Criptografía

Practica 1: Método de Euclides

ULPGC 2011-2012

Implementación del algoritmo Euclides, Euclides Extendido y el Inverso Modular, en una aplicación Android para dispositivos móviles

Gabriel Fernández Díaz
David Morales Sáez

1. Introducción

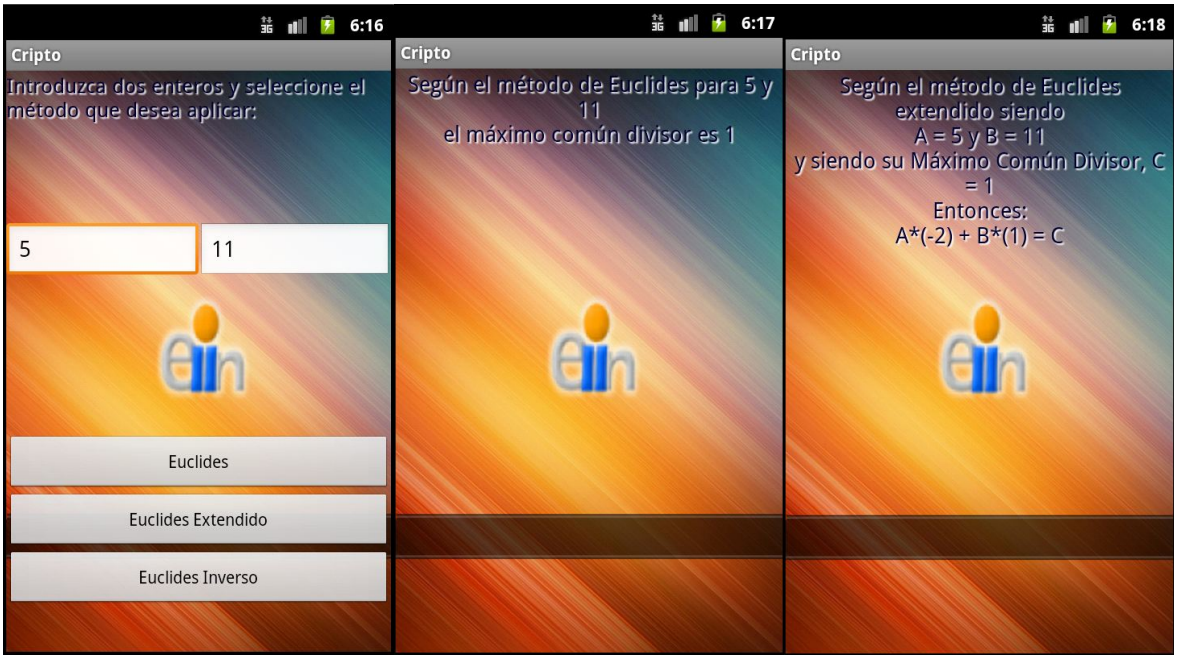
En esta práctica se ha propuesto es diseño del algoritmo de Euclides, su extendido y el inverso modular para crear una aplicación que los resuelva.

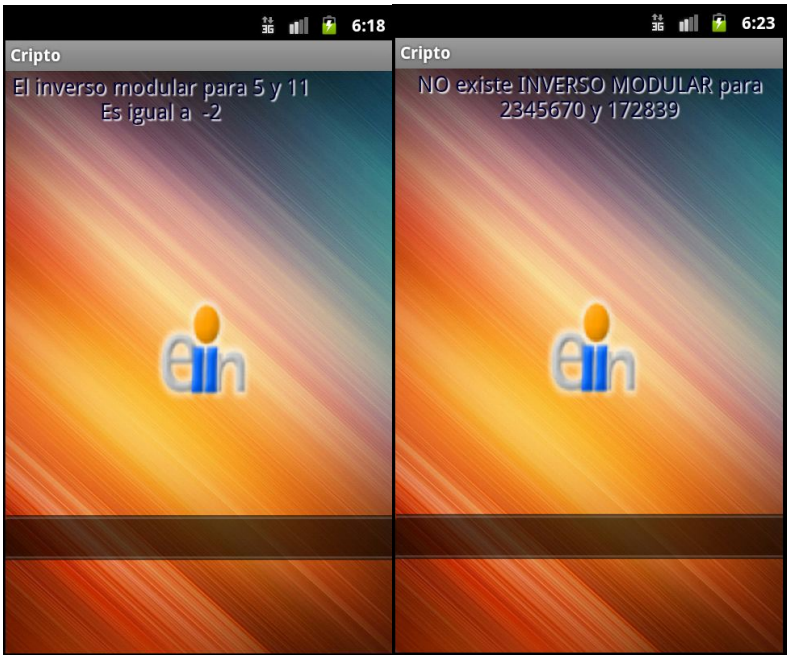
2. Desarrollo teórico

El Algoritmo de Euclides fue desarrollado por Euclides (como su propio nombre indica) en su libro Elementos. Este algoritmo es un método para calcular el máximo común divisor, que es el mayor número de los divide sin dejar resto. Por otra parte, el algoritmo de Euclides extendido es una modificación que permite expresar el máximo común divisor como una combinación lineal del valor con aquel número que lo multiplica. Finalmente, el inverso modular es aquel valor que, multiplicando al máximo común divisor, su módulo es 1.

3. Algoritmos desarrollados

Debido a que hemos desarrollado la práctica para la plataforma Android, hemos hecho el algoritmo en lenguaje JAVA. Por otro lado, al trabajar en esta plataforma, la interfaz ha de ser táctil y de fácil uso, como muestran las siguientes imágenes:




6:18
Cripto
El inverso modular para 5 y 11
Es igual a -2
6:23
Cripto
NO existe INVERSO MODULAR para
2345670 y 172839