FUN-ECM プロジェクト

FUN-ECM Project

A グループ(A)　Search Group (A)

1017217　下地健介　Kensuke Shimoji

1　背景

情報化が進んだ現代では,暗号化の技術が重要である. 暗号化の技術の一つに RSA 暗号がある. 本プロジェクトでは RSA 暗号技術の安全性を検証し,その RSA 暗号解読方法の一つである楕円曲線法(ECM : Elliptic Curve Method)について学ぶ.

RSA 暗号とは約 40 年前に考案された公開鍵暗号であり, 現在でも広く利用されている. RSA 暗号は 2 つの素数を掛け合わせて作られた長大桁合成数の素因数分解が困難であることを根拠に安全性が保障されている暗号である. 楕円曲線法は, 与えられた曲線の点の演算結果より合成数の因数である素数を見つけることができる方法である. これを利用し, 長大桁数合成数を素因数分解することで RSA 暗号を解読することができるが, ただ行うだけでは非常に長い時間と大きな計算量を要する.

前年度までのプロジェクト活動で, 楕円曲線法によって素因数分解を行うプログラム funecm が完成していた. そこで, 今年度のプロジェクト活動では funecm を高速化すること, または別のプログラムを作成することによって, 前年度までに作成されたプログラム以上の速度で素因数分解を行うことを目標とした. また, 去年度に作成された Web サイトには正しくページが表示されない, 特定のページから特定のページに飛ぶことが出来ないなど様々な問題点があった. そのため, Web サイトを新しく作成し, また高校生向けに理解しやすい楕円曲線法の説明を載せることを目標とした.

2　課題の設定と到達目標

まずメンバー全員で楕円曲線法について基礎学習を行い, その後前項で述べた本プロジェクトの 2 つの目標に沿って活動を行うために, 次の 2 つの班に分かれた.

・PARI/GP によって素因数分解プログラムを作成するプログラム班

・Web サイトを作成する Web 班

前期は楕円曲線法について学び理解を深めた. 後期ではこの 2 班体制に分かれてそれぞれ活動を行った.

また, 作成したプログラムの性能確認のために, STUDIO KAMADA[1]という Web サイトで公開されているチャレンジ合成数を対象に素因数分解を行った. これに成功すると, STUDIO KAMADA 上に本プロジェクトの名前が記載される.

以下に各班の課題を述べる.

プログラム班

前年度までに C 言語によって作成された素因数分解プログラム funecm と同様の動作をするプログラムを, 計算機代数アプリケーションである PARI/GP でプログラムを作成することで高速化を図ろうとし, PARI/GP の学習, 及び C と PARI/GP の速度比較を課題とした.

Web 班

Web サイトを更新するにあたり, 従来の Web サイトの問題点を探した. その後, HTML, CSS の学習を行い実際に新しい Web サイトの作成を行った. その中で, どのような説明が高校生に理解してもらえるかを課題として作成した.

3　課題解決のプロセスとその結果

3.1 基礎学習

まず楕円曲線法を理解するため基礎学習を行った．有限体，Euclid の互除法，拡張 Euclid の互除法，楕円曲線の定義，楕円曲線上での加算・逆元・スカラー倍算，無限遠点，2 倍算などについてメンバー全員で学んだ．その後，メンバーの希望をもとに班分けを行い課題解決に向けて活動を開始した．

3.2 プログラム班

今年度では，PARI/GP を利用して ECM での素因数分解を行うプログラムを作成することで高速化，およびプログラム上でどのようにして ECM を行っているのかを把握しやすくすることを図った．高速化に関しては，通常の ECM より効率の良い方法を実装することでさらなる高速化を図った．

ECM は Stage1, Stage2 の 2 つに大きく分けられる．

Stage1 では，合成数 N の因数 p を見つけることについて考えている．合成数 N の桁数から，因数の大きさを予想して，パラメータ B_1, B_2 を決める．本プロジェクトでは B_1, B_2 の値を ECMNET[2]から引用した．ある楕円曲線上の射影座標で与えられた点 $P=(X_p : Y_p : Z_p)$ に対してある手順によって確率的に因数を見つけることができる．この Stage1 では P に対するスカラー倍は B_1 の階乗よりも 1 から B_1 までの数すべての最小公倍数を入れた方が効率が良くなる．そのため，1 から B_1 までの数すべての最小公倍数を求めるプログラムを作成した．

