

$$A \circ B = C$$

$$\underline{(A \circ B) \circ C = A \circ (B \circ C)}$$

$$A \circ \perp = A$$

$$\perp \circ A = A$$

Fortgeschrittene Techniken der Kryptographie

$$\hat{A} \circ A = \perp / A \circ \hat{A} = \perp$$

Jürgen Fuß

$$\underbrace{(A \circ \perp) \circ \hat{A}}_{A \circ \hat{A}} = A \circ (\perp \circ \hat{A})$$

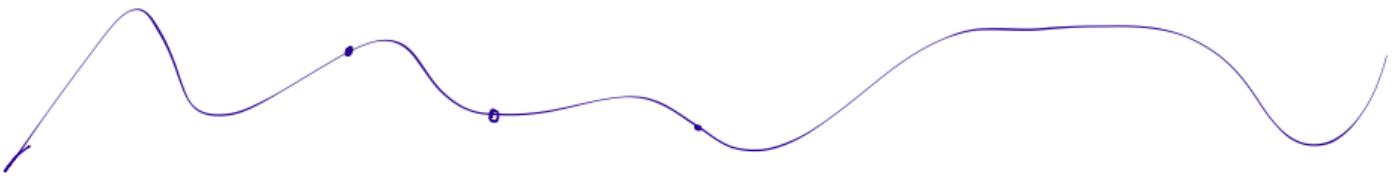
Episode 8: Elliptische Kurven

HAGENBERG | LINZ | STEYR | WELS



UNIVERSITY
