# FUN-ECM プロジェクト
# FUN-ECM Project

b1014129　池野竜將　Ryusuke Ikeno

## 1　プロジェクトの目的

本プロジェクトの目的は，素因数分解を行いより大きな桁数の素因数を発見し，ECMNET にランクインすることである．素因数分解は，40 年ほど前から重要になってきている．その理由は，RSA 暗号に大きくかかわっている．RSA 暗号とは，現在のインターネット上の通信で広く使われいる暗号技術である．この暗号は巨大な合成数の素因数分解が難しいことを安全性の根拠とする暗号である．つまり，素因数分解は RSA 暗号の安全性を確認するために重要になっている．この素因数分解のアルゴリズムに楕円曲線法（以下 ECM と記述する）がある．私たちは ECM による素因数分解プログラムの高速化を目指す．また，ECMNET という ECM を利用し大きな素因数を見つけることを目的とするウェブサイトがある．記録されている素因数の桁数を超える素因数を見つけることでランクインすることができ，名前を載せることができる．私たちは，このランキングに載っている素因数よりも巨大な素因数の発見を目指す．加えて，今年度のプロジェクトから広報活動を行うことにした．ECM は多くの人が知っているテーマではなく，未来大でも知らない学生が多い．そのため，ECM について解説をする web ページを作成し，多くの人に ECM を知ってもらうと共に，本プロジェクトに興味を持ってもらうことを目指す．

## 2　課題の設定と到達目標

本プロジェクトの目的を達成するためには，プログラムの改善が必要である．改善のために以下の項目を課題として達成した．

- 楕円曲線法の理解
- ECM プログラムの高速化アルゴリズムの理解と実装
- ECM プログラムの評価

プロジェクト開始時点では，メンバー全員が ECM についての理解が不十分だった為，白勢先生・由良先生のご指導の下，楕円曲線法の基礎的な学習を行った．6 月ごろから，理論班とプログラム班に分かれて高速化アルゴリズムの提案と実装を並行して行った．後期では，高速化アルゴリズムの実装と並行して ECM プログラム評価の活動を行った．また，後期からは，今年度初の試みとして広報活動を行う．広報活動の目標である「ECM について多くの人に知ってもらう」ということを達成するため，以下の項目を課題とした．

- 広報媒体の設定
- ターゲットに合わせた内容の設定

広報は，今年度初めて行う活動なので，誰に向けて発信するかを決めた．主なターゲットを未来大の 1・2 年生とし，サブターゲットとして来年度以降のプロジェクトメンバーとした．また，それに合わせた内容をプロジェクトメンバー全員で議論した．

## 3　活動内容

### 3.1　基礎学習

ECM プログラムの改善や前年度から引き継いだ ECM プログラムを理解するために 5 月の中旬ごろまではメンバー全員が教授のご指導の下で ECM の基礎知識やアルゴリズムについての基礎学習を行った．具体的な内容は以下のとおりである．

- 楕円曲線法の基礎
- 剰余（Mod）について
- 楕円曲線上の点の加算・2 倍算

今年度は，前年度に比べて基礎学習の期間を短くし，ECM プログラムの高速化アルゴリズムの提案・実装・実行の期間をより長く確保した．基礎学習を終えた後，本プロジェクトの目的であるプログラムの高速化のため

の作業に移った．ECM プログラムの高速化には，多数ある高速化アルゴリズムから実装可能であり，大きな効果が期待できるアルゴリズムを選び実装する必要がある．これを 1 つのメンバー全員で一斉に行うことは効率が悪いと考え，プログラム班と理論班に分かれて作業を行った．

### 3.2 理論班

#### 3.2.1 活動目的

理論班は，プログラミング班の実装のために ECM プログラムの高速化アルゴリズムを調査し，提案することを目的とする．まず，プログラム班に提案するアルゴリズムを絞り，それを理解しわかりやすくすることを目標とした．以下にそのアルゴリズムを示す．

- Twisted Edwards Curve[1]
- Atkin-Morain ECPP[2]

#### 3.2.2 活動内容

まず，提案するアルゴリズムを決定するために，CiNii や Google Scholar を利用して高速化アルゴリズムの提案をしている文献を探し，それぞれ理解を進めた．その中で 3.2.1 で挙げた 2 つのアルゴリズムに注目した．このアルゴリズムに関しての文献を輪読し，アルゴリズムをわかりやすく書き起こしてプログラム班に提案した．

#### 3.2.3 活動成果

Twisted Edwards Curve は早い段階で提案することができたため，プログラム班によって前期中に実装し高速化させることができた．Atkin-Morain ECPP は前期の終わりごろに提案を行ったため，実装は後期になってしまったが，実装できた．しかし，発見確率の検証は行えなかった為，効率が改善したかは不明である．

