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.

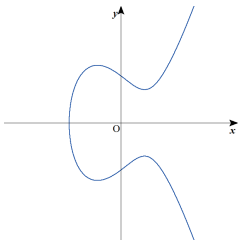
基礎学習

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 $y^2 = x^3 + ax + b$.

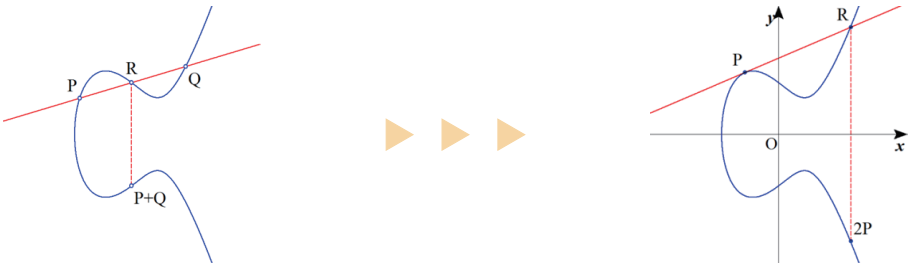
楕円曲線上の 2 点 P,Q の加法 Addition method point P and point Q in Elliptic curve

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.

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

活動内容

広報班

再構築までのフローチャート

構造化

既存のウェブサイトを構造化して、各ページの内容やつながりを視覚化した。そこから、ウェブサイトの問題点を明らかにした。

カテゴリ化

FUN-ECM プロジェクトの宣伝を主軸として、グローバルナビゲーションのカテゴリ分けを行った。カテゴリは HOME・PURPOSE・WORKS・MEMBER・ECM・PROGRAM・NEWS である。

再構築

構造化・カテゴリ化を踏まえて、過去から現在に至るまでの FUN-ECM プロジェクトの活動内容を報告する新しいウェブサイトを作成した。

新規ウェブサイトのプレビュー

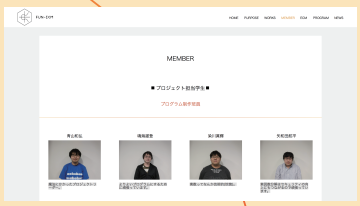
PURPOSE

FUN-ECM プロジェクトの活動目的を説明している。

WORKS

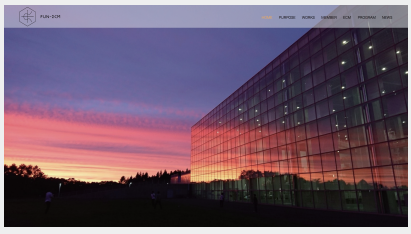
FUN-ECM プロジェクトの活動内容を月毎に紹介している。

MEMBER



FUN-ECM プロジェクト構成員の紹介と一言を記載している。

HOME



グローバルナビゲーションを使用して、カテゴリを選択できる仕様である。

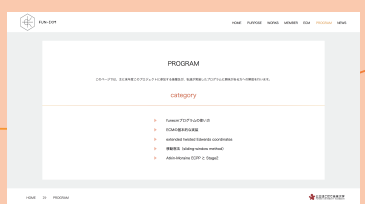
ECM

楕円曲線法 (ECM) の詳しい説明と具体的な仕様方法を紹介している。

NEWS

挑戦した素因数分解の結果を紹介している。

PROGRAM



FUN-ECM プロジェクトで実際に使用したプログラムの紹介をしている。

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

システム班

素因数分解待ちキューの実装

昨年度までに作成された素因数分解プログラムは、プログラムの実行毎にワークステーションにアクセスし、引数をプログラムに受け渡す必要があった。そこでこれまでプログラムを実行するために受け渡していた引数を格納するキューを用意し、一度のプログラム実行で複数回分の処理に用いる引数を受け渡せるようにした。

処理結果の外部出力

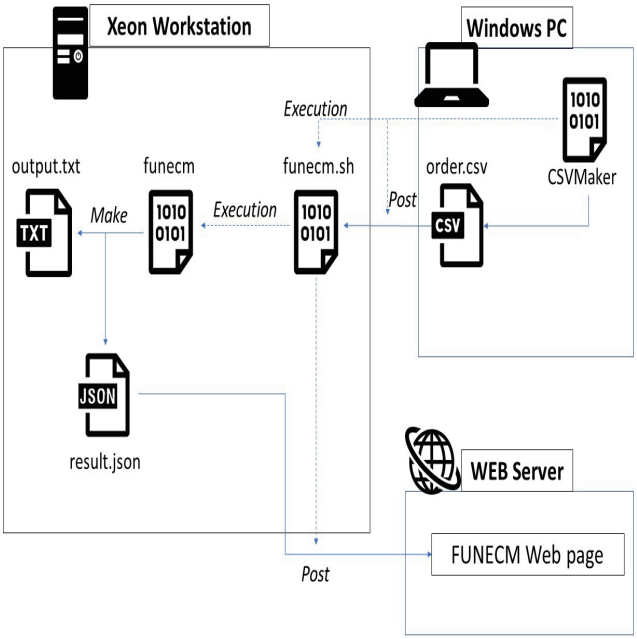
昨年度までのプログラムでは、処理結果の確認のためにワークステーションにアクセスし出力結果を確認する必要があった。これではプログラムの処理が終わったのかどうかを外部から確認するための手段がなかったため、プログラムの終了から次の実行までの時間が空くことがあった。この空き時間を減らす方法として、外部から処理結果を確認することが挙げられた。処理結果を Web ページにアップロードすることで処理状況と、簡易的な処理結果を確認できるようにした。

FUNECM システムのフロントエンド作成

上述の通り、プログラムの実行にはその都度ワークステーションにアクセスする必要があった。そこ 00 で外部から実行に必要な引数を格納したファイルを作成し、ワークステーションに送信、その後ワークステーションに SSH 接続し素因数分解プログラムを実行するアプリケーションを作成することでシステムのフロントエンド化を行った。

既存プログラムとの統合

本年度実装した機能を昨年度までに制作されたプログラムと結合し、FUNECM システムとした。システムの挙動は以下の図の通りである。



FPGA 班

FPGA について

FPGA とは Field Programmable Gate Array の略で直訳すると、現場で書き換え可能な論理回路の多数配列である。その名の通りにハードウェア言語で誤った回路設計をしても、即座にハードウェア言語によって修正ができるデバイスである。FPGA で回路を構成することは高い並列性が期待できる分野やアルゴリズムに効果的で、暗号解読や総当たりがその典型例であるこの長所が ECM の高速化にも効果的であると考えたため、FPGA に ECM を構成することとなった。

後期活動内容

右図が今期に設計した FPGA による ECM の回路図である。ECM では「分解したい合成数を N、任意の楕円曲線の適当な点を P として十分に大きな n に対して nP を計算し nP の x 座標の分母と N の最大公約数を取れば、ある確率で N の素因数が得られる。」という事実を用いため nP を何度も計算する必要がある。そこでこの FPGA の FUNECM では従来の FUNECM と比較して、nP を計算する処理の高速化が図られている。具体的にしたこととしては、使用した n は 4300 万までの素数ごとの 4300 万を超えない中で最大の累乗の総乗（例えば 10 までの素数ごとの 10 を超えない中で最大の累乗の総乗は (2^3=8)×(3^2=9)×5×7 で 2520 となる。）なので計算に多大な時間がかかる。そこで 4300 万までの素数ごとの 4300 万を超えない中で最大の累乗のリストを作成することで高速化を図っている。この回路図は現在、シミュレータ ModelSTM で動作確認中である。