OF APPLIED SCIENCES
UPPER AUSTRIA

Elliptische Kurven über \mathbb{R}



Elliptische Kurve

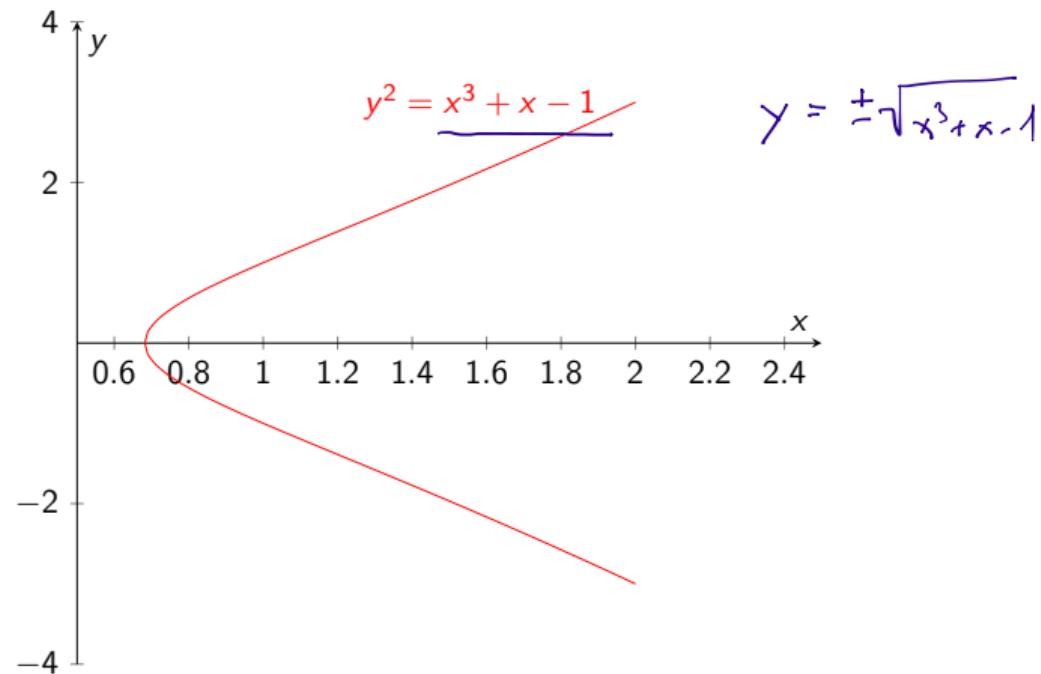
Definition

Es seien $a, b \in \mathbb{R}$ so, dass $4a^3 + 27b^2 \neq 0$. Dann ist

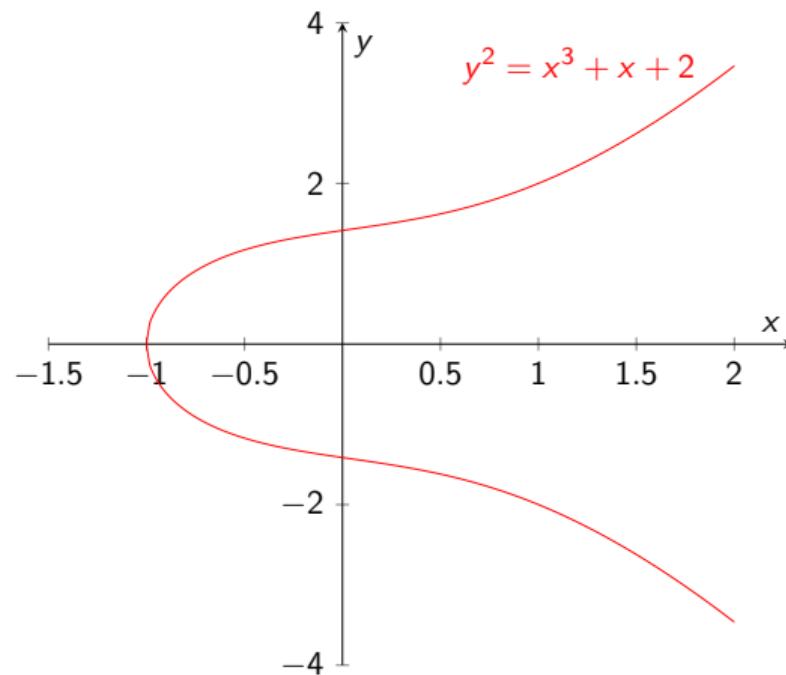
$$\mathcal{E} := \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$$

eine **elliptische Kurve über \mathbb{R}** .

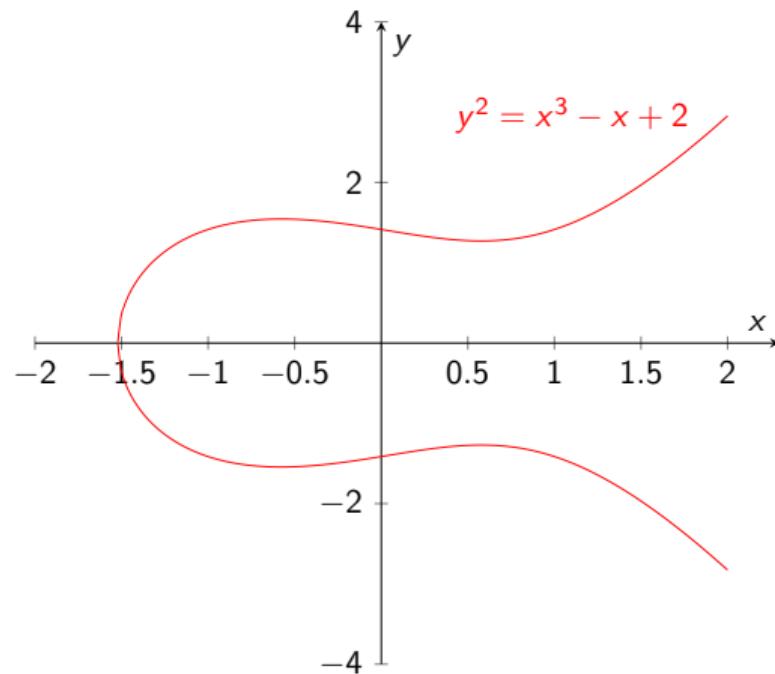
Beispiele ($a = 1$, $b = -1$)