### 3.3 プログラム班

#### 3.3.1 活動目的

プログラム班は，ECM プログラムの高速化アルゴリズムを実装し実行速度，素因数発見効率の改善を行うことを目的とする．そのために以下の項目を課題として設定した．

- 前年度の ECM プログラムの理解
- 理論班の提案したアルゴリズムの実装

#### 3.3.2 活動内容

まず，前年度の ECM プログラムの理解から始めた．ECM プログラムは C 言語を利用して記述されており，プログラム班全員で読み進めた．わかりにくい部分はその都度，文献や論文を利用して理解した．多倍長演算を行うライブラリである GMP については，読み進めていく中で順次調べて理解した．また，これらの活動中に前年度から引き継いだプログラムに冗長な部分があったため，変更しても問題が発生しないことを確認したのち冗長な部分を変更した．次に理論班から提示されたアルゴリズムの実装を行った．アルゴリズムの内容は 3.2.1 に記述した．また，プログラムを読み進める中で，改善できると予想された部分についても実装を行った．以下にプログラム班で実装したアルゴリズムを示す．

- Extended twisted Edwards coordinates
- 楕円曲線の生成法の変更
- Atkin-Morain ECPP
- 移動窓法 [3]
- Stage2 [4]

それぞれのアルゴリズムを実装するごとに，前年度のプログラムとの簡易的な比較を行った．比較項目は楕円曲線 1 つの処理を終える時間と，全処理が終了した際に発見できた素数の桁数とした．改善されたことが確認して次のアルゴリズムを実装した．Atkin-Morain ECPP は素因数の発見効率を上げるアルゴリズムであるため，検証ができなかった．そのため，このアルゴリズムは使用するかをコンパイル時のオプションで設定できるように実装した．

#### 3.3.3 活動成果

それぞれのアルゴリズムでプログラムの処理速度が高速化されたことが確認され，昨年度より優れた ECM プログラムが完成した．詳細な検証は次の章で記述する．

### 3.4 検証

後期から，前年度作成した ECM プログラムとの詳細な比較を行うため，理論班の中でプログラムの検証を行うグループ（以下検証班と記述する）を作成した．

#### 3.4.1 活動目的

検証班の目的は，前年度と今年度のプログラムの詳細な比較評価を行うことである．高速化のために取り入れたアルゴリズムが処理時間にどのような影響がでるのかを調査することは，今後もプログラムを改善していくうえで重要である．今年度のプロジェクトでは，ECM プログラムの高速化に加えて素因数発見効率の改善を行っ

たため，前年度のプロジェクトとは比較方法を変更する必要があった．そのため，以下の項目を課題として設定した．

- 検証方法の調査・提案
- 実際に検証を行う
- 検証結果の可視化

#### 3.4.2　活動内容

まずは，検証結果に統計的な信憑性を持たせるために検証方法の調査を行った．しかし，どの検証方法も今回の検証には適切でない，または実行するだけの時間が足りないなどの理由で使用しなかった．今年度は 20 桁から 50 桁の合成数を 5 桁刻みで各 5 回ずつ入力し，処理時間のトータルタイムの平均を比較した．検証環境は以下の通りである．

- コンパイラ:icc 14.0.1
- OpenMP:301
- GMP:6.0.0
- CPU:Intel Xeno Phi 5110P(60 コア)
- RAM:64GB(DDR3L-1600 8GB DIMM×8)

#### 3.4.3　活動成果

今年度と昨年度のプログラムのトータルタイムの平均を比較した結果，20 桁から 30 桁では今年度の結果の方が下回る結果になったが，35 桁以降は徐々に上がっていき，最大 15% ほど改善し，処理速度が上がったことが確認できた．少ない桁数の場合に処理速度が低下してしまった原因は，今年度新たに実装した移動窓法の事前計算のコスト大きく，高速化した分のコストを超えてしまったことが原因だと考えられる．上記の通り，本プロジェクトの目的である巨大な合成数の素因数分解を行うのに昨年度よりも優れた ECM プログラムが完成したことがわかる．

### 3.5　広報

後期から，FUN-ECM の活動を発信するため，理論班の中で広報活動を行うグループ（以下広報班と記述する）を作成した．

#### 3.5.1　活動目的

広報班の目的は，FUN-ECM の活動を外部に発信し，ECM について多くの人に認知してもらうことである．本プロジェクトは，前年度からプログラムを引き継ぎ改善することを中心に活動しており，継続性の強いプロジェクトである．そのため，今年度ならではの活動をしたいと考えた．新奇的な活動を行うにあたり，未来大生でも ECM について知らない生徒が多いことからより多くの人に ECM を伝えられるように広報的活動を行うことにした．広報を行うにあたり，以下の項目を課題とした．

