Euler's φ-function

and the Euler-Fermat theorem

Definition

$\varphi(n)$ is the number of elements of $\mathbb{Z}_n^*$:

$$\varphi(n) = |\mathbb{Z}_n^*|$$

$5^4 = 625 \mod 12$
$= 52 \cdot 12 + 1$

Theorem

For all $a \in \mathbb{Z}_n^*$ (that means gcd(a, n) = 1)

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

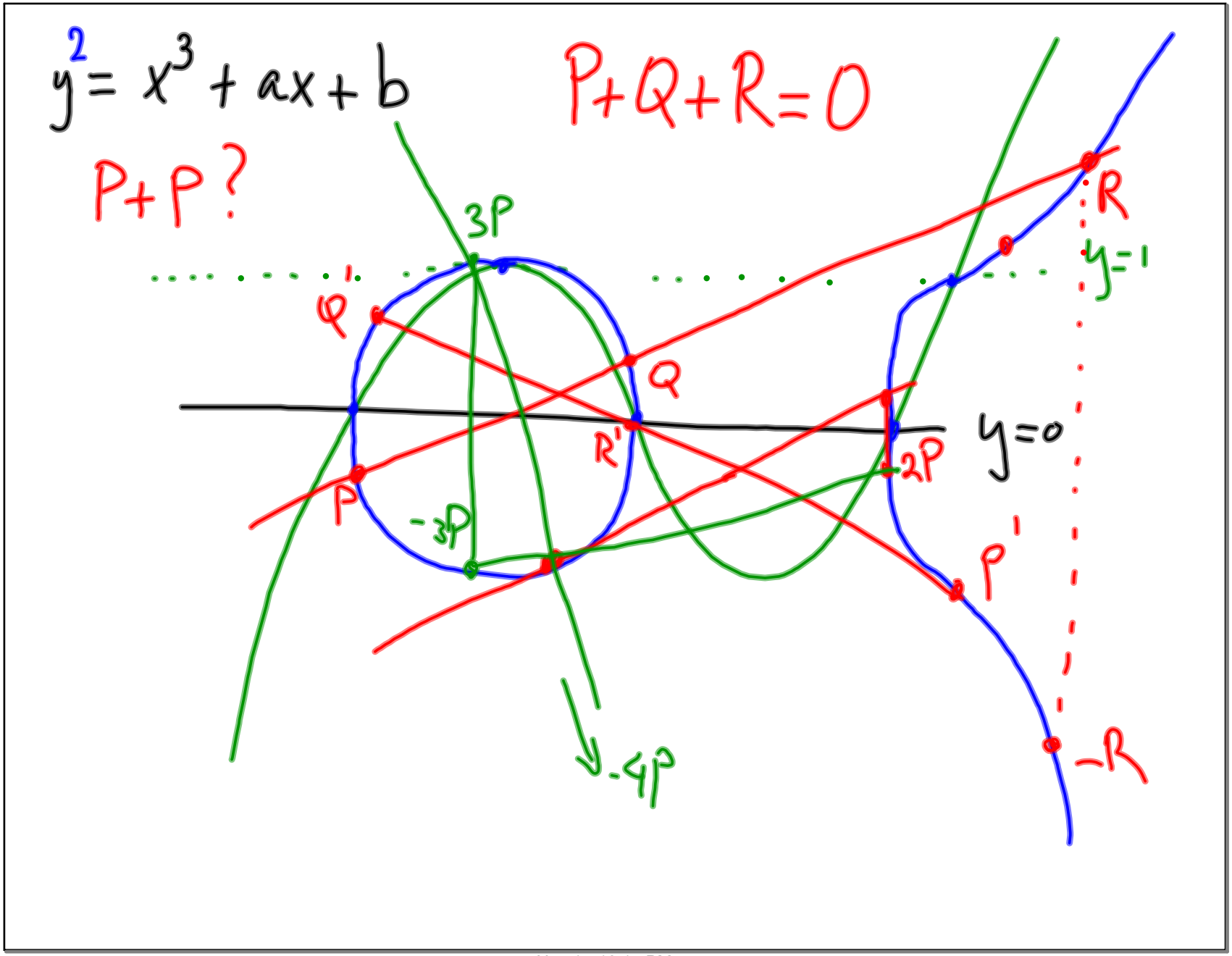
$3^4 = 81 \equiv 1 \pmod{10}$

Example

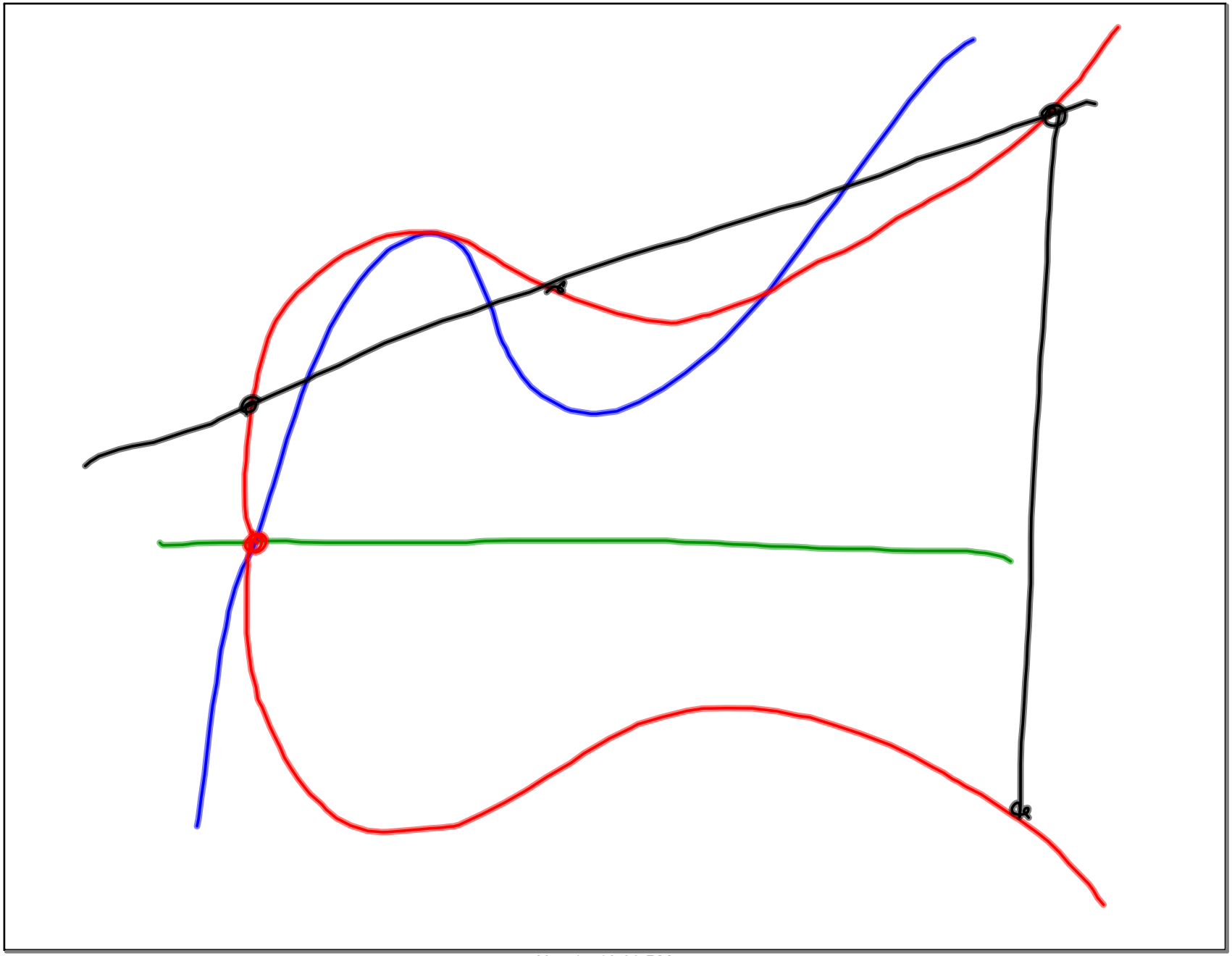
$$\varphi(10) = 4$$

$$\varphi(12) = 4$$

Nov 17-10:10 AM



Nov 17-12:14 PM



Nov 17-12:29 PM