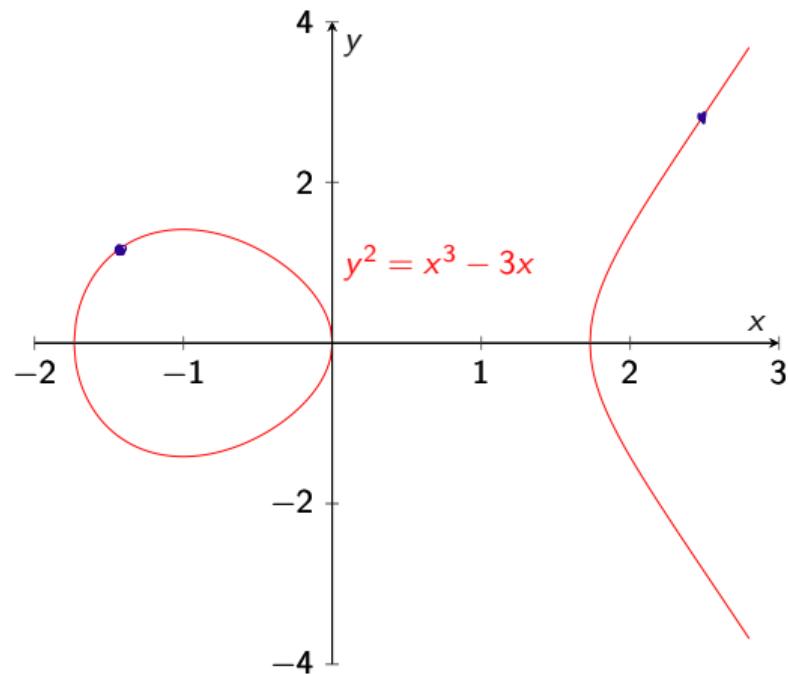
Beispiele ($a = 1$, $b = 2$)



Beispiele ($a = -1$, $b = 2$)



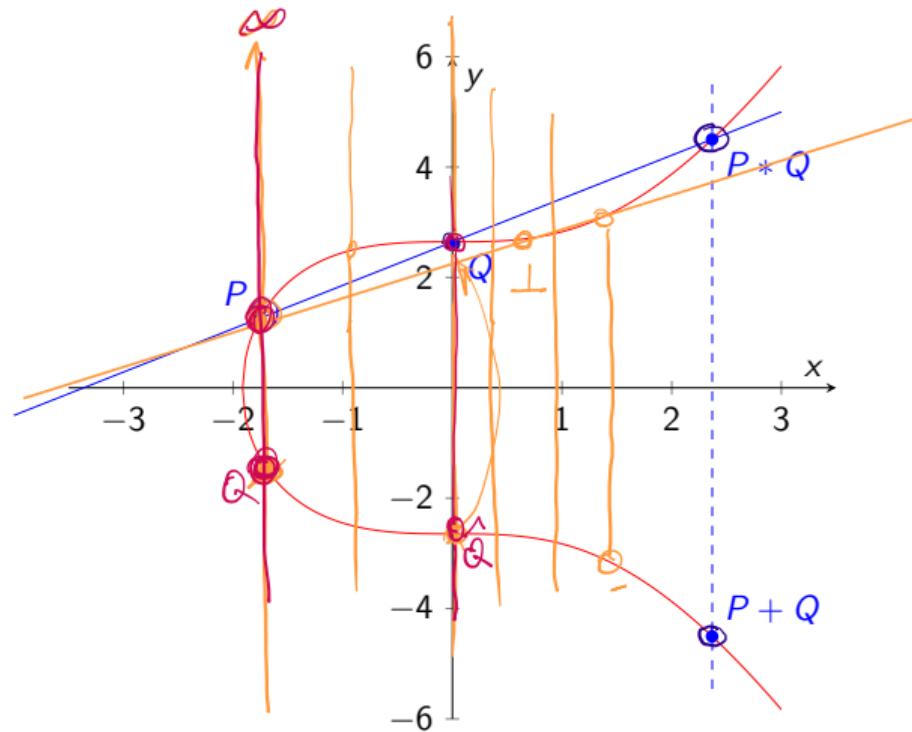
Beispiele ($a = -3$, $b = 0$)