Stage2 では，B_1 から B_2 までの素数 s の中に，位数があるかを調べる．これは，Stage1 のみを利用していると，素因数を見つけやすくするためには B_1 を大きくし，非常に大きい数 I に対して，スカラー倍 IP を計算する必要がある．そしてスカラー倍の計算は，非常に計算量が大きくなるため，Stage2 を利用する．本来の Stage2 では B_1 から B_2 までの素数を Stage1 が終わった後の点のスカラー倍に入れていくが，それよりも効率の良い *Baby-step Giant-step* がある．そして *Baby-step Giant-step* の高速化として素数テーブルの利用がある．

Baby-step Giant-step とは，$B_1 < s < B_2$ を満たす全ての素数 $s_1, s_2, s_3, \cdots, s_k$ に対して，s を変形して計算を行うことで高速化を図る手法である．Stage2 は $sP = O$ の際に成功する．この式を変形することである確率で素因数分解を行うことができる．*Baby-step Giant-step* の改良として素数テーブルを用いた．*Baby-step Giant-step* では x 座標の差を掛け合わせるが，この差が素数でなければ掛ける必要はない．そのため，素数かどうかを判断することが高速化につながる．PARI/GP の関数としては isprime 関数があるが時間を要する．そのため，素数テーブルを実装した．素数テーブルとはあらかじめメモリ上に小さい順に素数が用意されたものである．メモリ上には連番で配置されており，配列としてアクセスすることで n 番目の素数が取得できる． これにより，一瞬で素数判定ができるため，高速化につながる．素数テーブルはあらかじめ別のプログラムで作成し用いる．この手法は多くのメモリを消費し，素数テーブルを読み込む時間が必要となるが， その後の素数判定の部分が大幅に高速化される．

また，作成したプログラムを用いて funecm と実行時間を比較した．PARI/GP の実行環境は Core i3-7100U 及び Xeon E5-2640 を用いた．昨年度の実行環境は Xeon E5-2640 を用いた．Core i3-7100U のスペックとしては，CPU2 コアである．Xeon E5-2640 のスペックは，CPU12 コアである．この時，$B_1 = 3000000$, $B_2 = 300000000$, 分解する合成数は STUDIO KAMADA に載っている桁数 159 桁の合成数とした．そして，200 回の合計試行時間から平均を取り，昨年度のプログラムは一番速い実行時間を平均として比較した．比較した結果，Stage1 での実行時間は funecm と比べて約 1.14 倍速くなった．また，Stage 1, Stage 2 合わせた速度比較も行った．PARI/GP の実行環境は Core i3-

7100U 及び Xeon E5-2640 を用いた．昨年度の実行環境は Xeon E5-2640 を用いた．

この時，$B_1 = 4572523$，$B_2 = 457252300$，分解する合成数は STUDIO KAMADA に載っている合成数とした．そして，100 回の合計試行時間から平均を取った．括弧内には用いた CPU を示す．ここで，Core とは Core i3-7100U を指し，Xeon とは Xeon E5-2640 を指すこととする．Core i3 を用いた PARI/GP のプログラムと，Xeon を用いた funecm に着目する．Stage 1 では Core を用いた PARI/GP のプログラムの方が約 1.32 倍速くなった．Stage 2 では Core を用いた PARI/GP のプログラムの方が遅くなったものの，全体としては Core の PARI/GP のプログラムが約 1.15 倍速くなった．次に，Xeon を用いた PARI/GP のプログラムと，同じく Xeon を用いた funecm に着目する．Stage 2 では PARI/GP のプログラムの方が約 1.14 倍速くなった．しかし，全体として比較すると funecm の方が約 1.4 倍速いという結果となった．

3.3 Web 班

後期から，楕円曲線法をより一般に知ってもらうために新しく Web サイトを作成することとなった．はじめに，去年度の Web サイトを参考にし，どのような Web サイトを作成するかをメンバーと話し合った．去年度の Web サイトは，老若男女幅広い年代の方々が親しみやすく，操作しやすい Web サイトを目指していた．また，去年度の Web サイトの問題点は 2 つあった．1 つ目は，デザインの問題である．Web サイトのページが中心からずれている，タブレット端末でサイトを閲覧した際正しく表示されないなどがあった．2 つ目は，掲載されている楕円曲線法の説明文が長くなり，分かりづらくなっていた．それらの問題点を踏まえて今年の Web サイトは対象者である高校生が見やすく，理解しやすい Web サイトを目指した．

次に，高校生が理解しやすいような Web サイトにはどのようなものが必要であるかを話し合った．挙がった意見では，高校生は楕円曲線法を調べることがない，というものであった．そのため，公開鍵暗号方式や共通鍵暗号方式などの暗号の説明を丁寧にしてから，楕円曲線法について説明することとなった．また，数式をできるだけ使わず，図を多く入れることを重視すべきだと考えた．

