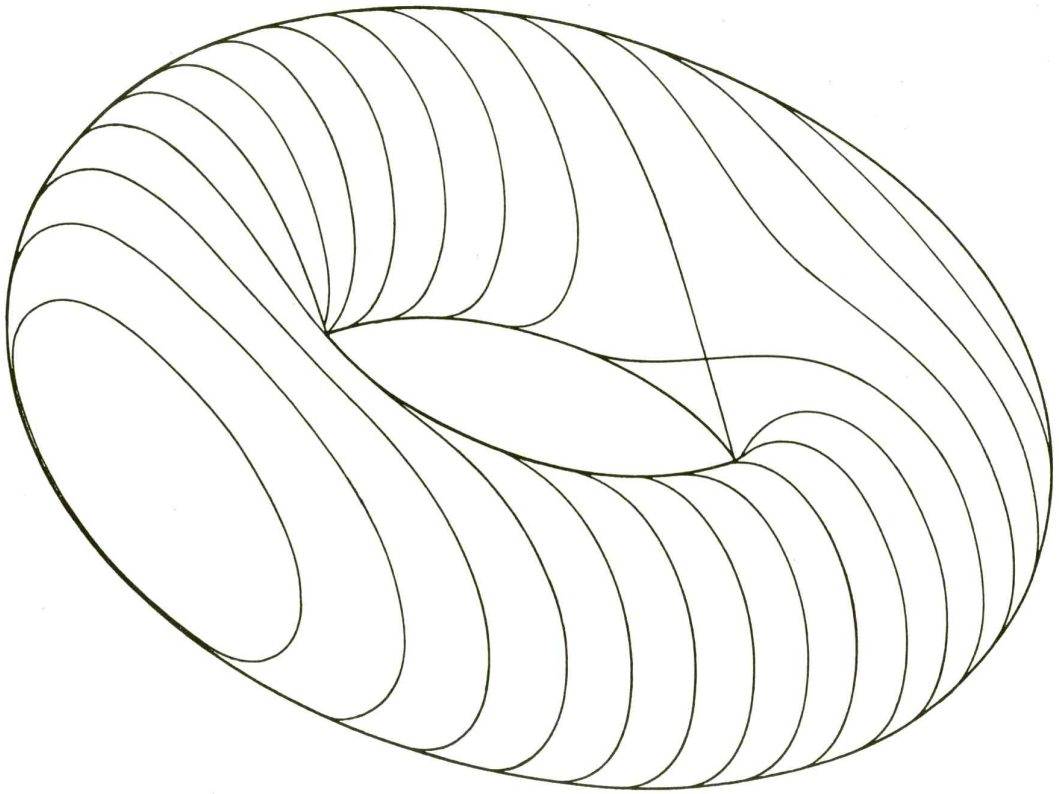
$$y^2 = x\left(x^2 - 1\right)$$

*** Complex Tori

- Let $x = a + b\sqrt{-1}$, $y = c + d\sqrt{-1}$.
- For fixed $x = a + b\sqrt{-1}$, there are possibly two y's. Namely

$$+\sqrt{x(x^2-1)}, -\sqrt{x(x^2-1)}$$

- Example



Why is it called Torus?

- If we introduce *points at infinity* and the *complex numbers*, we can argue that the graph is a torus.

*** Why torus ?

- If a sphere, then always the level curves are circles.

- If a torus, the level curves are a circle or two circles.

Why Elliptic Curve ?

- Discrete Logarithm Problem

- Given a finite group G with two of its elements a and b.
- Find an integer x such that ,
  $a^x = b$ if it exists.

- Ex) Non-zero elements of some finite field.