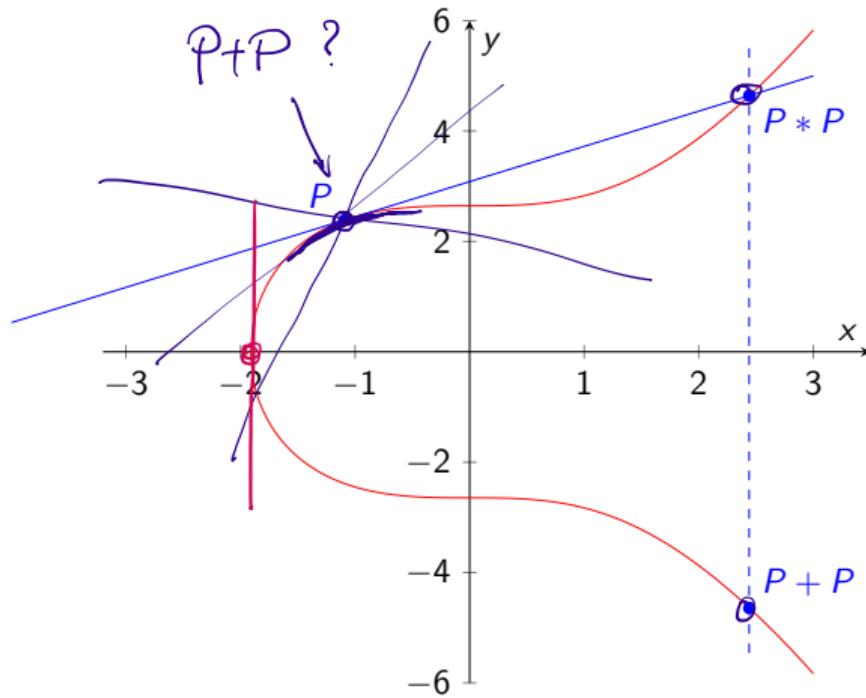
Verknüpfung von Punkten einer elliptischen Kurven über \mathbb{R}
Aus elliptischen Kurven werden Gruppen

$P + Q$ (Addition)

$$\hat{P} + \hat{P} = \infty$$



$P + P$ (Verdopplung)



Um schließlich wirklich eine Gruppe zu erhalten, fehlt noch ein neutrales Element. Dieses muss „dazuerfunden“ werden. Es wird üblicherweise (auch wenn das zunächst verwirrend ist) mit dem Symbol ∞ bezeichnet, ein Punkt, der keine Koordinaten besitzt.

Elliptische Kurven als Gruppen

Definition

Es sei \mathcal{E} eine elliptische Kurve. Wir definieren für alle $P, Q \in \mathcal{E}$:

1. $-\infty := \infty$ und $P + \infty := \infty + P := P$. (Damit wird ∞ zum neutralen Element.)
2. Ist $P = (x, y)$, dann sei $-P := (x, -y)$.
3. Ist $Q = -P$, dann sei $P + Q := \infty$.
4. $P + P := -(P * P)$, wobei $P * P$ der andere Schnittpunkt der Tangente an \mathcal{E} in P ist.
5. Ist $P \neq \pm Q$, dann sei $P + Q := -(P * Q)$, wobei $P * Q$ der dritte Schnittpunkt der Geraden durch P und Q mit \mathcal{E} ist.

Satz (Teil 1: Sonderfälle)

Es seien $\mathcal{E} : y^2 = x^3 + ax + b$ eine elliptische Kurve über \mathbb{R} und $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ zwei Punkte auf \mathcal{E} . Dann lassen sich die Koordinaten (x_3, y_3) von

$$R := P + Q$$

nach folgenden Formeln berechnen:

- ▶ Falls $P = -Q$, dann ist $R = \infty$.
- ▶ Ist $P = \infty$, dann ist $P + Q := Q$.
- ▶ Ist $Q = \infty$, dann ist $P + Q := P$.

Formeln zur Addition und Verdopplung

Satz (Teil 2: Addition)

Es seien $\mathcal{E} : y^2 = x^3 + ax + b$ eine elliptische Kurve über \mathbb{R} und $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ zwei Punkte auf \mathcal{E} . Dann lassen sich die Koordinaten (x_3, y_3) von

$$R := P + Q$$

nach folgenden Formeln berechnen:

- Falls $P \neq Q$, dann ist

$$\begin{aligned} x_3 &= k^2 - x_1 - x_2, \\ y_3 &= -y_1 + k(x_1 - x_3), \end{aligned} \quad \text{wobei } k := \frac{y_2 - y_1}{x_2 - x_1}. \quad (1)$$

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

P(x₁/y₁)