Web 班のメンバーは HTML と CSS をほとんど触ったことがなかった．そのため，HTML と CSS の参考書を用いて，2 週間ほど学習した．参考書は，HTML などのタグの説明とソースコード，実行結果が並んで表示されており，その工程をすべて行うと一つの Web サイトが作成できる仕組みとなっていた．はじめに大まかな Web サイトを HTML で作成した．その後，CSS を実際に使ってコーディングした．実際に Web サイトが作成することができる点が魅力的であった．このことによって，理解しやすく，楽しみながら学習を進めることができた．また，よく分からないところやうまくコンパイルできなかった時には，メンバー同士で作成したソースコードを見ながら学習を行った．学習はメンバーが揃って行っていたので助け合い，情報共有しながらスムーズに進めることができた．Web サイトのレイアウトを決定する前に，広報班のメンバーで様々な Web サイトを閲覧し，どのようなサイトが見やすいかを挙げた．そのようなサイトはシンプルなデザインで，ページごとに色が統一されていた．また，画面上部にヘッダーや画面下部にフッターがあった．その後，閲覧した Web サイトを参考にしながら，Web サイトのレイアウトを作成した．採用したレイアウトは，画面上部にヘッダーがあり，シンプルなデザインなものである．このとき，ワイヤーフレームを作成し，実際にページの移動や見出しの位置などを確認した．ワイヤーフレームを作成する際には，Adobe の XD というソフトを用いた．Adobe XD は，ユーザ操作性をデザイン，プロトタイプ化し，ユーザの立場になってそのレイアウトを確認することができるものである．FUN-ECM の Web サイト

にはすでにロゴがあった．去年のロゴは十分良いものであったが，今回の Web サイトはシンプルなものを目指していたので，去年のロゴの良い点を取り入れながら新しく制作した．新しいロゴには，去年と引き続き代表的な楕円曲線と，新たに有限体の記号を追加した．また，全体の色を黒にした．このロゴは Web サイトの画面最上部に使用した．

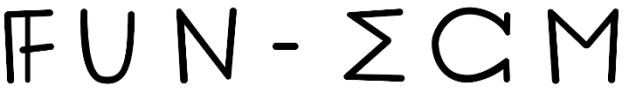

図 1　作成したロゴ

ロゴを制作したのは Web 班の富樫である．Adobe Illustrator を用いて制作した．今年の Web サイト作成は Ameba Ownd という Web サイト無料作成サービスを用いた．Ameba Ownd を用いた理由としては 3 つ挙げられる．1 つ目は，複数人で 1 つのものを編集することができることである．後でファイルをまとめる必要がなく，他のメンバーが制作した部分を見ることができるため，間違っているところをお互いに直しながら作成することができる．2 つ目は，操作が簡単なことである．Ameba Ownd では用意されているデザインの中から 1 つ選び，編集していく．画像，地図やテキストなどを簡単に入れることができる．さらに，細かいコーディングやメンバーがそれぞれコーディングするわけではないので，ページのずれが起きない．また，スマートフォンやタブレットにも対応しているため，去年の問題点が解決する．3 つ目は，HTML と CSS でのコーディングが可能であることである．Ameba Ownd ではテキストをそのまま打ち込めるが，色や大きさなどを細かく指定するとき，線を引いたり囲んだりしたいときに，HTML と CSS を用いることができる．Ameba Ownd 内での HTML と CSS は通常のタグを使用することができる．以上の点を踏まえて，Ameba Ownd を利用することにした．

次に，主に担当するカテゴリを決めた．下地が HOME と暗号を，谷山が楕円曲線法(ECM)とその他である．活動内容と Link は 2 人で作成した．担当するページを作り，時々プレビューを確認しながら進めていった．メンバーと話し合った結果，HOME 以外のすべてのページで文字の大きさを調整できる HTML として書くことに決めた．また，画像の大きさがページによって異なることが分かった．また，楕円曲線法と暗号の仕組みの図はすべて Adobe Illustrator を用いて作った．楕円曲線のグラフは Python で作成した．

最終成果発表会の一週間前に，全体の微調整と最終確認を行うことが出来た．

4　今後の課題

以下が来年度以降の課題として挙げられる．

・Stage1 での素因数発見確率を調べること

・PARI/GP のさらなる高速化とサーバー上での実装

・実際に高校生に Web サイトを見てもらいフィードバックをすること

参考文献

[1]STUDIO KAMADA. http://stdkmd.com/ ,（最終アクセス 2019 年 7 月 22 日）

[2]ECMNET. https://members.loria.fr/PZimmermann/ecmnet/（最終アクセス 2019 年 7 月 22 日）