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

1. 概要

1.1 プロジェクト名について About project name

FUN-ECMのFUNは、はこだて未来大学を、ECMは Elliptic Curve Method(楕円曲線法)を意味しており、
それらを繋げたのが本プロジェクト名の由来である。

Why this project name is FUN-ECM is that FUN means Future University Hakodate and ECM means Elliptic Curve Method that is a best algorithm for prime factorization.

1.2 背景 Background

約40年前に RSA暗号※1が登場し、安全な電子商取引が可能となった。RSA暗号の安全性は公開鍵の素因数分解の困難さ等価であると考えられるため, RSA暗号の普及以降、素因数分解実験は重要なテーマとなっている。本プロジェクトが素因数分解法の中でECMを対象とする理由は、最良法の1つであることや並列実装のしやすさ、近年普及している楕円曲線暗号(ECC)※2が関連しているためである。

※1 素因数分解が困難であればあるほど安全である公開鍵暗号の一つ。
※2 楕円曲線上の離散対数問題の困難性を安全性の根拠とした公開鍵暗号の一つ。ECMと楕円曲線暗号のアルゴリズムは類似している。

RSA encryption ※1 was developed at 40 years ago, and secure e-commerce has become possible. Prime factorization experiments have become an important theme since the spread of RSA. Because the security of RSA cryptosystem is considered to be equivalent difficulty in prime factorization of public key". We have three reasons that prime factorization among ECM is selected. First, it is one of the best methods. Second, it is easy to implement in parallel. Third, elliptic curve cryptography (ECC) ※2 have become widespread relate in recent years.

※1 RSA is one of public key cryptographies. RSA is based on the hardness of prime factorizations.
※2 ECC is one of public key cryptographies. ECC is based on the hardness of elliptic curve discrete logarithm problems. Algorithm for ECM is similar to one of ECC.

1.3 目的 The purpose

- ECMを利用した素因数分解のプログラムの作成
- 素因数分解チャレンジECMNETにランクイン(※1)
- STUDIO KAMADA(※2)にランクイン
- 活動や結果を発信・報告するサイトを作成

- Making of program for prime factorization using ECM.
- Ranking in ECMNET, which is a factorization challenge
- Ranking in STUDIO KAMADA.
- Making a website to report activities and results

※1:ECMNETの目的は、主にECMにより大きな合成数の因数を見つけることで Cunningham projectに貢献すること。(詳細はQRコードを参照)

The purpose of ECMNET is to find large factors by ECM, mainly by contributing to the Cunningham project.

URL: https://members.loria.fr/PZimmermann/records/ecmnet.html

※2:STUDIO KAMADAの目的は、ニアレプディジット(ゾロ目の自然数)関連の数の素因数分解表を作成する。(詳細はQRコードを参照)

The purpose of STUDIO KAMADA is to create a prime factorization table of numbers related to near replicates (natural number of Repdigit).

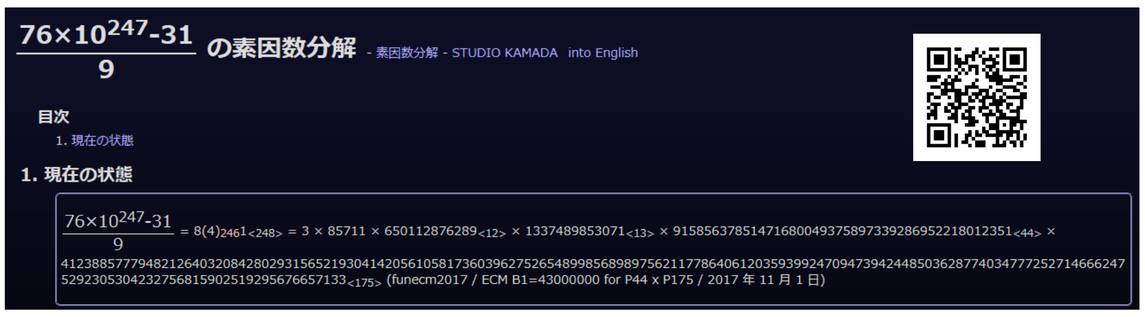
URL:http://stdkmd.com/nrr/#summary

ECMNET

STUDIO KAMADA

1.4 今期活動成果

STUDIO KAMADAに載っているまだ素因数が
見つかっていなかった合成数2つの素因数分解に成功した。
詳細は、QRコードを参照。



2. 活動内容

2.1 年間スケジュール