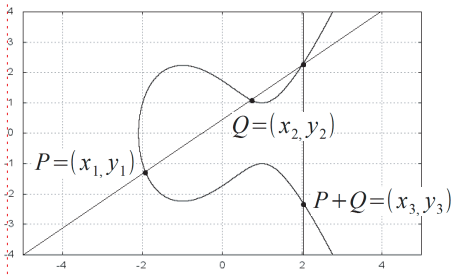
素因数分解 Prime factorization 理論班

グループリーダー 上戸 真裕 Masahiro Ueto　木村 純平 Junpei Kimura　狩野 大樹 Taiki Karino　清水目 佳樹 Yoshiki Shimizume

私たちは楕円曲線法を用いた素因数分解について、計算量を削減させる事を目的に活動した。逆元計算は計算上大きな負荷になるため、いかに逆元計算の回数を減らす事ができるかに注目し以下の方法を用いて検証した。

←【文章設定限界】
文章の左端をこのラインに揃えること
また図表についてもこの位置の範囲におさまるのが望ましい

楕円曲線$E: y^2=x^3+ax+b\left(a,b\in K, 4a^3+27b^2\neq 0\right)$に対し、$P+Q$ を求める式



射影写像とは:
２次元の直交座標系において３個の変数を用いる。

$$(x,y)^T\rightarrow(X,Y,Z)^T$$

右辺全体をZで割る事で$(X/Z,Y/Z,1)$となり線形性から

$$(X/Z,Y/Z,1)^T\rightarrow(x,y)^T$$

ともとの直交座標系に戻るという特性を利用する。

【右端限界】→
文章・図表とも右端はこのラインに揃えること

（図版拡張スペース）

直交座標系の手法:

$$P=(x_1,y_1)$$
$$Q=(x_2,y_2)$$
$$P+Q=(x_3,y_3)$$
$$\begin{cases}\lambda=\dfrac{y_1-y_2}{x_1-x_2}\\ x_3=\lambda^2-x_1-x_2\\ y_3=\lambda(x_1-x_3)-y_1\end{cases}$$

本文スペース

射影座標系の手法:

$$P=(X_1,Y_1,Z_1)$$
$$Q=(X_2,Y_2,Z_2)$$
$$P+Q=(X_3,Y_3,Z_3)$$
$$\begin{cases}X_3=vA\\ Y_3=u(v^2X_1Z_2-A)-v^3Y_1Z_2\\ Z_3=v^3Z_1Z_2\end{cases}$$
$$v=X_2Z_1-X_1Z_2$$
$$u=Y_2Z_1-Y_1Z_2$$
$$A=u^2Z_1Z_2-v^3-2v^2X_1Z_2$$

計算コストの比較をしてみると

直交座標系の $P+Q$ のコスト: $I+2M+S\approx 14.8M$

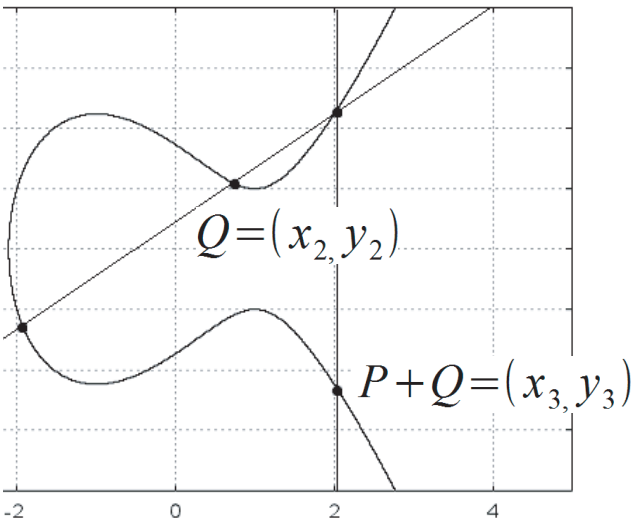
射影座標系の $P+Q$ のコスト: $12M+2S\approx 13.6M$

掛け算(M):M
2乗算(S):0.8M
逆元計算(I):12M

←【図表設定限界】
レイアウトの仕方によって図表の左端が
【文章設定限界】をこえる場合、
このラインまで図表の位置を拡張してもよい

楕円曲線$y^2=x^3+ax+b\left(a,b\in K, 4a^3+27b^2\neq 0\right)$において射影座標系を導入することにより約1割の高速化をすることができた。

表についてもこの位置の範囲におさまるのが望ましい



射影写像とは：
２次元の直交座標
変数を用いる。

$$(x, y)^T \rightarrow ($$

右辺全体をZで割
となり線形性から

$$(X/Z, Y/Z, .$$

ともとの直交座標
を利用する。

文章・図表とも右端はこの

系の手法：

(x_1, y_1)

(x_2, y_2)

$=(x_3, y_3)$

$\dfrac{y_1-y_2}{x_1-x_2}$

$\lambda^2-x_1-x_2$

$\lambda(x_1-x_3)-y_1$

本文スペース

射影座標系の手

$P=(X_1, Y_1, Z_1)$

$Q=(X_2, Y_2, Z_2)$

$P+Q=(X_3, Y_3, Z$

$$\begin{cases} X_3=vA \\ Y_3=u(v^2 \\ Z_3=v^3 Z_1 Z \end{cases}$$

$v=X_2Z_1-X_1Z$

$u=Y_2Z_1-Y_1Z$

$A=u^2Z_1Z_2-v^3$

トの比較をしてみると

系の $P+Q$ のコスト：　$I+2M+S \approx 14.8M$

掛