素因数分解

東京都立戸山高等学校 SSII数学 白石彩花

動機

　数学の問題で素因数分解をするとき、もっと速く簡単に素因数分解できないのかと思ったため、素因数分解の研究を始めた。研究について調べるうちにRSA暗号を知ったので、それに関する研究を始めた。

前回までの研究

　3桁の数字について、2~11までの数字の何で割れるのかを見抜く方法を探した。

RSA 暗号とは

　桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つ。デジタル署名などに使われている。
⇒本当に解読は困難なのか？

研究内容・方法

　コンピューターの素因数分解の速度を調べ、規則性を見つける。

1 ,Pythonを用いて素因数分解のプログラムを作成
2 ,プログラムを実行
3 ,素因数分解にかかる時間を計測

仮説

①元の数の桁が大きくなるとその分時間がかかる
②因数が数の大きいものほど時間がかかる
③因数の個数が多いものほど時間がかかる

検証

　今回は以下のようなプログラムを使用し、2桁～5桁の素因数分解をそれぞれ行った。
今回は仮説①のみの検証である。

```python
import random
n = random.randint(100000,999999)
def prime_factorize(n):
    a = []
    while n % 2 == 0:
        a.append(2)
        n //= 2
    f = 3
    while f * f <= n:
        if n % f == 0:
            a.append(f)
            n //= f
        else:
            f += 2
    if n != 1:
        a.append(n)
    return a
print("number=",n)
print(prime_factorize(n))
```

↓プログラムを実行すると..

```
number= 7
[7]

number= 54
[2, 3, 3, 3]

number= 2400
[2, 2, 2, 2, 2, 3, 5, 5]
```

↑Pythonで作った素因数分解のプログラム(5桁の数の場合)

結果・考察

　以下の表のような結果となった。

・2桁は1.4秒台、3,4,7桁が1.5秒台、5,6,8,9が1.61秒台となった。
⇒どれも1秒台で速いので、より大きな桁数の数字でもかなりのスピードで素因数分解ができるのではないか

・相関係数を計算したところ0.83367となり、正の相関関係があることが分かった。
⇒桁が大きいほど素因数分解には時間がかかる。

	2	3	4	5	6	7	8	9
1	1.75	1.54	1.51	1.5	1.6	1.79	1.58	1.57
2	1.61	1.63	1.59	1.61	1.64	1.53	1.45	1.73
3	1.53	1.59	1.25	1.59	1.64	1.63	1.76	1.59
4	1.74	1.45	1.31	1.62	1.58	1.49	1.78	1.75
5	1.61	1.58	1.53	1.68	1.59	1.47	1.77	1.64
6	1.65	1.56	1.63	1.56	1.65	1.52	1.78	1.69
7	1.25	1.56	1.58	1.54	1.58	1.57	1.68	1.71
8	1.27	1.61	1.55	1.68	1.65	1.43	1.66	1.7
9	1.17	1.65	1.56	1.67	1.61	1.55	1.6	1.65
10	1.31	1.47	1.58	1.73	1.62	1.65	1.73	1.62
計	14.89	15.64	15.09	16.18	16.16	15.63	16.79	16.65
平均	**1.489**	**1.564**	**1.509**	**1.618**	**1.616**	**1.563**	**1.679**	**1.665**

↑2～9桁までの数字の素因数分解の速さ(単位：秒)

今後の展望

・計測したデータが手作業のため正確ではないので、機械やプログラミングを用いて測るなど工夫したい。
・この検証結果をRSA暗号の研究にどのように活用していくか検討したい。
・RSA暗号についてまだ理解できていない部分も多いので、理解を深めていきたい

参考文献

Wikipedia「試し割り法」
https://ja.wikipedia.org/wiki/%E8%A9%A6%E3%81%97%E5%89%B2%E3%82%8A%E6%B3%95
(プログラム作りの参考にした)

高校数学の美しい物語
「RSA暗号の仕組みと安全性」
https://manabitimes.jp/math/1146