研究班番号【86】

フェルマーテストを用いた確率的素数判定の正確性

数学班:柚木 平蔵

1. はじめに

RSA暗号は、LINEのトークの暗号化などに利用されており、巨大な素数の積を鍵とし、その数の素因数分解が難しいことを利用した暗号である。しかし、その数が簡単に解かれてしまうような小さな素数の積であれば、暗号としては機能しない。そこで、鍵となる巨大な数が、小さな素因数を持たない可能性が高いことを、素数判定を用いて、その数の素因数が大きな素数であると言うことで、暗号として機能することをある程度期待できると言えるのではないかと考えた。

図1 フェルマーテスト

①2≦a＜nの任意の自然数aを決める(aとnは互いに素)

②$a^{n-1} \not\equiv 1 \pmod{n}$　→nは合成数

③$a^{n-1} \equiv 1 \pmod{n}$　→nは確率的素数

2. 実験方法

今回は、素数判定にフェルマーテストを用いる(図1)。
フェルマーテストは、右図の手順で行うものであり、
③を満たした場合、nは素数であることがある程度
期待できる「確率的素数」となる。
今回の研究では、図1の③を満たした場合に、nが
実際に素数である確率が具体的にどの程度期待できるのか、
また、③を満たすようなa,nの組に規則性(aの個数、aとnの
関係性など)はあるのかについて調べた。

3. 結果

定理(右図)より、1回の試行で③を満たしたとき、
nが合成数である確率は、1/2以下であることがわかる。
つまり、③を満たしたとき、nが素数である確率は
1/2以上になる。また、nに19、21、35などの
自然数をいくつか代入してaとnとの関係性や
③を満たすaの個数について調べたが、規則性は
見られなかった。

定理:図1の③を満たすaは(n-1)/2個以下

4. 考察

1回の試行で、「nが確率的素数」と判定した際、nが素数である確率が1/2以上であることから、
他にもaを代入して、「確率的素数」という判定を何度も得ることで、nが素数である確率は大いに
上がると期待できる。

5. まとめ

今回の研究では、かなり大雑把な値しか出すことができなかった。他にも位数や公約数など様々な視点から規則性が見られないか調べていきたい。

6. 参考文献ならびに参考Webページ

「ミラー・ラビン素数判定 - 37zigenのHP」