FUN-ΣCM

Project18 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。

Project to create prime factorization program using elliptic curve method.

学生 青山和弘 Kazuhiro Aoyama，鳴海雄登 Yuto Narumi，染川眞輝 Masaki Somekawa，矢和田航平 Kohei Yawata，池田晴輝 Haruki Ikeda，上田隼人 Hayato Ueda，小泉建敬 Takehiro Koizumi

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

概要

由来 Origin of project name

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

本プロジェクトの目的はできるだけ大きな素因数を見つけ、「STUDIO KAMADA」のランキングに載ることである。

The purpose of this project is to find the largest prime factor as possible and be ranked in the STUDIO KAMADA.

背景 Background of project

大きな数の素因数分解は 30 数年前から非常に重要な研究対象となってきた。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一つである。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。

Prime factorization of big number has become a very important research subject around from 30 years ago. Elliptic Curve Method (ECM) handled in this project is one of best ways to do prime factorization. The security of RSA cryptography is greatly related to the difficulty of prime factorization.

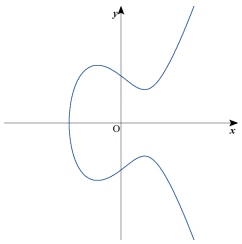
基礎学習

目的 The purpose

昨年度のプログラムを理解するために、メンバー全員が基礎知識として楕円曲線を知る必要があった。

In order to understand program of last year, we needed to learn basic knowledge of elliptic curve.

学習成果 The learning achievements



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

楕円曲線は、方程式 $y^2=x^3+ax+b$ で定義される。

Elliptic curve is defined as the equation $y^2 = x^3 + ax + b$.

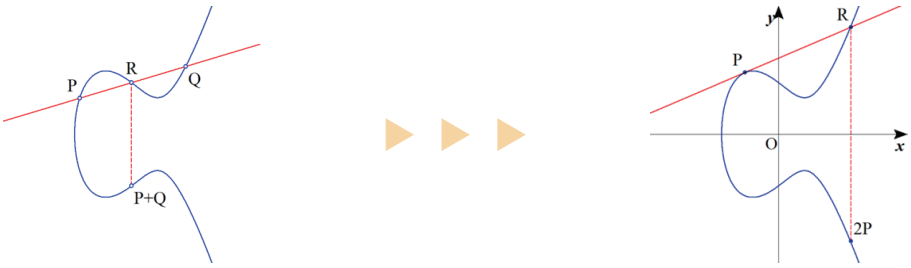
楕円曲線上の 2 点 P,Q の加法 Addition method point P and point Q in Elliptic curve

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。

When the intersection point of a straight line passing through P and Q and the elliptic curve is R, a point symmetrical with respect to the point R and the x axis is taken as 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。

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 multi plication of P

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

Calculate P+P+P+P+P which added P n times so that scalar n of point P calculates a certain nP in doubling.

楕円曲線法 Elliptic curve method

ECM は「合成数 N、楕円曲線の点 P、十分に大きな n に対して nP を計算し、nP の x 座標の分母と N の最大公約数を取ると、ある確率で N の素因数が得られる。」という事実を用いる。しかし、その確率は低く、STUDIO KAMADA にランクインするような合成数 N を素因数分解するためには、(3000000!)P の計算を数千回行う必要がある。

ECM uses the fact that calculating nP for a composite number N, a point P of an elliptic curve, a sufficiently large n, and taking the denominator of the x coordinate of nP and the greatest common divisor of N gives a prime factor of N. However, its probability is very low, and in order to factor the composite number N that ranks in STUDIO KAMADA, it is necessary to calculate (3000000!) P thousands of times.