Fabcoin crypto crash course

Elliptic curve preliminaries

Todor Milev
FA Enterprise System, Inc.

Spring 2019

Review of modular arithmetic ($\mathbb{Z}/n\mathbb{Z}$)

Definition (Modular arithmetic notation)

Let $n \geq 0$. If a, b have same remainder when divided by n, we say that:

$$a \equiv b \mod n$$

Every number is equivalent $\mod n$ to one lying between 0 and $n-1$:

Example

$10 \equiv 3 \mod 7$	$10 = 7 \cdot 1 + 3$ has remainder 3 when div. by 7.
$15 \equiv 0 \mod 5$	$15 = 3 \cdot 5 + 0$ has remainder 0 when div. by 5.
$-2 \equiv 1 \mod 3$	$-2 = 3 \cdot (-1) + 1$ has remainder 1 when div. by 3

Finding the number between 0 and $n-1$ as described above is called "reducing a number modulo n".

Lemma

Let $a_1 \equiv a_2 \mod n$ *and* $b_1 \equiv b_2 \mod n$*.*

- $a_1 \pm b_1 \equiv a_2 \pm b_2 \mod n$ *(Mod. arithm. respects addition).*
- $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod n$ *(Mod. arithm. respects multiplication).*

Proof. [Mult. respected].

Since $a_1 \equiv a_2 \mod n \Rightarrow a_1 = n \cdot p + a_2$ for some p.
Since $b_1 \equiv b_2 \mod n \Rightarrow b_1 = n \cdot q + b_2$ for some q.

$$\begin{aligned} a_1 \cdot b_1 &= (n \cdot p + a_2) \cdot (n \cdot q + b_2) \\ &= n^2(p+q) + n(b_2 + a_2) + b_2 + a_2 \\ &\equiv b_2 + a_2 \mod n \end{aligned}$$

□

Example

Reduce $2030 \cdot 201800003 \mod 2018$.

$$\begin{aligned} 2030 &= 2018 + 12 \equiv 12 && \mod 2018 \\ 201800003 &= 20180000 + 3 = 2018 \cdot 10^4 + 3 \equiv 3 && \mod 2018 \\ 2030 \cdot 201800003 &\equiv 12 \cdot 3 = 36 && \mod 2018 \end{aligned}$$

Definition (Group, mathematics)

A group $\mathcal{G}$ is a set equipped with operation $\cdot$ with $a \cdot b \in \mathcal{G}$ so that:

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for every $a, b, c \in \mathcal{G}$. (Associativity)
- There exists $e \in \mathcal{G}$ with $e \cdot a = a \cdot e = a$ for every $a \in \mathcal{G}$. (Identity)
- For every a exists $b \in \mathcal{G}$ s.t. $a \cdot b = e$. Write $b = a^{-1}$. (Inverse)

Definition (Abelian (commutative) group)

The group is called abelian (commutative) if in addition:

- $a \cdot b = b \cdot a$ for all $a, b \in \mathcal{G}$.

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- Exists e s.t. $e \cdot a = a \cdot e = a$.
- Given a exists b s.t. $a \cdot b = e$.
- $a \cdot b = b \cdot a$.

Example

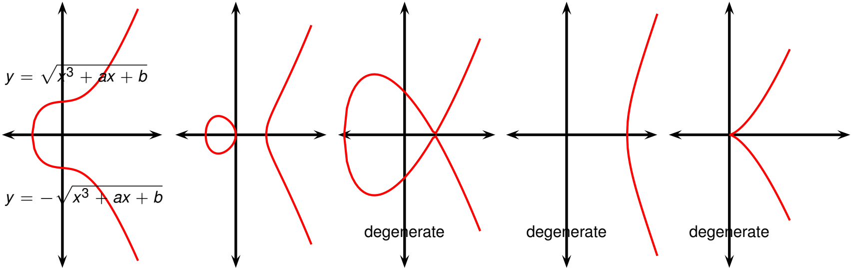
Take $G = \mathbb{Z}$, define $a \cdot b = a + b$.

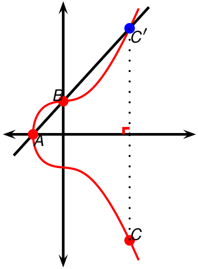
- $(a + b) + c = a + (b + c)$.
- Set $e = 0$. Then $0 + a = a + 0 = a$.
- For every a, take $b = -a$. Then $a + b = a + (-a) = 0 = e$.
- $a + b = b + a$ for all a, b.

Definition

The set of points $\{(x, y)\}$ for which
$$y^2 = x^3 + ax + b$$
is called an elliptic curve (possibly degenerate).