*** Better groups ?

- For a finite field F,

$$GL_2(F) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | \, ad - bc \neq 0, a, b, c, d \in F \right\}$$

- The Times(London) Jan. 1999 An Irish schoolgirl Sarah Flannery used matrices as an alternative to RSA. Her algorithm is far faster than the RSA and equally secure.
- The Art of Computer Programming by Donald Knuth

*** Better groups ?

- How about this group ?

$$F = Z/17Z = Z \pmod{17}$$
$$6^2 = 36 = 2 \bmod 17$$
$$6 \; behaves \; like \; \sqrt{2}$$

$$X^2 - 2Y^2 = 1$$
$$(3+2\sqrt{2})(3-2\sqrt{2}) = 1$$
$$(3+12)(3-12) = -136 = 1 \bmod 17$$

*** Better group ?

- G = {(x, y) | $x^2 - 2y^2 = 1$ over F}

$$(x_1, y_1) \bullet (x_2, y_2) =$$
$$(x_1 + \sqrt{2}\, y_1)(x_2 + \sqrt{2}\, y_2) =$$
$$(x_1 x_2 + 2y_1 y_2) + \sqrt{2}\,(x_1 y_2 + x_2 y_1)$$

$$(x_1, y_1) \bullet (x_2, y_2) =$$
$$(x_1 x_2 + 2y_1 y_2, x_1 y_2 + x_2 y_1)$$

Why Elliptic Curve ?

- DLP(Discrete Logarithm Problem) on finite field can be solved faster than we thought!
- by “index calculus”
- To protect against this attack...
- Elliptic curves!

index calculus

Elliptic curves in Cryptography

- Elliptic Curve (EC) cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller.

- The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of non-zero elements of) the underlying finite field.

on finite fields

- Consider $y^2 = x^3 + 2x + 3$ (**mod 5**)

  $x = 0,\ y^2 = 3$ no solution (mod 5)

  $x = 1,\ y^2 = 6 = 1,$ $y = 1,4$ (mod 5)

  $x = 2,\ y^2 = 15 = 0,$ $y = 0$ (mod 5)

  $x = 3,\ y^2 = 36 = 1,$ $y = 1,4$ (mod 5)

  $x = 4,\ y^2 = 75 = 0,$ $y = 0$ (mod 5)

- Then points on the elliptic curve are

  (1,1) (1,4) (2,0) (3,1) (3,4) (4,0) and the point at infinity. Denote it by O.

Notation

$GF(q)$ or F_q: finite field with q elements

typically, $q = p$ where p is prime, or 2^m

- $E(F_q)$: elliptic curve over F_q
- (x, y): point on $E(F_q)$
- ***O***: point at infinity

Definition of Elliptic curves

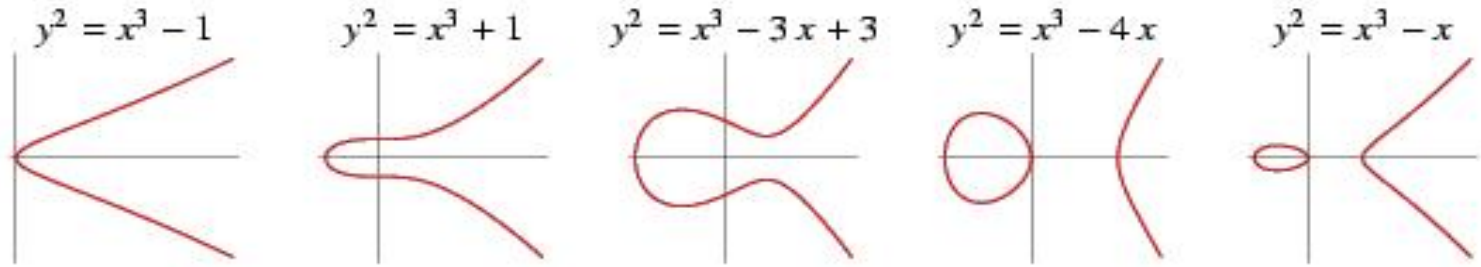
- An elliptic curve over a field ***K*** is a non-singular cubic curve in two variables, *f(x,y) =0* with a rational point (which may be a point at infinity).
- The field ***K*** is usually taken to be the complex numbers, reals, rationals, algebraic extensions of rationals, p-adic numbers, or a **finite field**.
- Elliptic curves groups for cryptography are examined with the underlying fields of $\boldsymbol{F_p}$ (*where p>3 is a prime*) and $\boldsymbol{F_2^m}$ (*a binary representation with* 2^m *elements*).

