【2014/最終】プロジェクトNo.8・素因数分解・担当教員 白勢政明・由良文孝

素因数分解 Prime factorization

今井 啄人 Takuto Imai　木村 純平 Junpei Kimura　上戸 真裕 Masahiro Ueto　佐藤 康太郎 Kotaro Sato　狩野 大樹 Taiki Karino　清水目 佳樹 Yoshiki Shimizume　吉田 努 Tsutomu Yoshida　小濱 拓也 Takuya Kohama

概要 Abstract

目的 Purpose

本プロジェクトの目的はできるだけ大きい素因数を見つけることである。

To discover prime factor is as much as possible.

背景 Background

現在、公開鍵暗号においてRSA暗号がよく使われている。RSA暗号は桁数の大きな素因数の分解の困難性を利用した暗号方式である。RSA暗号の安全性は素因数分解の困難性によって評価できる。その素因数分解の最も優れた解法の一つに楕円曲線法(ECM)がある。私たちはこのプロジェクトで、楕円曲線法による素因数分解プログラムの高速化とアルゴリズムの改良を目指している。また、楕円曲線法を用いて大きい素因数を見つけることを目的とする「ECMNET」というサイトがある。現在記録されている素因数よりも大きい素因数を見つけることで、ECMNETのランキングに名前を載せることができる。私たちは、ランクインしている素因数を参考にし、より大きな素因数を発見することが目的である。

Recently, RSA encryption is widespread on the world. This is related to the security of the RSA encryption(use of the combination of the factorization). RSA encryption can be evaluated safety by the prime factorization. Elliptic curve method is one of the best method to solve that. We aim at the acceleration of the program and improving the algorithm in our project. The site "ECMNET" ranking. ECMNET ranking. This site can record the anyone's name who get bigger factor than before one. We would like to discover the bigger one than recorded at ECMNET.

成果 Product

私たちは前期にECMのための基礎学習を行った。後期は理論班とプログラミング班に分かれて活動した。

We activie to run basic studies of ECM at first semester. Second semester, we were activities divided into group theorem and group program.

理論班 Algorithm group

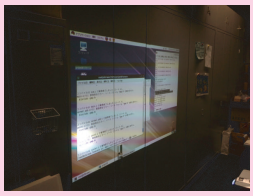
理論班は、ECMプログラムの計算量を減らすための手法を調べ、その手法が正しいかどうか検証した。調べた結果、射影座標系によって計算量を減らせることがわかった。そのため射影座標系について記述してある論文を理論班で輪読した。論文中の理論を自分たちの手で確認することにより、その内容を理解することができた。その結果、射影座標系を導入することにより計算量を約1割減らすことができることを確認した。

Algorithm group examined the methods for reducing computational complexity of the ECM program and verified what it is exactly. We found that projective coordinate system reduce the computational complexity. Algorithm group have read the monograph about projective coordinate system. We verified theories in the monograph and understood it. As a result, it was possible to reduce about 10% the amount of calculation by introducing a projective coordinate system.

プログラミング班 Programming group

プログラミング班は、前期に作成したECMプログラムをより高速に大きな桁数の素因数分解できるように改良した。まず一つ目に、GMP(GNU Multi-precision Library)を導入した。これにより任意桁数での計算が可能になった。二つ目に、射影座標系での計算プログラムを作成した。三つ目に、XeonPhi上でプログラムを並列処理するためにOpenMPを導入した。これにより約240スレッドで並列処理できるようになった。

Programming group improved a ECM program that we made in last term to solve high speed. Firstly, we import GMP to calculate in any number of digits. Secondly, we create a calculation program in projective coordinate system. Thirdly, we introduced OpenMP to parallel processing programs on XeonPhi. Therefore, it is possible to parallel processing at about 240 threads.



まとめ Conclusion

結果 Result

後期の目的としてのECMプログラムの改良を行うことは出来た。しかし、ECMNETのランキングに名前を載せるという目的は達成することが出来なかった。この目的を達成するためには65桁以上の素因数を見つけることが必要であるが、まだ私たちは31桁までしか発見することが出来なかった。大きな素因数を見つけるには時間をかける必要があるため、私たちは1月中まで挑戦を続けていく予定だ。

We achieved the goal of improving. However, we did not put in a ranking of ECMNET. It is necessary to find the 65 or more digits of the prime factors. However, we discovered one of only 31 digits. We take time to find a large prime factor. Therefore, we will continue to challenge it until in January.

問題点 Problem

・プログラミングに時間がかかってしまったため、実装にまで至らなかった手法がいくつかあった
・11月上旬でプログラムを完成させる予定だったが、2週間遅れて完成したためプログラムを実行する時間が足りなかった

・We've takes time to programming. Therefore, there were methods that we cannot implement.
・We had scheduled to complete the ECM program in early November. Because it was the middle of November that the program was completed, we didn't have enough time we executed program.

表についてもこの位置の範囲におさまるのが望ましい

Introduction

開鍵暗号においてRSA暗号がよく使われている。RSA暗号は桁数の大きな素因数の
SA暗号の安全性は素因数分解の困難性によって評価できる。その素因数分解の最も
る。私たちはこのプロジェクトで、楕円曲線法による素因数分解プログラムの高速化
円曲線法を用いて大きい素因数を見つけることを目的とする「ECMNET」というサイト
い素因数を見つけることで、ECMNETのランキングに名前を載せることができる。私た
)大きな素因数を発見することが目的である。

RSA encryption is widespread on the world. This is related to the security of the RSA encryptio
). RSA encryption can be evaluated safety by the prime factorization. Elliptic curve method is
celeration of the program and improving the algorithm in our project. Therefore, we challenge
ord the anyone's name who get bigger factor than before one. We would like to discover the bi

文章・図表とも右端はこの

成果 Product

期にECMのための基礎学習を行った。後期は理論班とプログラミング班に分かれて
run basic studies of ECM at first semester. Second semester, we were activities divided into g

班 Algorithm group

本文スペース

は、ECMプログラムの計算量を減らすため[illegible]手法を調べ、その手法が正しいかどうか
、調べた結果、射影座標系によって計算量を減らせることがわかった。そのため射影
ついて記述してある論文を理論班で輪読した。論文中の理論を自分たちの手で確認
により、その内容を理解することができた。その結果、射影座標系を導入することにより
約1割減らすことができることを確認した。

m group examined the methods for reducing computational complexity of the ECM program ar
at it is exactly. We found that projective coordinate system reduce the computational complex
group have read the monograph about projective coordinate system. We verified theories in th
and understood it. As a result, it was possible to reduce about 10% the amount of calculation
g a projective coordinate system.

プログラミング班 Programming group

ラミング班は、前期に作成したECMプログラムをより高速に大きな桁数の素因数分解
うに改良した。まず一つ目に、GMP(GNU Multi-precision Library)を導入した。
の任意桁数での計算が可能になった。二つ目に、射影座標系での計算プログラムを
、三つ目に、XeonPhi上でプログラムを並列処理するためにOpenMPを導入した。
の約240スレッドで並列処理できるようになった。

ming group improved a ECM program that we made in last term to solve high speed. Firstly, w
P to calculate in any number of digits. Secondly, we create a calculation program in projective
system. Thirdly, we introduced OpenMP to parallel processing programs on XeonPhi. Therefo
le to parallel processing at about 240 threads.