Q(x₂/y₂)

$$g: \boxed{y = kx + d}$$

$$\Rightarrow y = kx + y_1 - kx_1$$

$$\begin{aligned} y_1 &= kx_1 + d \\ y_2 &= kx_2 + d \\ y_1 - y_2 &= kx_1 - kx_2 \\ y_1 - y_2 &= k(x_1 - x_2) \\ k &= \frac{y_1 - y_2}{x_1 - x_2} \end{aligned}$$

$$\boxed{y^2 = x^3 + ax + b}$$

$$(kx+d)^2 = x^3 + ax + b$$

$$k^2x^2 + 2kxd + d^2 = x^3 + ax + b$$

$$x^3 - k^2x^2 + (a - 2kd)x + b - d^2 = 0$$

$$\begin{aligned} x^3 - k^2x^2 + (a - 2kd)x + b - d^2 &= (x - x_1)(x - x_2)(x - x_3) \\ -k^2x^2 &= (x^2 - x_1x - x_2x + x_1x_2)(x - x_3) \\ &= x^3 - x_1x^2 - x_2x^2 + x_1x_2x + x_1x_3x + x_2x_3x \\ &= x^3 + (x_1 - x_2 - x_3)x^2 + \dots \end{aligned}$$

$$\begin{aligned} -k^2 &= -x_1 - x_2 - x_3 \\ \boxed{x_3 = \frac{-k^2 - x_1 - x_2}{}} & \quad \boxed{k = \frac{y_1 - y_2}{x_1 - x_2}} \end{aligned}$$

$$y_3 = k \cdot x_3 + y_1 - kx_1 = \boxed{y_1 + k(x_3 - x_1)}$$

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

$$t: y = kx + d$$

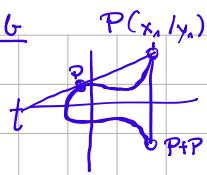
$$y = \pm \sqrt{x^3 + ax + b}$$

$$y' = \pm \frac{1}{2\sqrt{x^3 + ax + b}} \cdot (3x^2 + a)$$

$$y' = \frac{1}{\pm 2\sqrt{x^3 + ax + b}} \cdot (3x^2 + a)$$

$$\cancel{y'} = \frac{1}{2y} \cdot (3x^2 + a)$$

$$k = \frac{3x_1^2 + a}{2y_1}$$



Formeln zur Addition und Verdopplung

Satz (Teil 3: Verdopplung)

Es seien $\mathcal{E} : y^2 = x^3 + ax + b$ eine elliptische Kurve über \mathbb{R} und $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ zwei Punkte auf \mathcal{E} . Dann lassen sich die Koordinaten (x_3, y_3) von

$$R := P + Q$$

nach folgenden Formeln berechnen:

- Falls $P = Q$, dann ist

$$\begin{aligned} x_3 &= k^2 - 2x_1, \\ y_3 &= -y_1 + k(x_1 - x_3), \end{aligned} \quad] \quad (2)$$

wobei $k := \frac{3x_1^2 + a}{2y_1}$.