EC

- An *elliptic curve* is a plane curve defined by an equation of the form, when characteristic is neither 2 nor 3, and ..... What the hell ?

$$y^2 = x^3 + ax + b$$

Examples



*** Hmm...

- $x^3 + y^3 + 1 = 0$ is a cubic curve... ?
- $x = u + v,\ \ y = u - v$
- $(u+v)^3 + (u-v)^3 + 1 = 0$
- $2u^3 + 6uv^2 + 1 = 0$
- $6(v/u)^2 = -(1/u)^3 - 2$
- $X = -6/u,\ Y = 36v/u$
- $Y^2 = X^3 - 432$

*** $y^2 = x^4 + \ldots$

- Don't panic.

- Even $x^4 + y^4 = 1$ becomes
- $Y^2 = X^3 - 4X$

- Under
- $X=2(y^2+1)/x^2$, $Y=4y(y^2+1)/x^3$

Weierstrass Equation

- A two variable equation F(x,y)=0, forms a curve in the plane.

- generalized Weierstrass Equation of elliptic curves:

$$y^2 + a_1xy + a_3y = x^2 + a_2x^2 + a_4x + a_6$$

generalized Weierstrass ?

- An elliptic curve over a field ***K*** is a non-singular cubic curve with a rational point (which may be a point at infinity).

- any elliptic curve over any field can be written by a generalized form.

Quadratic Equation

$$x^2 + ax + b = 0 \qquad x = t - \frac{a}{2}$$

$$t^2 - \frac{a^2 - 4b}{4} = 0$$

Cubic Equation

$$x^3 + ax^2 + bx + c = 0 \qquad x = t - \frac{a}{3}$$

$$t^3 + pt + q = 0$$

$$p = b - \frac{a^2}{3}$$

$$q = c + \frac{2a^3 - 9ab}{27}$$

- **If Characteristic field is not 2:**

$$(y+\frac{a_1x}{2}+\frac{a_3}{2})^2 = x^3+(a_2+\frac{a_1^2}{4})x^2+a_4x+(\frac{a_3^2}{4}+a_6)$$

$$\Rightarrow y_1^{\,2} = x^3+a_2'x^2+a_4'x+a_6'$$

- **If Characteristics of field is neither 2 nor 3:**

$$x_1 = x+a_2'/3$$

$$\Rightarrow y_1^{\,2} = x_1^{\,3}+Ax_1+B$$

*** Discriminant

- Discriminant of $x^2 + bx + c$ is $b^2 - 4c$
- $b^2 - 4c$ is non-zero $\Leftrightarrow$ no double roots

- Discriminant of $x^3 + ax + b$ is $-4a^3 - 27b^2$
- $-4a^3 - 27b^2$ is non-zero $\Leftrightarrow$ no double roots

*** j-invariant

- Define j of this elliptic curve E as
- $j(E)/1728 = 4a^3/(4a^3+27b^2)$
- If we change $x = m^2x$, $y = m^3y$, get E:
- then j(E) = j(E)
- j - value fixes E

$$y^2 = x^3 + ax + b$$

*** j-invariant

- If we change $x = m^2x$, $y = m^3y$, get E:
- then $j(E) = j(E)$

- Why not something like $x = mx + ny^2 + s$?

- It has to keep the point at infinity and keep the form $y^2 = x^3 + ax + b$

Points on the Elliptic Curve (EC)

- Elliptic Curve over field L

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 + \ldots = x^3 + \ldots\}$$

- It is useful to add the point at infinity.