- 広報媒体の設定
- ターゲットに合わせた内容の設定

#### 3.5.2　活動内容

まず，広報を行うターゲットを設定した．メインターゲットは，未来大を中心とする情報系の大学生とした．加えて，サブターゲットとして ECM に興味を持った方や，来年度のプロジェクトメンバーを設定した．今年度は，昨年度のプログラムを理解する為に実装してあるアルゴリズムについて文献を利用して調べた．これを事前に簡単にまとめておくことで来年からの活動をスムーズに進めることができると考えサブターゲットをこのように設定した．次に広報媒体の設定を行った．中間発表の意見で，プレゼンだけでは理解しにくかったという意見をいただいたことから，手軽に閲覧することができ，よりわかりやすく伝えることができる媒体として web ページを採用した．サブターゲット向けのページはプログラム班と協力して作成した．

#### 3.5.3　活動成果

メインターゲット向けのページとして，ECM について解説したページが完成した．このページでは ECM の基礎理論ページ，FUN-ECM の活動目的に分かれている．章ごとに分けて詳細な説明を行い，段階的に読み進めることができるようにした．また，プレゼンテーションでは使用することのできなかったグラフの gif 画像などを利用し，より理解しやすいように工夫したはっき．サブターゲット向けのページとして，プログラムの解説ページが完成した．現在実装してあるアルゴリズムの簡単な解説を載せている．また，来年のプロジェクトメンバー向けに，プログラムの実行手順を載せた．

### 3.6　発表

#### 3.6.1　中間発表会

中間発表会では，楕円曲線法の基本的なアルゴリズムや，前期中に実装したアルゴリズムについてプレゼン

テーションを行った．ECM についての解説は数学の要素を多く含み難解なため，専門的な単語を避けて時間をかけて説明した．ポスターは，前年度の構成を参考にしながら作成した．本番ではプロジェクターの電源が落ちるアクシデントもあったが，用意した内容をすべて発表することができた．聴講者の評価は発表技術が 7.1 点，発表内容が 7.5 点だった．コメントは内容を理解できた人とできなかった人に分かれていたため，さらに前提知識のない聴講者にもわかりやすい内容にしていく必要があることがわかった．

#### 3.6.2 成果発表会

成果発表会では，中間発表会のレビューを元に，さらに前提知識のない聴講者でもわかりやすい内容を目指した．中間発表会に引き続き専門的な用語は極力減らした．加えて，最も大事なところを枠で囲み，その中身を見るだけで大まかな内容を理解できるように変更した．また，数学に抵抗のある人でも触れやすいように，例示を多く含める，長い数式に関しては説明を省きスライドに載せるだけにとどめるなどの工夫を行った．聴講者の評価は発表技術が 7.9 点，発表内容が 7.9 点だった．中間発表会に比べて大きく点数が伸びており，工夫の効果が表れていることがわかった．しかし，発表内容を省きすぎている，数式の説明を省略するのは良くないなどの意見もあった．

### 3.7 まとめ

本プロジェクトの目的は，ECM を利用して素因数分解を行い，より大きな桁数の素因数を発見することであった．これを達成するために，ECM の理解，高速化アルゴリズムの実装を中心に活動を行った．その結果，ECM への理解を深め，ECM プログラムを前年度と比較して最大 15% ほど高速化することに成功した．また，今年度の新たな活動として広報活動を行った．後期のみの活動だったが，web ページを完成させることができた．しかし，web ページがわかりやすいかどうかのアンケートをとることはできなかった．

### 3.8 今後の展望

今年度は前年度の反省を踏まえて，1 年間の活動計画を大きく変更して行った．改善された点もあったが，問題も発生した．来年度に向けて，今後の反省と展望を示す．

- 検証は時間に余裕をもって行うべきである．今年度の検証では，50 桁の合成数を入力した際に 3 時間ほど時間がかかっている．巨大な合成数の分解には多くの時間が必要なため，検証方法を早い段階で決定して検証を行いたい．
- 新たな活動を行う場合は，前期から行うべきである．今年度から，広報活動を行ったが前期中は基礎学習と実装を中心に行ったため，広報活動は行わなかった．そのため，アンケートをとる時間が不足してしまった．新たな活動をする場合は前年度の活動の流れを大きく変える必要がある．
- 発表の際には，素因数分解がどのように実世界で利用されているかを説明するべきである．最終発表会の評価では，素因数分解が重要なことはわかるが，どこで使われているかもっと具体例が聞きたいというコメントがあった．公開鍵暗号との関係などを発表で絡めて説明できるようにしたい．

## 参考文献


[1] Hisil, H., Wong, K.K.-H., Carter, G., Dawson, E. Twisted Edwards curves revisited. Advances in Cryptology - ASIACRYPT 2008, 2008

[2] Bernstein, D.J. , Birkner, P. , Lange, T. , Peters, C. ECM USING EDWARDS CURVES. Mathematics of Computation, 2013.

[3] シニアエンジニアの庵. http://sehermitage.web.fc2.com/index.html, （最終アクセス 2017 年 1 月 13 日）.

[4] Gaj, Kris, et al. Implementing the elliptic curve method of factoring in reconfigurable hardware. International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2006