- Precise definition of all curves that are “elliptic”: outside our scope.
- Precise definition of “degenerate”: outside our scope.
- We do not fix the number types of x, y: possibly $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, \dots$.
- Over $\mathbb{R}$, graph of elliptic has five types:





Definition (Elliptic curve group law)

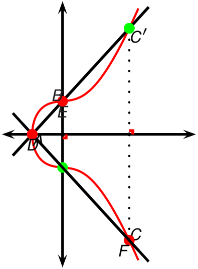
- If line through A, B non-vertical, define $A \cdot B = C$.
- Define $A \cdot A$ similarly but use the tangent through A in place of the line through A, B.
- If line through A, B vertical, define $A \cdot B = \mathbf{1}$.
- Define $\mathbf{1} \cdot A = A \cdot \mathbf{1} = A$ for all A.

Let $A = (x_A, y_A)$, $B = (x_B, y_B)$ - points on non-degenerate elliptic curve:

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

- Let C' be intersection of line through A, B with the elliptic curve.
- Unless the line through A, B is vertical, such C' exists.
- Let C be the reflection of C' across the x axis.

WARNING. Many authors use $+$ in place of $\cdot$ and $\mathbf{0}$ in place of $\mathbf{1}$.



Definition (Elliptic curve group law)

- If line through A, B non-vertical, define $A \cdot B = C$.
- Define $A \cdot A$ similarly but use the tangent through A in place of the line through A, B.
- If line through A, B vertical, define $A \cdot B = \mathbf{1}$.
- Define $\mathbf{1} \cdot A = A \cdot \mathbf{1} = A$ for all A.

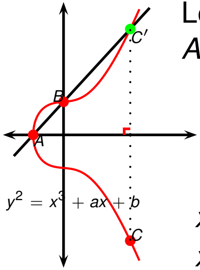
- $\cdot$ turns the points on the curve into a group.
- In particular: why does the associative law hold:

$$\underbrace{\left(\underbrace{A \cdot B}_{=C}\right) \cdot D}_{=E} \stackrel{?}{=} \underbrace{A \cdot \left(\underbrace{B \cdot D}_{=F}\right)}_{=E}$$

- I.e., why does AF intersect DC on a point on the curve?
- When we derive formulas for this construction, we can algebraically prove the above.
- However our proof will appear an algebraic coincidence/miracle.
- An answer to why this all works is beyond current scope.

Niels Henrik Abel (1802-1829), pioneer of modern algebra and elliptic functions. Abelian groups are named after him.

Karl Weierstrass (1815-1897), pioneer of elliptic functions. The definition of elliptic curve given in our text is sometimes called "Weierstrass normal form".



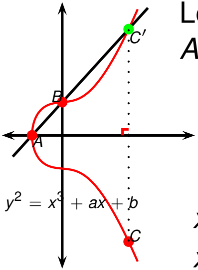
Let $A = (x_A, y_A)$, $B = (x_B, y_B)$. Let s be the slope of line AB. Let x_C, y_C be the unknown coordinates of C.

$$
\begin{aligned}
s &= \text{line slope}\\
\frac{-y - y_A}{x - x_A} &= s\\
-y &= s(x - x_A) + y_A && (*)\\
x^3 + ax + b &= (-y)^2 && (**)\\
x^3 + ax + b &= (s(x - x_A) + y_A)^2
\end{aligned}
$$

$$
\begin{array}{rcl}
x^3 + ax + b - \left(s^2(x - x_A)^2 + 2sy_A(x - x_A) + y_A^2\right) &=& 0\\
x^3 - s^2x^2 + 2s^2xx_A + s^2x_A^2 - 2sy_Ax + 2sy_Ax_A - y_A^2 + ax + b &=& 0\\
x^3 - x^2s^2 + x(2s^2x_A - 2sy_A + a) + s^2x_A^2 + 2sy_Ax_A - y_A^2 + b &=& 0
\end{array}
$$

Setting $x = x_A$ solves $(*)$, $(**)$. Similarly setting $x = x_B$ solves $(*)$, $(**)$. Since $(**)$ is cubic $\Rightarrow$ its unknown 3^{rd} root is x_C. By Vieta's formulas,

$$
\begin{array}{rcl}
x_A + x_B + x_C &=& s^2\\
x_C &=& s^2 - x_A - x_B\\
y_C &=& -s(x_C - x_A) - y_A
\end{array}
$$



Let $A = (x_A, y_A)$, $B = (x_B, y_B)$. Let s be the slope of line AB. Let x_C, y_C be the unknown coordinates of C.

