COMPLEX NUMBERS

JOHNEW ZHANG

$x^2 + 1 = 0.$

Definition 1. *The set of complex numbers is* $\mathbb{C} = \{x + 2y : x, y \in \mathbb{R}\}$*, where* i *is a symbol having the properties* $i^2 = -1$.

$\mathbb{Q}[\sqrt{2}]$.
We define addition and multiplication on $\mathbb{C}$.
$z = x + iy, w = u + iv \in \mathbb{C}$.
$z + w = (x + u) + i(y + v)$.
$z \cdot w = (x + iy)(u + iv) = (xu - yv) + i(xv + uy)$.

Theorem 1. $\mathbb{C}$ *is a field.*

If $z = x + iy \neq 0$, z has a multiplicative inverse.
$z^{-1} = \frac{1}{x+iy} = \frac{x-iy}{x^2+y^2}$.

Definition 2. *If* $z = x + iy \in \mathbb{C}$,
$x + iy$ *is the standard form of the* z.
(x, y) *are the Cartesian Coordinates.*
$x = Re(z)$ *is the real part of* z.
$y = Im(z)$ *is the imaginary part of* z.
$z = 0 + iy$ *is purely imaginary.*
Geometric representation of $\mathbb{C}$.
The function $f : \mathbb{C} \to \mathbb{R}$ *is a bijection.*
$x + iy \to (x, y)$
Check $(\mathbb{C}, +)$
Corresponds to parallelogram law of addition of vectors.

Exercise :
Write the standard form of $(1 + i)^{-2}$
$(1 + i)^{-2} = -\frac{1}{2}i$.

Definition 3. *If* $z = x + iy \in \mathbb{C}$*, the complex conjugate of* z *is* $\overline{z} = x - iy \in \mathbb{C}$.
The modulus (or obsolete value) of z *is* $|z| = \sqrt{x^2 + y^2}$.

Theorem 2. *Properties:*
(1) $\overline{z + w} = \overline{z} + \overline{w}$
(2) $\overline{zw} = \overline{z}\overline{w}$.

(3) $\overline{\overline{z}} = z$
(4) $z\overline{z} = x^2 + y^2 = |z|^2$.
(5) $z + \overline{z} = 2x$
(6) $z - \overline{z} = 2iy$.
(7) $z \neq 0, z^{-1} = \frac{\overline{z}}{|z|^2}$
(1) $|z| = 0 \iff z = 0$.
(2) $|\overline{z}| = |z|$.
(3) $|zw| = |z||w|$.
(4) $|z| \geq x, |z| \geq y$.
(5) Triangle Inequality
$|z + w| \leq |z| + |w|$.
(6) $|z - w| \geq ||z| - |w||$

1. Polar Coordinates

Let $z = x + 2y \in \mathbb{C}$.
Let $r = |z|, \theta =$ angle in radius.
(r, θ) polar coordinates of z.
$r \in \mathbb{R}, r \geq 0$.
$\theta \in \mathbb{R}, \theta$ is not unique $(\theta + 2k\pi, k \in \mathbb{Z})$
$0 = (0, \theta)$.
$z = r(\cos\theta + i\sin\theta) = rcis\theta$.
Converting $\rightarrow$ from polar to standard form.
$z = rcis(\theta), \rightarrow z = r\frac{\cos\theta}{x} + r\frac{r\sin\theta}{y}$.
From standard to polar form.
$z = x + iy \rightarrow z = |z|cis(), r = \sqrt{x^2 + y^2} = |z|, \theta / \tan\theta = \frac{x}{y}$.
and some quodrant as (x, y).

Examples
(1) Write $z = 5cis\frac{\pi}{4}$ in standard form.
(2) Write $-\sqrt{3} - i$ in polar form.

Theorem 3. *Let* $z_1 = r_1cis(\theta_1), z_2 = r_2cis(\theta_2)$ *be complex number.*
Then $z_1z_2 = r_1r_2cis(\theta_1 + \theta_2)$.

Proof. $z_1z_2 = (r_1\cos\theta_1 + ir_1\sin\theta_1)(r_2\cos\theta_2 + ir_2\sin\theta_2) = r_1r_2cis(\theta_1 + \theta_2)$. □

Corollary 1. *De Moivre's Theorem :*
$(rcis(\theta))^n = r^ncis(\theta n)$, $n \in \mathbb{N}, r \in \mathbb{R}, \theta \in \mathbb{R}$.

Write $(1 - \sqrt{3}i)^6$ in standard form.
Convert to polar form $(1 - \sqrt{3}i) = 2cis(-\frac{\pi}{3})$.

