

FUN-ECMプロジェクト

FUN-ECM Project

中島俊平

Nakajima Shunpei

福永慧

Fukunaga Kei

小澤貴也

Ozawa Takaya

落合航平

Ochiai Kouhei

金子真澄

Kaneko Masumi

水上敬介

Mizukami Keisuke

外山拓

Toyama Taku

2.2 後期活動内容詳細

プログラムの計算時間を短縮させるために、様々なアルゴリズムの実装を行った。他にも、シェルスクリプトやドキュメントの作成した。

・素数テーブル

ECMではやや小さ目な素数のテーブル(例えば43億以下の素数のテーブル)が必要となる。去年までのプログラムでは素数を求めるのにC言語のライブラリを使用していたが、それでは素数を求めるのに時間がかかってしまうため、予めテキストファイルに素数を用意して、素数が必要になった際はそのファイルを読み込み、計算に用いる。

・新たなアルゴリズムの実装

プログラムの計算の速度を向上させるために、様々なアルゴリズムを実装した。アルゴリズムはBaby-Step Giant-Step、モンゴメリー曲線、素数ペアリングを使用した。

・シェルスクリプトの作成

プログラムの実行を効率良く行うために、スクリプトを作成した。実行された結果をテキストに出力するようにしてあり、指定した桁数の合成数を計算できるようにした。

3. ECMについて

3.1 基礎学習

目的

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。

方法

『楕円曲線暗号入門(2013年度)』(著 伊豆哲也)を用いて学習した。

学習内容

・ Z/nZ の世界での加算、減算、乗算、除算について

$Z/nZ = \{0, 1, 2, \dots, n-1\}$ までの整数の集合を考えると、加算・減算・乗算は普通に計算した結果の $\text{mod } n$ をとる。除算について、 $a, b \in Z/nZ$ に対して、 $a \div b$ の解は $a = bc \text{ mod } n$ となる c である。 n が素数の場合、 $b \neq 0$ ならば $a \div b$ の計算が可能

・楕円曲線の定義(方程式)

楕円曲線 E は、方程式 $E: y^2 = x^3 + ax + b$ で定義される。

・楕円曲線 E 上の2点 P, Q の加法

・ $P + Q$ の定義: P, Q を通る直線 l 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 R' のこと。
・ $2P$ の定義: 直線 l を点 P における接線とする。さらに、この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 R' のこと。 P の座標と Q の座標から $P + Q$ の座標や $2P$ の座標を計算する公式が存在する(加算公式と2倍算公式)。

・スカラー倍

・ E の点 P と自然数 n から、 n 個の P の和 $nP = P + P + \dots + P$ をスカラー倍という。
・ECMの支配的な演算はスカラー倍である。本プロジェクトにとって、スカラー倍の高速化は重要である。高速化の方法として、バイナリ法や射影座標の手法がある。

・射影座標

点 (x, y) を z 座標を追加して (x, y, z) で表す座標を射影座標と言い、射影座標を用いるとスカラー倍が高速になる。

・Stage1 とは

素因数分解したい合成数 N に対して、適切な大きさの B_1 から k を求め、 $\text{mod } N$ 上でスカラー kP を計算する。そして、 kP の z 座標と N との最大公約数が1でなければ N の因数である。見つからなかったらStage2へ。
見つかる理由として、 P を N の素因数の1つとすると、 m が $\#E \text{ mod } p$ の倍数の時、 $mP = 0 \pmod{p}$ となり、 $mp = (x: y: z) \text{ mod } N$ に対して、 $z \equiv 0 \pmod{p}$ となる。

・Stage2 とは

$B_1 < s < B_2$ を満たす、すべての素数 $s_1, s_2, s_3, \dots, s_k$ までのStage1で得られた点を Q として全てのスカラー倍 $s_i Q$ を求め、 $s_i Q$ の z 座標と N との最大公約数をとる。Stage2を高速に行う方法にBaby-Step Giant-Step法がある。

3.2 ECMの計算の流れ

Stage1の流れ

$P \in E \text{ mod } N$ に対して、 $Q = mP = (x, y, z) \text{ mod } N$ を計算する

$\text{gcd}(n, z) \neq 1$ の時
終了

$\text{gcd}(n, z) = 1$ の時
 Q を返して、stage2へ

Stage2の流れ

Stage1で見つかった Q をもとに、Baby-Step Giant-Step法を使用(Baby-Step Giant-Step法については3.3.2を参照)

未発見の時、曲線を変えてStage1へ移行

発見した時、終了