Group Law

- A group law may be defined where the sum of two points is the reflection across the *x*-axis of the third point on the same line

- Chords and tangents

The Abelian Group

Given two points P,Q in *E*, there is a third point, denoted by *P*+*Q* on *E*, and the following relations hold for all P,Q,R in *E.*

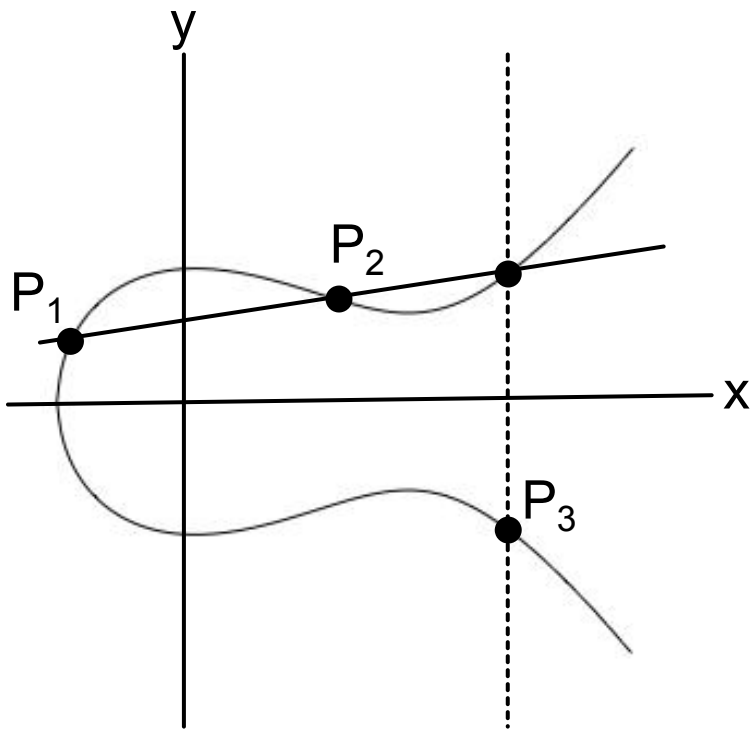
- $P + Q = Q + P$ (*commutativity*)
- $(P + Q) + R = P + (Q + R)$ (*associativity*)
- $P + O = O + P = P$ (*existence of an identity element*)
- there exists $(-P)$ such that $(-P) + P$

  $= P + (-P) = O$ (*existence of inverses*)

(P+Q)+R = P+(Q+R)

- Associativity is non-trivial.
- It gives Pascal's theorem and Pappus's theorem.