$(1-\sqrt{3}i)^6 = (2cis(-\frac{\pi}{3}))^6 = 2^6$.

Theorem 4. *Roots of Complex Numbers :*
Let $z = r_i cis(\theta), n \in \mathbb{N}$. $(w \in \mathbb{C}, w^n = z)$
Then the nth complex root of z are $r^{\frac{1}{n}} cis(\frac{\theta+2k\pi}{n}), k = 0, 1 \ldots n-1$.

Find the standard form of $1^{\frac{1}{4}}$.
Solve $z^4 + z^2 + 1 = 0$, Let $w = z^2$.
$w^2 + w + 1 = 0$. $w = \frac{-1\pm\sqrt{3}i}{2}$

Exponential Form
Define the function : $\mathbb{R} \to \mathbb{C}$
$\theta \to \cos\theta + i\sin\theta = e^{i\pi}$.
Why exponential?
(1) $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$
(2) $(e^{i\theta})^n = e^{in\theta}, n \in \mathbb{N}$.
(3) $\frac{de^{i\theta}}{d\theta} = ie^{i\theta}$.

(1) When $z \cdot \overline{z} = 1$?

2. Elliptic Curve

Simple Answer
Solution to an equation of the form $y^2 = x^3 + ax + b$, where a and b are given (in come field).$(27b^2 + 4a^3 \neq 0)$

$F = \mathbb{R}$.
Example: $y^2 = x^3 + 1$.
Elliptic curves are groups.
Rule for adding points
Example : Let $C : y^2 = x^3 + 1$.
Suppose you pick two points on the elliptic curve, p and q.
Rule 1: $p = q$, then we pick the tangent line of p.
We need to add a point O, which is an all vertical lines. Reflection of O is O.
Fact : This operation makes the points on the curve (along with O) into a group, with O as the identity.
For all points p and q, $p + q = q + p$.
(Abelian group)
1) $p + O = p$ for all p on C.
2)For every p on the curve, there is a -p such that $p + (-p) = O$.
So $-(x, y) = (x, -y)$.
$p + (q + r) = (p + q) + r$.
If p and q have rational coordinates, then the line joining p and q has rational coefficient.

So the equation $x^3 + 1 = (mx + b)^2$.

Then $x^3 -$ polynomial in$\mathbb{Q}[x] = 0$.

Since the x-coordinates of p and q are rational the third point must have a rational x-coordinate.

Since $y = mx + b$, the y-coordinate is rational and same for the flip.

If p and q have coefficients in any field F, so does $p + q$.

Example : On $y^2 = x^3 + 1$, calculate $2(2, -3)$

$(0, -1)$.

Interpret tangents as double intersections.

Inflection points : interpret as triple intersection.

2.1. **Elliptic Curve Brief Conclusion.** Elliptic Curve is the solution to an equation of the form $y^2 = x^3 + ax + b$, where a and b are give in some field $(27b^2 + 4a^3 \neq 0)$

Then let's define some properties.

1. Rule of adding points

Suppose we pick up two points on the elliptic curve, p and q.

$p + q = c$: c is the reflection of the other solution of the line (pass p and q) and the curves.

Rule 1 : $p = q$, then we pick the tangent line of p.

Rule 2 : If the tangent line is vertical. We need to add a point O, which is all vertical lines. Reflection of O is O.

Fact : This operation makes the points on the curve (along with O) into a group, with O as the identity.

For all points p and q, $p + q = q + p$

$p + O = p$

$p + (-p) = O$

$p + (q + r) = (p + q) + r$

for a point $(x, y) = -(x, -y)$

Above all is a brief description of elliptic curves.

2.2. **Application of Elliptic Curve.** Consider this field, $\mathbb{Z}_p$. p is a prime number.

We can actually find all the point on $y^2 = x^3 + ax + b$, such that $27b^2 + 4a^3 \neq 0$.

What can those points be used for?

With an elliptic curve C over a finite field.

Consider Diffie-Helmon Key exchange on $\mathbb{Z}_p$, it also applies to the elliptic curve.

Suppose Alice and Bod want to agree on a common secret

1) Alice and Bob select a prime p and an elliptic curve C over $\mathbb{Z}_p$, and a point Q on C.

2) Alice choose a, and make aQ public

3) Bob choose b, and make bQ public. $(a, b \geq 2$ are integers)

4) Common secret : abQ.

For a third person, to get the key, he has to solve the ECDLP.

Given an elliptic curve C over $\mathbb{Z}_p$, a point Q and the point aQ and find a.

However this process is hard.