$$s = \text{line slope}$$

$$\frac{-y - y_A}{x - x_A} = s$$

$$\begin{array}{rcl|l} -y &=& s(x - x_A) + y_A & (*) \\ x^3 + ax + b &=& (-y)^2 & (**) \\ x^3 + ax + b &=& (s(x - x_A) + y_A)^2 & \end{array}$$

$$\begin{array}{rcl|l}
x_A + x_B + x_C &=& s^2 & \\
x_C &=& s^2 - x_A - x_B & \\
y_C &=& -s(x_C - x_A) - y_A & \\
s &=& \dfrac{y_B - y_A}{x_B - x_A} & \text{if } x_A \neq x_B \\
s &=& \dfrac{\mathrm{d}y}{\mathrm{d}x} = \dfrac{3x_A^2 + a}{2y_A} & \text{if } x_A = x_B, y_A = y_B \\
y^2 &=& x^3 + ax + b & \text{apply d} \\
2y\mathrm{d}y &=& 3x^2\mathrm{d}x + a\mathrm{d}x & \\
\dfrac{\mathrm{d}y}{\mathrm{d}x} &=& \dfrac{3x^2 + a}{2y} &
\end{array}$$

(Elliptic curve group law, algebraic definition)

Let $(x_A, y_A), (x_B, y_B)$ *be two points on the elliptic curve.*

- *Suppose* $y_A \neq -y_B$. *Define:*

$$
\left.
\begin{array}{rcl}
s & = & \begin{cases} \dfrac{y_B - y_A}{x_B - x_A} & \text{if } x_A \neq x_B \\[2ex] \dfrac{3x_A^2 + a}{2y_A} & \text{if } x_A = x_B, y_A = y_B \end{cases} \\
x_C & = & s^2 - x_A - x_B \\
y_C & = & -s(x_C - x_A) - y_A
\end{array}
\right|
\begin{array}{l}
\\ \\ \\
\text{if } y_A \neq -y_B \\
\text{if } y_A \neq -y_B
\end{array}
$$

- *If* $y_A = -y_B$, *define* $(x_C, y_C) = \mathbf{1}$.
- *Define* $\mathbf{1} \cdot (x_A, y_A) = (x_A, y_A)$.
- *Define* $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$.

- Above we assumed working over $\mathbb{C}$ or $\mathbb{R}$.
- However, formulas are well-defined over arbitrary field.
- A field is a set where the operations $+, -, *, /$ are defined and follow the basic arithmetic rules.
- Full definition of field: outside of present scope.

Product: $s = \begin{cases} \dfrac{y_B - y_A}{x_B - x_A} & \text{if } x_A \neq x_B \\ \dfrac{3x_A^2 + a}{2y_A} & \text{if } A = B \end{cases}$, $\begin{array}{rcl} y_C & = & -s(x_C - x_A) - y_A \\ x_C & = & s^2 - x_A - x_B \end{array}$

Example

Let $y^2 = x^3 - x + 1$. Show $g = (3,5)$ is a point on the curve. Compute $g^2 = g \cdot g$ and $g^3 = g \cdot g \cdot g$.

- That the point is on the curve can be seen from: $25 = 5^2 \stackrel{?}{=} 3^3 - 3 + 1 = 25$
- $$\begin{array}{rcl} g^2 & = & (3,5)\cdot(3,5) = \left(-\frac{19}{25}, \frac{103}{125}\right) \\ s_2 & = & \dfrac{3\cdot 3^2 - 1}{2\cdot 5} = \dfrac{13}{5} \\ x_2 & = & \left(\dfrac{13}{5}\right)^2 - 3 - 3 = -\dfrac{19}{25} \\ y_2 & = & -\dfrac{13}{5}(x_2 - 3) - 5 = \dfrac{103}{125} \end{array}$$

$$\text{Product: } s = \begin{cases} \dfrac{y_B - y_A}{x_B - x_A} & \text{if } x_A \neq x_B \\ \dfrac{3x_A^2 + a}{2y_A} & \text{if } A = B \end{cases}, \quad \begin{array}{rcl} y_C & = & -s(x_C - x_A) - y_A \\ x_C & = & s^2 - x_A - x_B \end{array}$$

Example

Let $y^2 = x^3 - x + 1$. Show $g = (3, 5)$ is a point on the curve. Compute $g^2 = g \cdot g$ and $g^3 = g \cdot g \cdot g$.

- $$\begin{array}{rcl} g^3 & = & g^2 \cdot g = \left(-\frac{19}{25}, \frac{103}{125}\right) \cdot (3, 5) = \left(-\frac{223}{784}, -\frac{28414}{46225}\right) \\ s_3 & = & \frac{\frac{103}{125} - 5}{-\frac{19}{25} - 3} = -\frac{261}{140} \\ x_3 & = & s_3^2 - \left(-\frac{87}{64}\right) - 2 = -\frac{223}{784} \\ y_3 & = & -\frac{28414}{46225} \end{array}$$