FUN-ECMプロジェクト

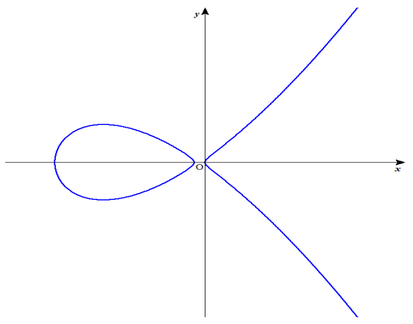
FUN-ECM Project

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

3.3 アルゴリズム

3.3.1 Montgomery曲線について

Montgomery曲線とは、$By^2 = x^3 + Ax^2 + x$ という式から表される曲線である。メリットとして、y座標を保存する必要がなくなるため、Weierstrass曲線と違って、y座標を用いずに計算を出来るようになる。デメリットとして今まで使用した曲線と違って$P - Q$の点を用意する必要がある。



Montgomery曲線

Montgomery曲線の座標の計算ついて

・2点同士の加算

点PとQを加算するためには以下のアルゴリズムに従って加算を行う。
点$P = (Xp : Zp)$,点$Q = (Xq : Zq)$とする。$P_0 = (Xp - q : Zp - q) = P - Q$とする。
これらを用いて計算を行う。

- **Montgomery ladder**

Montgomery ladderはMontgomery曲線のスカラー倍を効率よく行うためのアルゴリズムである。

3.3.2 Baby-Step Giant-Step法（以下,BSGS）について

去年までは、Stage2の部分では効率の悪い総当り法が実装されていた。
そこで今年は、より速く計算できるBSGSを実装した。

BSGSとは？

$B_1 < s < B_2$を満たす全ての素数を$s_1, s_2, s_3, ..., s_k$，Stage1の結果で得られた点Pとして、
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$s * Q = O$のとき成功する。この式を変形していく。$s = 210 * v + u\ (-105 < u < 105)$ とすると
$(210 * v) * P = -u * P$ となる。
この式を満たせばよいので、楕円曲線の逆元の定義より、$\mathrm{mod}\ p$上で、右辺と左辺のx座標が等しい。
$(210 * v) * P$のx座標をGx、 $-u * P$のx座標をHxとすると
$Gx \equiv Hx\ (\mathrm{mod}\ p)$となり、これは$Gx - Hx \equiv 0\ (\mathrm{mod}\ p)$を意味し、
$(Gx - Hx)$がpの倍数となる。ここで、全てのsについて$(Gx - Hx)$を計算し、
すべてを掛け合わせた数をdをすると、$Gx - Hx \equiv 0\ (\mathrm{mod}\ p)$となる$s$が存在すれば、$d \equiv 0 (\mathrm{mod}\ p)$となる。
そのため、dと合成数Nの最大公約数を求めることでpが判明する。

3.3.3 素数ペアリングについて

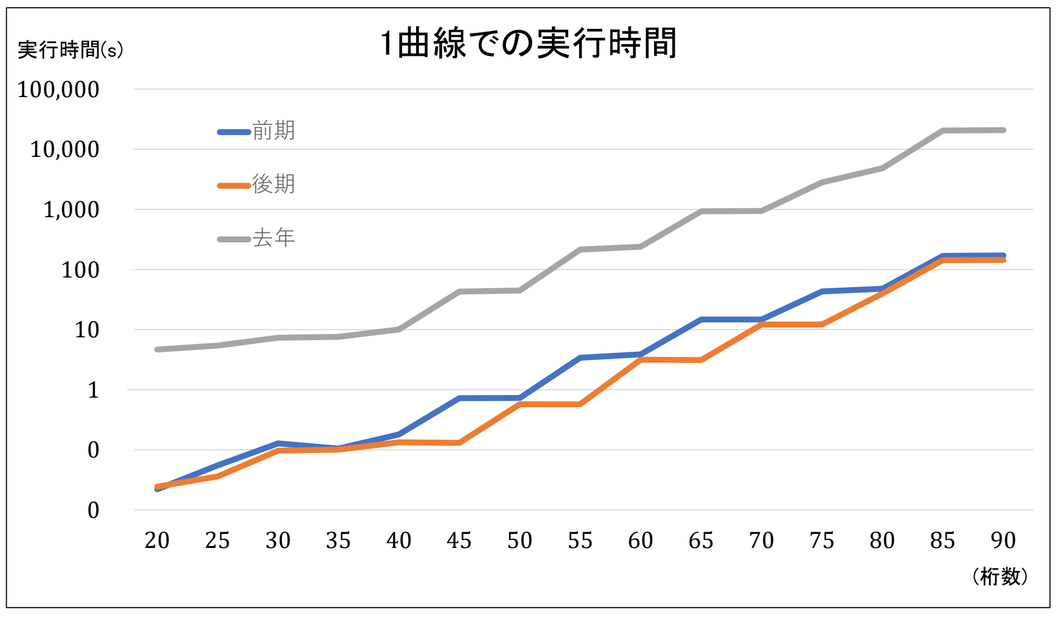
BSGSをより高速化する手法として、素数ペアリングがある。

$(210 * v) * P = -u * P$ ⋯ ☆

☆式の計算をについて考える。
楕円曲線の逆元の定義より、$-u * P$ と $u * P$は、x軸に対して対称であり、x座標の値が等しい。よって、$(Gx - Hx)$ の値は同じになる。
もし、$210 * v + u,\ 210 * v - u$ がともに素数だったとき、従来の計算手法だと、同じ計算を二重に行うことになり効率が悪い。
そこで、$210 * v + u$ と $210 * v - u$ がともに素数になるペアを計算し、sがどちらかの時のみ$(Gx - Hx)$ を求める。
これにより、試行回数が減るため高速化することができる。

☆式はこのようにも変形可能である。
もし、$s = 210 * v + u$ は素数だったが、$210 * v - u$ が素数でないためにペアリングできなかったときに、
$s = 210 * v + u = 210 * (v - 1) + (210 + u) = 210 * (v - 2) + (2 * 210 + u) = 210 * (v - 3) + (3 * 210 + u) = \cdots$
と考えることで、より深くペアを探すことができ、ペアの数が増え、試行回数がより減るため、BSGSの高速化が期待できる。
ただし、☆式の右辺が増える分、多くの事前計算が必要となるため、注意が必要になる。

4. 計測結果



去年と今年の前期と後期に作成したそれぞれのプログラムの1つの楕円曲線にかかる計算時間の平均を比較した。
1つの楕円曲線にかかる計算は今年度に作成したプログラムが去年のプログラムより約80倍速度が向上した。
今後の展望として、符号付き2進展開法を実装し、新たなアルゴリズムを実装して素因数を見つける速度を高めていきたい。
ECMNETにランクインすることを試みる。その為、少なくとも桁数128桁以上の合成数の素因数分解をする必要がある。
(2017/12/6 現在)