x_1
 ~~$-x_1$~~ ~~$-x_2$~~

Elliptische Kurven sind Gruppen

$$(A+B)+C = A+(B+C)$$

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

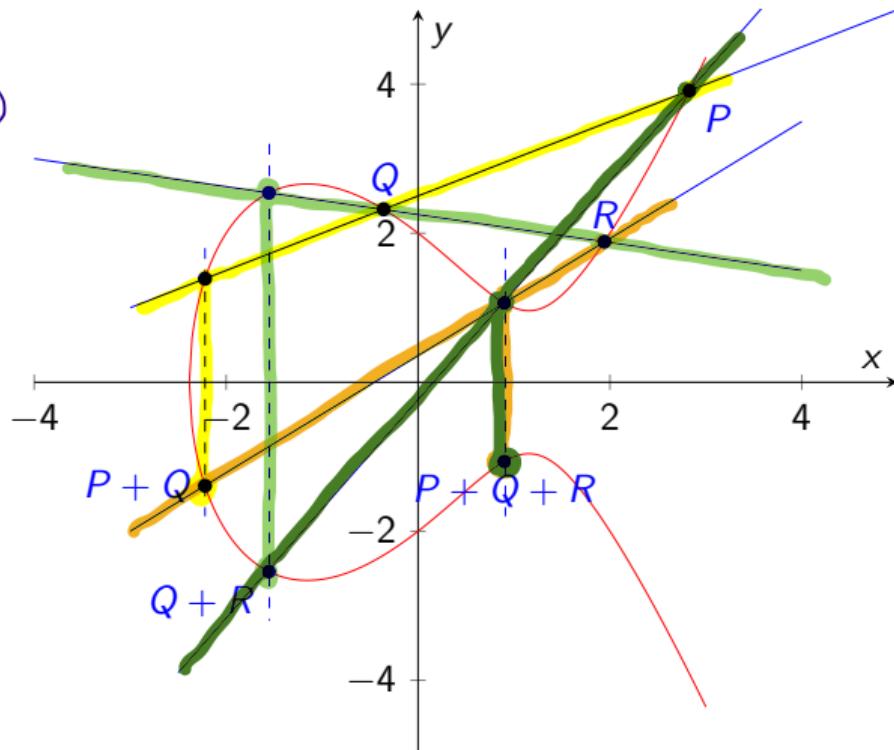
Satz

Ist \mathcal{E} eine elliptische Kurve, dann ist $(\mathcal{E}, +, \infty, -)$ eine abelsche Gruppe.

Die Abbildung rechts illustriert, dass

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

gilt.



Punktmultiplikation

Für kryptografische Anwendungen ist (z. B. DH) das Potenzieren in Gruppen von Interesse. Im Zusammenhang mit elliptischen Kurven ist dies das mehrfache Addieren eines Punktes zu sich selbst. Naheliegend ist, hier

$$\alpha \cdot P := \underbrace{P + P + \cdots + P}_{\alpha \text{ mal}}$$

zu definieren.

Definition (Punktmultiplikation auf elliptischen Kurven)

Es seien \mathcal{E} eine elliptische Kurve, $P \in \mathcal{E}$ und $\alpha \in \mathbb{Z}$. Dann sei

$$\alpha \cdot P := \begin{cases} \infty & , \text{ falls } \alpha = 0 \\ \underbrace{P + P + \cdots + P}_{\alpha \text{ mal}} & , \text{ falls } \alpha > 0 \text{ und} \\ (-\alpha) \cdot (-P) & , \text{ falls } \alpha < 0. \end{cases}$$

Double-&-Add

$$g^6 =$$

Effizient lassen sich **Punktmultiplikationen** durch Anwenden der Square-and-Multiply-Idee durchführen.

- ▶ Das Quadrieren entspricht nun einer Punktverdopplung,
- ▶ das Multiplizieren einer Punktaddition,
man könnte also von einer **Double-and-Add**-Methode sprechen.

$$\begin{array}{c} g \\ g^2 \\ g^4 \end{array} \geqslant g^6$$

$$\begin{array}{c} P \\ 2P \\ 4P \end{array} \geqslant 6P$$

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

$a = 1$
 $b = -1$

$P(2/-3)$

$P+P$

$Q(3/\sqrt{29})$

$$R\left(\sqrt{10} / \sqrt{\sqrt{10}^3 + \sqrt{10}-1}\right) \frac{3 \cdot 2^2 + 1}{2(-3)} = \frac{13}{-6} = -\frac{13}{6}$$

$-P = (2/3)$

$$(2/-3) + (2/3) = \infty$$

$$x_3 = b^2 - 2x_1$$

$$y_3 = -y_1 + b(x_1 - x_3)$$

$$b = \frac{3x_1^2 + a}{2x_1}$$

$$x_3 = \frac{169}{36} - 2 \cdot 2 \\ = \frac{25}{36}$$

$$y_3 = -(-3) + \left(-\frac{13}{6}\right) \cdot \left(2 - \frac{25}{36}\right)$$

$$y_3 = 3 + \left(-\frac{13}{6}\right) \cdot \frac{47}{36} \\ = \dots$$

$$\binom{2}{-3} + \binom{2}{3} \stackrel{!}{=} \infty$$

~~$\neq \binom{4}{0}$~~

$$(2/3) + \infty = (2/3)$$

$$\infty + \infty = \infty$$

$$\infty - \infty = \infty$$

$$(2/3) - \infty = (2/3)$$