Elliptic Curve Picture



- Consider elliptic curve

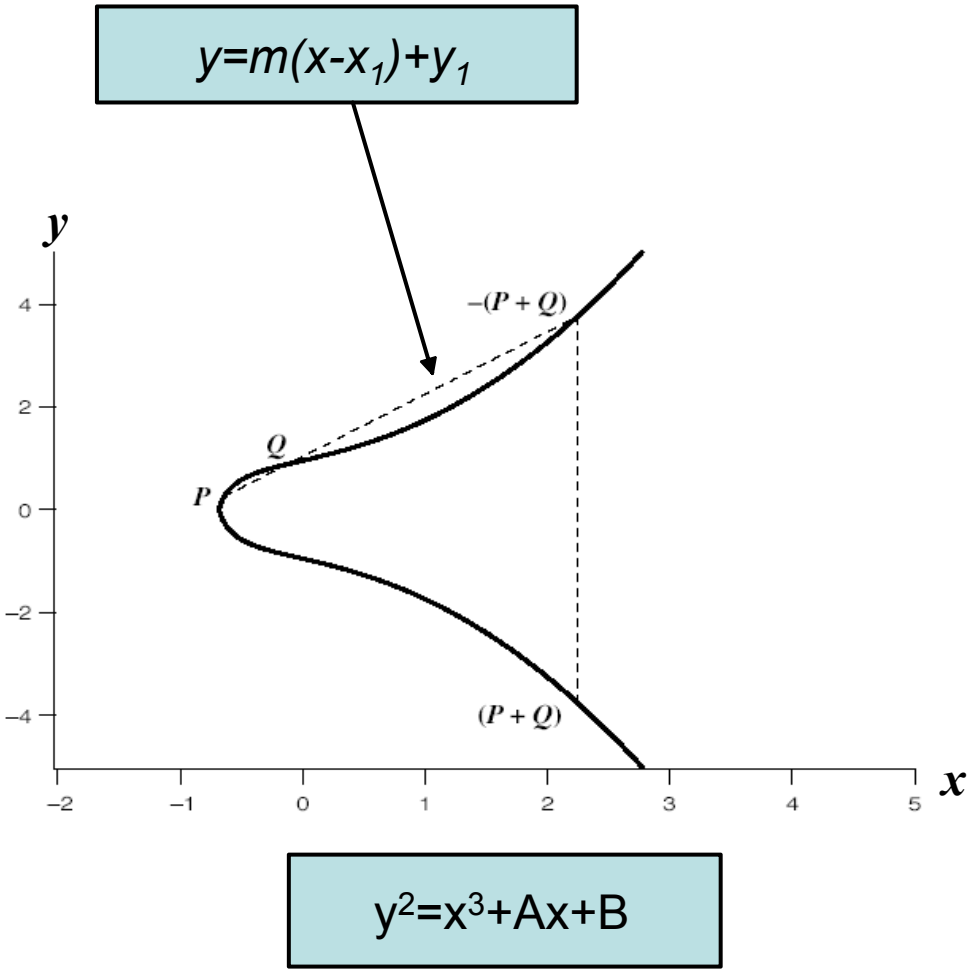
  E: $y^2 = x^3 - x + 1$

- If P_1 and P_2 are on E, we can define

  $P_3 = P_1 + P_2$

  as shown in picture

Addition in Affine Co-ordinates



$$P = (x_1, y_1), Q = (x_2, y_2)$$

$$R = (P + Q) = (x_3, y_3)$$

- Chords and tangents

Doubling of a point

- Let, P=Q

$$2y\frac{dy}{dx} = 3x^2 + A$$

$$\Rightarrow m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

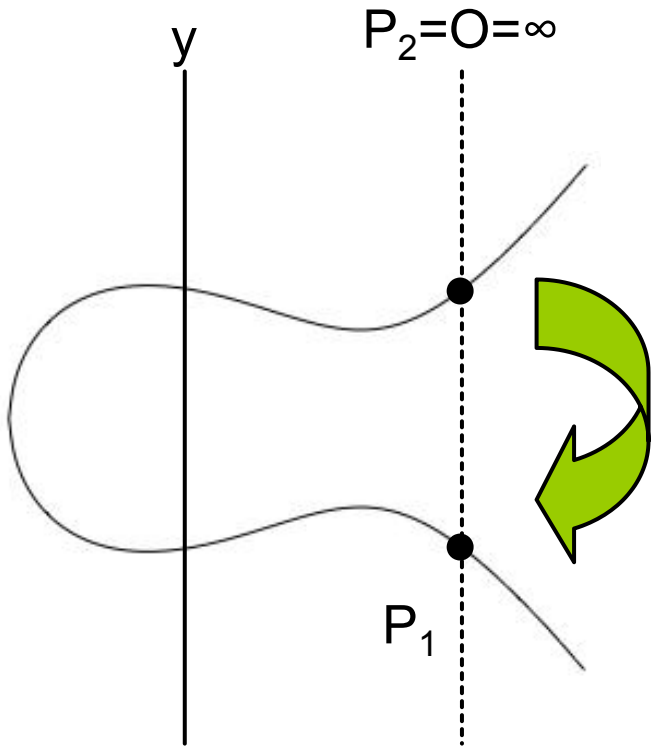
$$If, y_1 \neq 0 \text{ (since then } P_1 + P_2 = \infty\text{):}$$

$$\therefore 0 = x^3 - m^2x^2 + \ldots$$

$$\Rightarrow x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$$

- What happens when $P_2 = \infty = \boldsymbol{O}$?

