# 自主課題研究
# ガウス整数による ElGamal 暗号

0608060947 情報システム工学科 3 年 076 美多佑樹

平成 21 年 2 月 16 日

## 1　ElGamal 暗号

ElGamal 暗号とは、公開鍵暗号のひとつである。同じ公開鍵暗号の RSA 暗号は、素因数分解の困難性を安全性の根拠としているが、ElGamal 暗号は、離散対数問題の困難性を安全性の根拠としている。離散対数問題の困難性とは、$(a, b), b = a^x \bmod n$ が与えられたときに、$x$ を求めることが困難であるという性質のことである。

ElGamal 暗号は、整数の剰余類だけでなく、一般の巡回群に拡張することができる。例えば、楕円曲線上の有理点を元として、元の間の加算と乗算を定義した巡回群に適用したものが、楕円曲線暗号である。このことは、ある巡回群における離散対数問題が解かれたとしても、依然として他の巡回群における ElGamal 暗号は有効であり続けるという利点がある。本稿では、後述するガウス整数における剰余類についての ElGamal 暗号について述べる。

## 2　ガウス整数

整数 $a, b$ について、複素数 $\alpha = a + bi$ をガウス整数という。ガウス整数には、加法と乗法が定義でき、ガウス整数全体の集合をガウス整数環という。

除法の原理より、$\alpha = \beta\gamma + \rho, \rho = 0 \vee N(\rho) < N(\beta)$ を満たす $\gamma, \rho$ が存在する。これより、ガウス整数の剰余を定義した。また、ガウス整数における因数分解によって、ガウス素数が考えられ、フェルマーの定理が成り立つことを確認した。これにより、ガウス整数の剰余類は、巡回群を作ることができることがわかった。

## 3　ガウス整数による ElGamal 暗号

ガウス整数の実部を x 座標、虚部を y 座標とすれば、ガウス整数を平面上の点として見ることが出来る。そこで、ガウス整数による ElGamal 暗号の例として、2 値画像の各点を平文として、暗号化することを試みた。そのために、Visual C++を用いて、ガウス整数のクラスを定義し、暗号化するプログラムを製作した。

## 4　まとめ

ガウス整数による ElGamal 暗号を考える上での利点としては、有理整数における既存の資産を利用することが出来ることがある。ひとつは、ガウス素数は既知の有理整数から求めることが出来ることである。もうひとつは、有理整数の領域で考えていた巡回群を、ガウス整数の領域に拡張することが出来ることである。例えば、RSA 暗号からは、ガウス整数による RSA 暗号を考えることが出来る。また、楕円曲線における x 軸と y 軸をガウス整数に拡張することによって、新たな有理点が考えられ、これによって新しい楕円曲線暗号を構成することが出来ると思われる。