平成２４年度卒業研究概要

RSA 暗号に関する研究

中等教育教員養成課程　数学専攻　成瀬 公志郎

暗号とは, メッセージを第三者には秘匿し, 意図した受信者だけが判読できるような形にする秘密通信手段のことである. もとのメッセージを平文, 第三者に秘匿する形にしたメッセージを暗号文という. 平文を暗号文に変換するアルゴリズムを暗号化といい, 暗号文を平文に変換するアルゴリズムを復号化という. 本論文の目標は, 次に述べる暗号化, 復号化の 2 つのアルゴリズムを紹介し, そのアルゴリズムによって暗号化され, 復号化されたメッセージが暗号化する前の平文と一致することを確認することである.

暗号化のアルゴリズム. 数字列 A を次の手順で暗号化する.

1. $m = pq$ (p, q は異なる素数) と $\gcd(\varphi(m), k) = 1$ である k を選ぶ.
2. A を数字列が m 未満となるように区切り, $a_1,\ a_2,\ \ldots\ ,\ a_r$ $(0 < a_i < m)$ とおく.
3. $a_1^k \pmod m,\ a_2^k \pmod m,\ \ldots\ ,\ a_r^k \pmod m$ を計算し, それらを $b_1,\ b_2,\ \ldots\ ,\ b_r$ $(0 < b_i < m)$ とする.
4. $b_1,\ b_2,\ \ldots\ ,\ b_r$ を送信する.

復号化のアルゴリズム. $b, k, m \in \mathbb{N},\ \gcd(b, m) = 1,\ \gcd(k, \varphi(m)) = 1$ に対し, 以下のステップは合同式 $x^k \equiv b \pmod m$ の解を与える.

1. $\varphi(m)$ を計算する.
2. 方程式 $ku - \varphi(m)v = 1$ を満たす正の整数解 u, v を求める. (合同式 $ku \equiv 1 \pmod{\varphi(m)}$ を満たす正の整数解を求める.)
3. $x \equiv b^u \pmod m$ を計算する.

この 2 つのアルゴリズムを使い, メッセージを送受信する一連の過程を RSA 暗号という.

上記アルゴリズムにおいて, 復号化されたメッセージが暗号化する前の平文と一致することは, 次の 2 つの命題を用いて示される.

命題 4. $b, k, m \in \mathbb{N},\ \gcd(b, m) = 1,\ \gcd(k, \varphi(m)) = 1$ とする. また, $ku - \varphi(m)v = 1$ を満たす正の整数解を u, v とする. このとき $x \equiv b^u \pmod m$ を満たす x は $x^k \equiv b \pmod m$ の解である.

命題 5. $b, k, m \in \mathbb{N},\ \gcd(b, m) = 1,\ \gcd(k, \varphi(m)) = 1$ に対し, m を法とした b の k 乗根は高々1 つである.

また, 本論文では, 具体的な数を用いていくつかの例を見ている.