reflection



$P_1=P_1+O=P_1$

Sum of two points

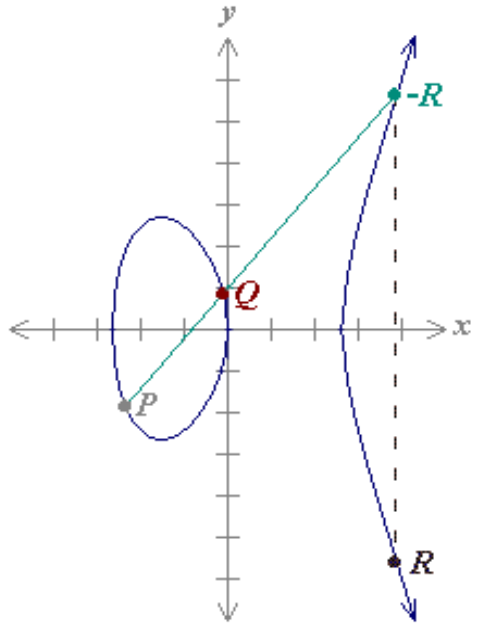
Define for two points ***P* (x_1,y_1)** and ***Q* (x_2,y_2)** in the Elliptic curve

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \; for\_ x_1 \neq x_2 \\ \dfrac{3x_1^{\,2} + a}{2y_1} \; for\_ x_1 = x_2 \end{cases}$$

Then ***P+Q*** is given by ***R*(x_3,y_3)** :

$$x_3 = \lambda - x_1 - x_2$$

$$y_3 = \lambda(x_3 - x_1) + y_1$$



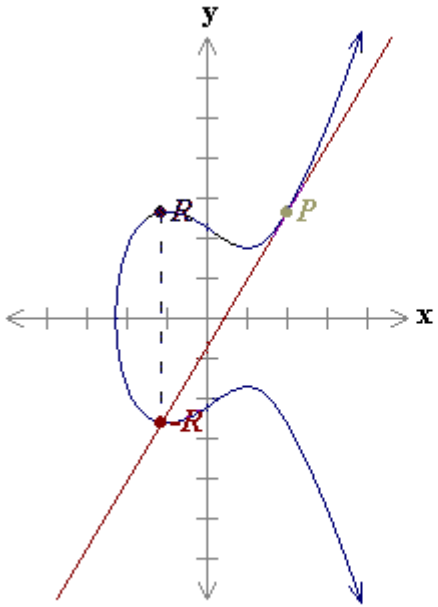
P (-2.35, -1.86)
Q (-0.1, 0.836)
-R (3.89, 5.62)
R (3.89, -5.62)

P + *Q* = *R* = (3.89, -5.62).

$y^2 = x^3 - 7x$

Point at infinity ***O***

P+P = 2P



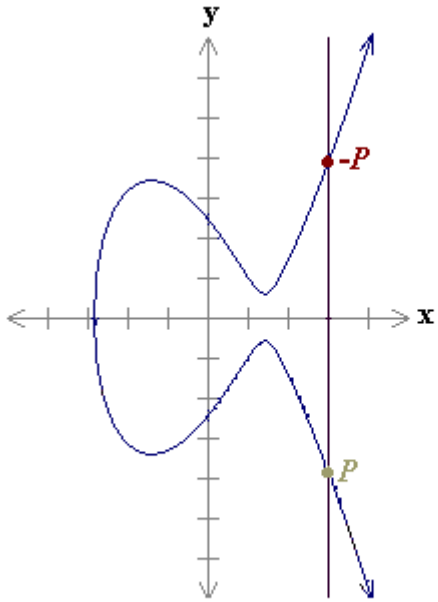
$y^2 = x^3 - 3x + 5$

P (2, 2.65)

-R (-1.11, -2.64)

R (-1.11, 2.64)

$2P = R = (-1.11, 2.64)$.



$P + (-P) = O$

$y^2 = x^3 - 6x + 6$

As a result of the above case ***P=O+P***

***O* is called the additive identity of the elliptic curve group.**

Hence all elliptic curves have an additive identity ***O***.

*** What is -P ?

- $y^2 = x^3 + ax + b$
- $P = (x_1, y_1)$
- What is -P ? Is $-P = (x_1, -y_1)$?

