Analytiquement. $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

$P + Q = R$.

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \pmod p \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod p \end{cases}$$

où λ est la pente de la droite PQ ou la pente de la tangente au pt. P (si on calcule $P+P$).

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \pmod p \text{ si } P \neq Q. \\ \dfrac{3x_1^2 + a}{2y_1} \pmod p \text{ si } P = Q. \end{cases}$$

§§5.2. PLD sur une courbe elliptique.

Théorème Sur une courbe elliptique C existe des sous-groupes cycliques.

Exemple. Soit C: $y^2 \equiv x^3 + 2x + 2 \pmod{17}$

$(C, +)$ est un groupe cyclique ici, et $\#C = 19$ premier $\Rightarrow$ chaque pt de C est primitif. Soit $P = (5,1)$.

On calcule $\langle P \rangle = \{P, 2P, 3P, \dots, 19P\}$

$2P = (6,3)$ $\quad 3P = (10,6), \dots, 18P = (5,16)$,

$19P = \mathcal{O}_\infty$ $\quad 20P = P + 19P = P + \mathcal{O}_\infty = P$.

$18P + P = \mathcal{O}_\infty$. (l'inverse de P est $18P$). ☒

Théorème (Hasse) une courbe elliptique C sur $\mathbb{Z}_p$ vérifie:

$$p + 1 - 2\sqrt{p} \leq \#C \leq p + 1 + 2\sqrt{p}$$