暗号用の乱数の研究

福井県立武生高等学校　吉崎琥珀　奥山颯太　萩原瑠大　落合翔大　石坂仁

はじめに

暗号には乱数を使うものがある。しかし、大量の乱数を必要とするので、合同式と漸化式を用いることによって擬似的に乱数を作る方法が採用されている。この漸化式は周期を大きくするために、法の値を大きくする必要がある。私達は、法の値を大きくせずに床関数を用いた数列の周期を考えることにした。

研究方法

注　$x \in \mathbb{Q}$、⌊x⌋(床関数)をx以下の最大の整数と定義する。

周期を「任意の正の整数iに対して、$a_i = a_{i+r}$ となる最小の正の整数r」と定義する。

(Ⅰ):線形合同法の数列 $a_{n+1} = xa_n + y \bmod z,\ a_1 = f$　…①　の周期がどのようになっているか考える。

(Ⅱ):①で求めた一般項に床関数を導入する。

(Ⅲ):床関数を入れた数列の周期と線形合同法の数列の周期を比較して、どれくらい変化しているか考える。

研究結果

作った漸化式（以下②と呼称）

$$b_{n+1} = xb_n + (x-1)u - \left\lfloor \frac{n}{s} \right\rfloor + x\left\lfloor \frac{n-1}{s} \right\rfloor \bmod z,\ b_1 = t - u + z \bmod z$$

この漸化式の性質

②の周期は $LCM(s, z, z-1)$ である。
a_{R_2} までならば、②の漸化式は均等分布する。（未証明）
②は①よりも周期の値を大きくしやすい。
①は同じ値を連続で出すことがないが、②は連続で同じ値を出すことがある

式の導出方法

①の漸化式において $t = f + \frac{y}{x-1}$, $u = \frac{-y}{x-1}$ とおくと、　$a_n = tx^{n-1} + u \bmod z$

①の一般項から、$x^{n-1} \bmod z$ の値のみ①の周期に関わっていることがわかる。また、フェルマーの小定理を考えると、①の周期は最大でもzということが分かる。ここで、床関数を加える。

$\lfloor \frac{n}{s} \rfloor$ はnが+sされるごとに値が変化する。この「+sされるごとに変わるという性質」を周期に利用する。modを除いた①の一般項から $\lfloor \frac{n-1}{s} \rfloor$ を引き、再度modを加えた数列を b_n とすると b_n の一般項は $b_n = tx^{n-1} - \lfloor \frac{n-1}{s} \rfloor - u \bmod z$ 。これを漸化式にすると②になる。

考察・今後の課題

乱数の乱雑さを測る方法を調べても高校数学では太刀打ちできなかったので、周期を求めることにしたのだが、想像できない結果になった。今後の課題としては、証明の方法を考える。また、簡単な線形合同法は暗号に向いていないことが分かっているが、この漸化式が暗号に向いているか分からないので、これも調べていきたい。

・【数表】500以下の素数の原始根一覧” . https://blog.thetheorier.com . 2016 . https://blog.thetheorier.com/entry/primitiveroot-list#google_vignette .
・ニューアクション編集委員会 . NEW ACTION LEGEND 数学Ⅱ+B 令和4年度新課程版 . 東京書籍 , 2022 .　・IPUSIRON . 暗号技術のすべて . 翔泳社 , 2017 .
・光成滋生 . 図解即戦力 暗号と認証のしくみと理論がこれ1冊でしっかりわかる教科書 . 技術評論社 , 2021 .　・Wolfram|Alpha: Computational Intelligence” . Wolfram|Alpha . 2009 . https://ja.wolframalpha.com .