§§ 5.1. La loi de groupe sur une courbe elliptique.

• **Définition** C courbe elliptique sur $\mathbb{Z}_p$ $(p \geq 3)$ est l'ensemble des points $(x,y) \in \mathbb{Z}_p$ tq.

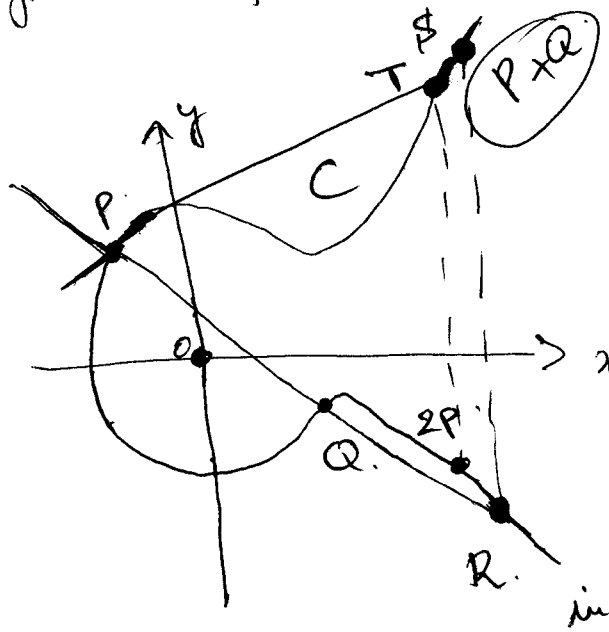
$$y^2 \equiv x^3 + ax + b \pmod p,$$

en plus d'un point O_∞ (à l'infini : jouant le rôle de l'élément neutre de la loi de groupe définie sur C).

où $a, b \in \mathbb{Z}_p$ avec le discriminant

$$\Delta = 4a^3 + 27 \cdot b^2 \not\equiv 0 \pmod p. \quad \square$$

Z **Remarque** ! (les dessins suivants sont dans $\mathbb{R}$ ou $\mathbb{C}$ pour faire manifester une courbe elliptique)



1) $P + Q = S$.
La droite (PQ) intersecte C en un pt. R dont on prend l'opposé S qui est P+Q.

2) La tangente au pt P intersecte C au pt T, dont on prend l'opposé qui est 2P.

Proposition. $(C, +)$ est un groupe commutatif avec l'élément neutre O_∞ et l'opposé de P est le pt $-P$ tq

$$P + (-P) = O_\infty.$$