担当教員　白勢政明 Masaaki Shirase　由良文孝 Humitaka Yura

FUN - ECM

楕円曲線法を用いた素因数分解プログラムを作成するプロジェクト

メンバー Member　下地健介 Kensuke Shimozi　松崎伸彦 Nobuhiko Matuzaki　谷山真子 Mako Taniyama　富樫北斗 Hokuto Togashi

概要

由来 Origin of project name

FUN-ECM プロジェクトの FUN は公立はこだて未来大学のことを、ECM は Elliptic Curve Method つまり楕円曲線法のことを意味する。

FUN means Future University Hakodate, and ECM means Elliptic Curve Method.

目的 Purpose of project

- **楕円曲線法を用いて高速に素因数を見つけるプログラム「funecm」の改良を行う。**
  Improve the program "funecm" that finds prime factors at high speed using the elliptic curve method.
- **「funecm」よりも速いプログラムを見つける。**
  Track down a program that is faster than "funecm".
- **桁の大きな数字を素因数分解し、「STUDIO KAMADA」に載せる。**
  A large number of digits is factored and submit it to "STUDIO KAMADA".

背景 Background of project

現在 、RSA 暗号がインターネットで広く使われている。RSA 暗号は、桁が大きい数の素因 数分解が困難であることを利用している。このプロジェクトで扱う楕円曲線法 (ECM) は 素因数分解を行う最良な方法の 1 つである。RSA 暗号の安全性は、素因数分解の困難さに大きく関わっている。

Currently, RSA encryption is widely used on the Internet. RSA encryption takes advantage of the difficulty of factoring large numbers.

Elliptic Curve Method (ECM) handled in this project is one of the best ways to do prime factorization.

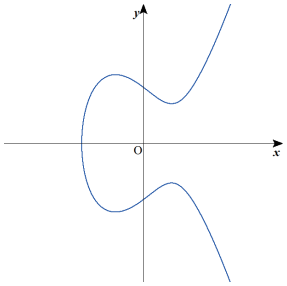
The security of RSA encryption is greatly related to the difficulty of prime factorization.

楕円曲線法とは

楕円曲線の定義 (方程式) Definition of Elliptic Curve (equation)

楕円曲線 : $y^2 = x^3 + ax + b$

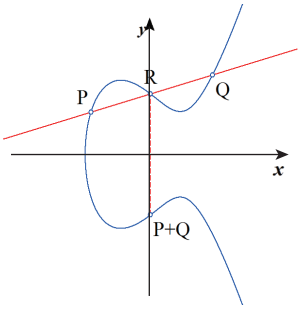
Elliptic curve : $y^2 = x^3 + ax + b$.



楕円曲線上の 2 点 P,Q の加法 Addition method point P and point Q in Elliptic curve

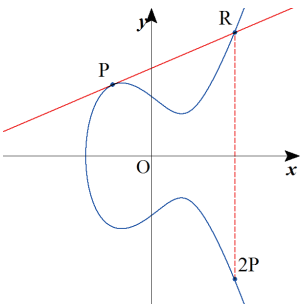
P,Q を通る直線と楕円曲線の交点を R とすると、点 R と x 軸に関して対称な点を P+Q とする。**(加算)**

Assuming that an intersection of a straight line passing P and Q and an elliptic curve is R, a point with respect to the x axis of R is P + Q.



点 P における接線と楕円曲線の交点を R とすると、点 R と x 軸に関して対称な点を 2P とする。**(2 倍算)**

When the intersection of the tangent and the elliptic curve at the point P is R, the point symmetrical with respect to the point R and the x axis is 2P.



スカラー倍算 A scalar method of doubling

点 P のスカラー n 倍である nP を計算するには、加算と 2 倍算より P を n 回加算した P+P+...+P を計算することでできる。

In order to calculate nP which is a scalar n times of point P, it is possible to calculate P+P+...+P by adding P n times by addition and doubling.

楕円曲線法 Elliptic Curve Method(ECM)

nP の座標を mod N で計算すると、ある確率で N の素因数分解を見つけることができる。

ECM can find a prime factor of N with a certain probabilty by computing nP mod N.

担当教員　白勢政明 Masaaki Shirase　由良文孝 Humitaka Yura

FUN - ECM

楕円曲線法を用いた素因数分解プログラムを作成するプロジェクト

メンバー Member　下地健介 Kensuke Shimozi　松崎伸彦 Nobuhiko Matuzaki　谷山真子 Mako Taniyama　富樫北斗 Hokuto Togashi

活動内容

プログラム班

後期の目標

・stage2 を実装
・全体のプログラムの速度に関する改良

プログラムの改良案

・Baby step giant step による stage2 の改良
・移動窓法による全体のプログラムの速度比較
・素数テーブルの改良

実行結果

・Baby step giant step による stage2 の改良は終了
・移動窓法はまだ実現できていない

速度比較について

stage1　stage2 の速度を比較

funecm

Stage1平均		Stage2平均		全体平均
67.78		27.51		95.28

PARIGP

Stage1平均		Stage2平均		全体平均
84.15		24.23		108.37

Web 班

Web 班では主に Web サイトの作成に取り組んだ。

構造化

今年は、楕円曲線法を高校生向けに紹介するための Web サイトの作成を目的とした。

カテゴリ化

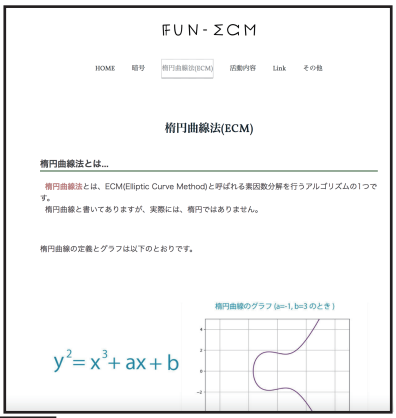
楕円曲線法を紹介することをメインとした。
カテゴリは「HOME」、「暗号」、「楕円曲線法 (ECM)」、「活動内容」、「Link」、「その他」の６つである。

構築

構造化・カテゴリ化を踏まえて、高校生に、楕円曲線法について興味を持ってもらえるようなサイトを作成した。

① HOME

FUN-ECM についての説明をしているページ



③ 楕円曲線法 (ECM)

楕円曲線法の定義とグラフ、そして楕円曲線法を何に使っているかを説明するページ。暗号のページとリンクする内容になっている。

② 暗号

暗号について簡単な説明をしているページ。二種類の暗号を説明し、例として RSA 暗号を取り上げている。

理解しやすいように図解表現をしている。

④ 活動内容

2019 年度の FUN-ECM の活動を説明するページ。前期と後期に分けて説明している。