- Yes. But this works only for $y^2 = x^3 + ax + b$.
- For $$y^2 + a_1xy + a_3y = x^2 + a_2x^2 + a_4x + a_6$$
- $-P = (x_1, -a_1x_1-a_3-y_1)$

Motivation

- over F_3

$$Y^2Z + 2XYZ + YZ^2 = X^3 - XZ^2 + 7Z^3$$

$$has\ a\ solution\ (1, 2, 1)$$

- Note that (0, 1, 0) is a solution.
- Important Point 1 : We do not say (0, 0, 0) is a solution of the Weierstrass equation.

homogeneous vs affine

- Important Point 2 : We treat (1, 2, 1) ~ (2, 1, 2), i.e. consider them to be identical and call it a point of the curve given by the Weierstrass equation.

$$5^2 + 12^2 = 13^2 \qquad 10^2 + 24^2 = 26^2$$

$$\left(\frac{5}{13}\right)^2 + \left(\frac{12}{13}\right)^2 = 1, \quad \left(\frac{10}{26}\right)^2 + \left(\frac{24}{26}\right)^2 = 1$$

$$X^2 + Y^2 = Z^2 \Leftrightarrow \left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right)^2 = 1 : 1$$

Projective Co-ordinates

- Two-dimensional projective space P_K^2 over *K* is given by the equivalence classes of triples (x,y,z) with x,y z in K and at least one of x, y, z non-zero.
- Two triples (x_1,y_1,z_1) and (x_2,y_2,z_2) are said to be equivalent if there exists a non-zero element λ in K, st:
  - $(x_1,y_1,z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$
  - The equivalence class depends only on the ratios and hence is denoted by (x : y : z)

Projective Co-ordinates

- If z≠0, (x : y : z)=(x/z : y/z : 1)
- What if z=0? We obtain the point at infinity.
- The two dimensional affine plane over K:

$$A_K^2 = \{(x, y) \in K \times K\}$$

Hence using,

$$(x, y) \to (X : Y : 1)$$

$$\Rightarrow A_K^2 = P_K^2$$

Singularity

- For an elliptic curve $y^2 = f(x)$, define $F(x,y) = y^2 - F(x)$. A singularity of the EC is a point (x_0,y_0) such that:

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

$$or, 2y_0 = -f'(x_0) = 0$$

$$or, f(x_0) = f'(x_0)$$

$$\therefore \text{ f has a double root}$$

*** Singularity

- $y^2 = x^2(x-1)$ double roots $x=0$

- Let $x-1=s^2$
- $y^2 = (s^2+1)^2\,(s^2)$

- Hence $x=s^2+1$, $y=s(s^2+1)$

*** Singularity

- $y^2 = x^3$?
- $y = t^3,\ x = t^2$

If singular, then

- K = a field
- K(x, y) = K(t)

- For $y^2 = x^2(x-1)$, $x=s^2+1$, $y=s(s^2+1)$
- For $y^2 = x^3$, $y = t^3$, $x = t^2$

- For an elliptic curve, K(x, y) is never K(t).

Projective Form

$$E : Y^2Z + a_1XYZ + a_3YZ^2$$

$$= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

- has a point (0, 1, 0), point at infinity, denoted by ***O***.

If Characteristics of field is not 2, 3:

$$y^2 = f(x) = x^3 + Ax + B$$

Hence condition for no singularity is $4A^3+27B^2 \neq 0$

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

$$or, 2y_0 = -f'(x_0) = 0$$

$$or, f(x_0) = f'(x_0)$$

$\therefore$ f has a double root

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

For double roots,

$$x^3 + Ax + B = 3x^2 + A = 0$$

$$\Rightarrow x^2 = -A/3.$$

Also, $x^4 + Ax^2 + Bx = 0$,

$$\Rightarrow \frac{A^2}{9} - \frac{A^2}{3} + Bx = 0$$

$$\Rightarrow x = \frac{2A^2}{9B}$$

$$\Rightarrow 3\left(\frac{2A^2}{9B}\right)^2 + A = 0$$

$$\Rightarrow 4A^3 + 27B^2 = 0$$

Elliptic Curves in Characteristic 2

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- If a_1 is not 0, this reduces to the form:

$$y^2 + xy = x^3 + Ax^2 + B$$

- If a_1 is 0, the reduced form is:

$$y^2 + Ay = x^3 + Bx + C$$

- Note that the form cannot be:

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

EC over finite fields

- An elliptic curve may be defined over any finite field GF(q)
- For GF(2^m), the curve has a different form:

$$y^2 + xy = x^3 + ax^2 + b$$

where b is not 0

- Addition formulae are similar to those over the reals

Terminology

- Order of point P is the smallest integer r such that [r]P = ***O***.
- Order of the curve is the number of points of E(F), donated by #E(F).

