Tutorial week #10

10 de dezembro de 2025 15:45

1) $P = (4,7)$ Is P a point in C over Z_{23}? And over $\mathbb{R}$?

$C: y^2 = x^3 - 5x + 5$

For P to be a point in C over Z_{23} then

$y^2 \equiv x^3 - 5x + 5 \pmod{23} \iff$

$\iff 7^2 \equiv 4^3 - 5\times 4 + 5 \pmod{23} \iff$

$\iff 49 \equiv 64 - 20 + 5 \pmod{2} \iff$

$\iff 49 \equiv 49 \pmod{23} \iff$

$\iff 3 \equiv 3 \pmod{23}$ //

$\therefore P$ is a point of C over Z_{23}

For P be port of C over $\mathbb{R}$ then:

$y^2 = x^3 - 5x + 5 \iff$

$\iff 7^2 = 4^3 - 5\times 4 + 5 \iff 49 = 64 - 20 + 5 \iff$

$\iff 49 = 49$ //

$\therefore P$ is a point of C over $\mathbb{R}$