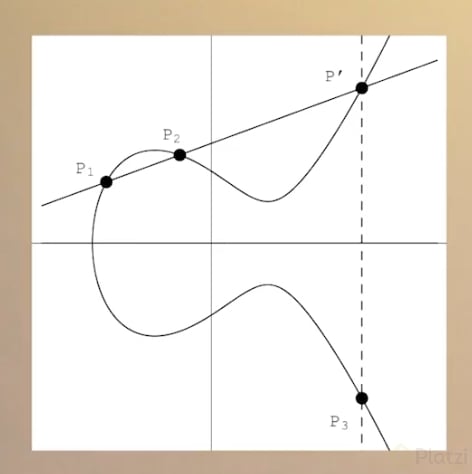
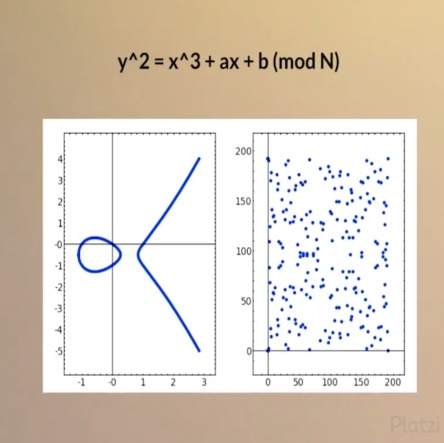
**Criptografía de Curvas Elípticas**

Es un tipo especial de criptografía que depende de operaciones de numero que no son necesariamente los naturales y depende de una construcción específica y esta construcción nos da garantías criptográficas, no solo se utiliza para firma electrónica, sino también para otros ámbitos de teoría de números y de investigación criptográfica.

Es una grafica definida por la ecuación y^2=x^3+ax+b , esta ecuación no es seleccionada de forma aleatoria, sino es seleccionada para mantener las mismas propiedades dentro de la curva. Hay diferentes curvas dependiendo de su uso, como por ejemplo unas especificas utilizadas para firma electrónica. Es posible realizar una operación sobre la curva (algo como una “suma inventada”)



En la suma de P1 + P2 el resultado será P´ la cual al invertirla nos dará otro punto P3



En la practica pasa por un proceso de aritmetización, la cual coloca dentro del campo de modulo N.

***Seguridad de Autenticación***

Las curvas elípticas se encuentran en diversas aplicaciones de autenticación, por ejemplo los dispositivos apple tienen un chip conocido como un enclave de seguridad, se encarga de custodiar una llave de seguridad y producir firmas sin que la llave abandone el dispositivo o en este caso el chip. Tambien existen las llaves fisicas para seguridad corporativa que muchas veces tienen codigos de autenticación dentro de ellos para autenticarse en servicios dentro de la empresa, otros permiten el firmado de arcfhivos. Adicionalmente en AWS encontramos el KMS en el cual bajo un modelo similar al de el enclave, donde AWS guardaría una llave privada y entregaria firmas bajo demanda cuando se solicite bajo la infraestructura, la llave privada nunca abandona el KMS y tambien esta custodiada en dispositivos que al abrirse se perderia toda la información.