ECM

(elliptic-curve factorization method)

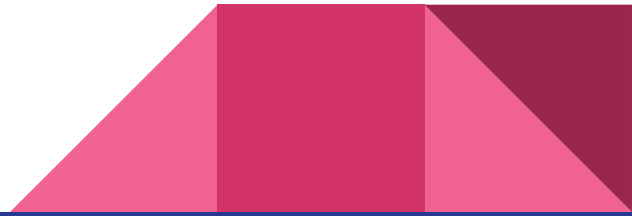
Canek García (kaan.ek@ciencias.unam.mx)

Agenda

Proyecto 3

Especificaciones

Elaborar un programa que reciba a la entrada un número compuesto **n** y devuelva su **factorización n = pq** donde **p** y **q** son primos. El programa deberá usar el algoritmo de factorización por curvas elípticas de **Lenstra**.



Notas

1. Es seguro que el número que leerá el programa es producto de únicamente dos números primos diferentes.
2. En el algoritmo de Lenstra utilizarán algunos de los algoritmos que ya se desarrollaron en las prácticas pasadas, como al algoritmo generalizado de Euclides, por esta razón se les recomienda “no reinventar la rueda”, es decir, si ya tienen estos algoritmos y funcionan, cópienlos tal cual al nuevo programa, o mejor aún, creen una librería con todos estos algoritmos e invóquenlos cada vez que lo necesiten.

Notas adicionales

El programa debe ser entregado en Java, Python ó C/C++.

Desarrollar el proyecto en equipos de dos integrantes (**los integrantes no pueden ser iguales que las dos prácticas pasadas**). **NO SE RECIBIRÁN PROYECTOS INDIVIDUALES**.

La entrega del código es el día **4 de diciembre de 2018**.

El proyecto debe ser enviado por **ambos** integrantes del equipo a través de la plataforma **ClassRoom**.

Documentar el código fuente de **todos** los métodos e incluir el **nombre completo** de ambos integrantes en el método **main** del programa.