Group Properties

- Let #E(F_q) denote the number of points on an elliptic curve $E(F_q)$, including $\boldsymbol{O}$
- Hasse bound: #E(F_q) = q + 1 - t, where

$$|t| < 2\ \mathrm{sqrt}(q)$$

- The group of points is either cyclic or a product of two cyclic groups

Scalar Multiplication

- *Scalar multiplication* is repeated group addition:

$$[c]P = P + \cdots + P \quad (c \text{ times})$$

- For all P in $E(F_q)$,

$$[n]P = \boldsymbol{O}$$

where $n = \#E(F_q)$

So it's an abelian group…

- group homomorphism ? isogeny, isogenous
- endomorphism, isomorphic
- Examples of endomorphisms are
- $[2] : E \rightarrow E,\ P \rightarrow [2]P,$
- $[n] : E \rightarrow E,\ P \rightarrow [n]P.$

Non-trivial Isogeny

$$E : y^2 = x^3 - x$$

$[i=\sqrt{-1}] : (x, y) \rightarrow (-x, iy)$

$[i=\sqrt{-1}]^2 = [i=\sqrt{-1}][i=\sqrt{-1}] : (x, y) \rightarrow (x, -y), \quad P \rightarrow -P$

here $i^2 = -1$

$6^2 = -1$ modulo 37

Called complex multiplication

*** Frobenius map

- GF(q), $q = p^k$
- F : GF(q) $\rightarrow$ GF(q)
- $F(x) = x^p$ for any x
- F is an isomorphism of GF(q). So F defines an isogeny for any elliptic curve over GF(q).

*** E[n]

- For any group G, any natural number n, $G[n] = \{g \mid g^n = 1\}$
- $E[n] = \{P \mid [n]P = 0\}$

$ 20, 000 + α

- 캐나다의 Certicom

Certicom ECC Challenge

Certicom Research

Since November 6, 1997

Latest update : November 10, 2009

NSA Suite B

- National Security Agency included Elliptic Curves in Suite B (for both unclassified and most classified information) on 16 February 2005.
- Unpublished Suite A is for highly sensitive and critical systems.
- The 256-bit elliptic curve (in FIPS 186-2) is sufficient for classified information up to the Secret level.
- The 384-bit elliptic curve (in FIPS 186-2) is necessary for Top Secret information.

참고문헌

- [1] G. Cornell, J. Silverman, and G. Stevens, A Survey of the Arithmetic Theory of Elliptic Curves (p. 17~40) in the book Modular Forms and Fermat's Last Theorem, Springer 1997
- [2] J. Silverman and J. Tate, Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, Springer 1992
- [3] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, 2nd ed., Graduate Texts in Mathematics, Springer 1993
- [4] I. Blake, G. Seroussi, and N. Smart, Elliptic Curves in Cryptography, London Mathematical Society Lecture Note Series, Cambridge University Press 1999
- [5] L. Washington, Elliptic Curves, Discrete Mathematics and Its Applications, Chapman & Hall/CRC 2003
- [6] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Springer 1986
- [7] J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Springer 1994
- [8] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers 1993

Silverman + Hoffstein etc

- NTRU Inc.
- fast
- Lattice-based
- public key system
- three Brown mathematics professors

- [9] RECOMMENDED ELLIPTIC CURVES FOR FEDERAL GOVERNMENT USE
- NIST recommends 15 elliptic curves (in FIPS 186-3)
- with prime fields for certain primes p of sizes 192, 224, 256, 384, and 521 bits.
- with binary fields for m equal 163, 233, 283, 409, and 571.
-
- In total 5 prime curves and ten binary curves.

The End