FUN-ECM プロジェクト

FUN-ECM Project

山本健太 石川夏樹 小野嘉翔 九島拓実 土田祐介 辻田陸

Kenta Yamamoto　Natsuki Ishikawa　Yoshiharu Ono　Takumi Kushima　Yusuke Tsuchida　Riku Tsujita

プログラム班

活動目的

ECMプログラムの高速化と並列化を実現し素数を発見する確率を高めるためにECMプログラムの改良を目指す。高速化には理論班が作成した射影変換のアルゴリズムとエドワーズ曲線をプログラムに組み込み、並列処理するプログラムの実装した。

並列化とは

並列化とは、同時に複数の処理を行うことである。並列処理していない場合、プログラムの処理は 1 つずつ逐次実行される。一方、並列処理をした場合、複数の処理を並行して行うことができるため、処理終了までの時間を短縮できる。並列処理は、XeonPhi上で行う。XeonPhiとは、60個のコアを持つコプロセッサーで、ホストCPUとしてXeonが必要となり、今回はXeonPhiを搭載したコンピュータを使用した。XeonPhiを用いることで、楕円曲線法の処理を240個まで同時に行うことができる。ECMプログラムを並列化し高速化を図っている。

図1 並列化の利点

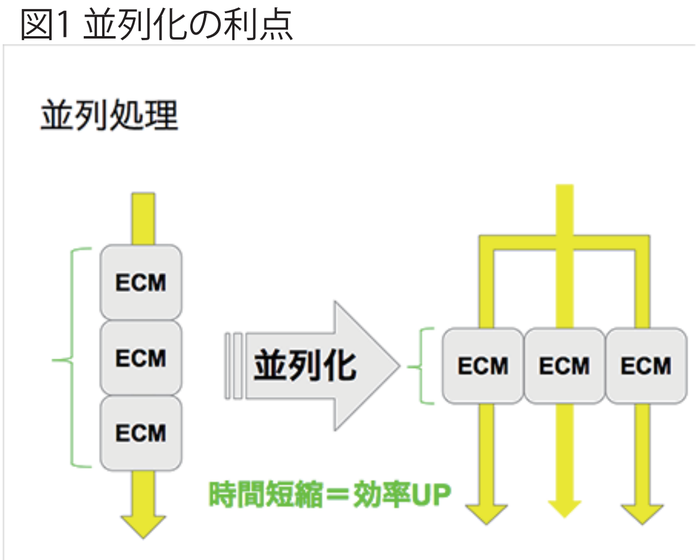

図2 XeonPhiを搭載したコンピュータ

多倍長計算を行うために

数値計算にはGMPを利用した。GMPとは多倍長計算を高速に行えるC言語算術ライブラリで、ECMで大きな桁数の素因数を見つけようとする場合100桁以上の非常に大きな数を扱うため、C言語の基本のデータ型では制限があるのでGMPを使用することでこの問題を解決した。

活動成果

実装したプログラムの性能評価として、40桁の素数同士の積、79桁の合成数を素因数分解したところ、2時間13分ほどで素因数を発見できた。ECMNETにランクインできるのが65桁以上のため、65桁の素因数の発見を目標にプログラムを動かし続けている。

活動過程

	9月 Sep.	10月 Oct.	11月 Nov.	12月 Dec.	1月 Jan.
統計班 Statistics team	統計方法決定 Determine statistical strategy		統計調査 Statistical survey	まとめ Summary	
射影班 Projection team	射影変換の学習 Learning of projective transformation		計算コスト評価 Asseasment of calculation cost	統計班と合流 Join statistics team	
プログラム班 Program team	プログラム実装 Implement a program		ECMNETに挑戦 Challenge to ECMNET		