レポート数学2班

「惜しいフェルマーの最終定理」

六鎗大翔　川崎知己　佐藤祐紀　千田至恩

指導教員　　千葉将仁先生　高橋寿彦先生　佐々木一也先生

ピエール・ド・フェルマー　　仏(1607~1655)

フランスの数学者兼裁判官。彼にとって数学は趣味の一つであり、数学書を読んでは思いついたことをその余白に記す習慣があった。フェルマーの最終定理もその一つである。

1　はじめに

「n が 3 以上のとき、$X^n+Y^n=Z^n$ を満たす自然数 X,Y,Z は存在しない」これは言わずと知れた「フェルマーの最終定理」である。私達はこの定理に興味を持ち、本当に n が 3 以上のとき、そのような X,Y,Zは存在しないのか調べてみた。すると、$X^n+Y^n=Z^n$ を満たす X,Y,Z は見つけることは出来なかったが、$X^n+Y^n=Z^n$ に 1 だけ足りなかったり、1 だけ多かったりする組は多く見つかった。「フェルマーの最終定理はすでに証明されたが、このような惜しい組には何らかの規則性があるのではないか」と考え、そのような惜しい組たちが満たす等式 $X^n+Y^n=Z^n\pm1$ を「惜しいフェルマーの最終定理」と名付け、研究をはじめた。

フェルマーの最終定理とは

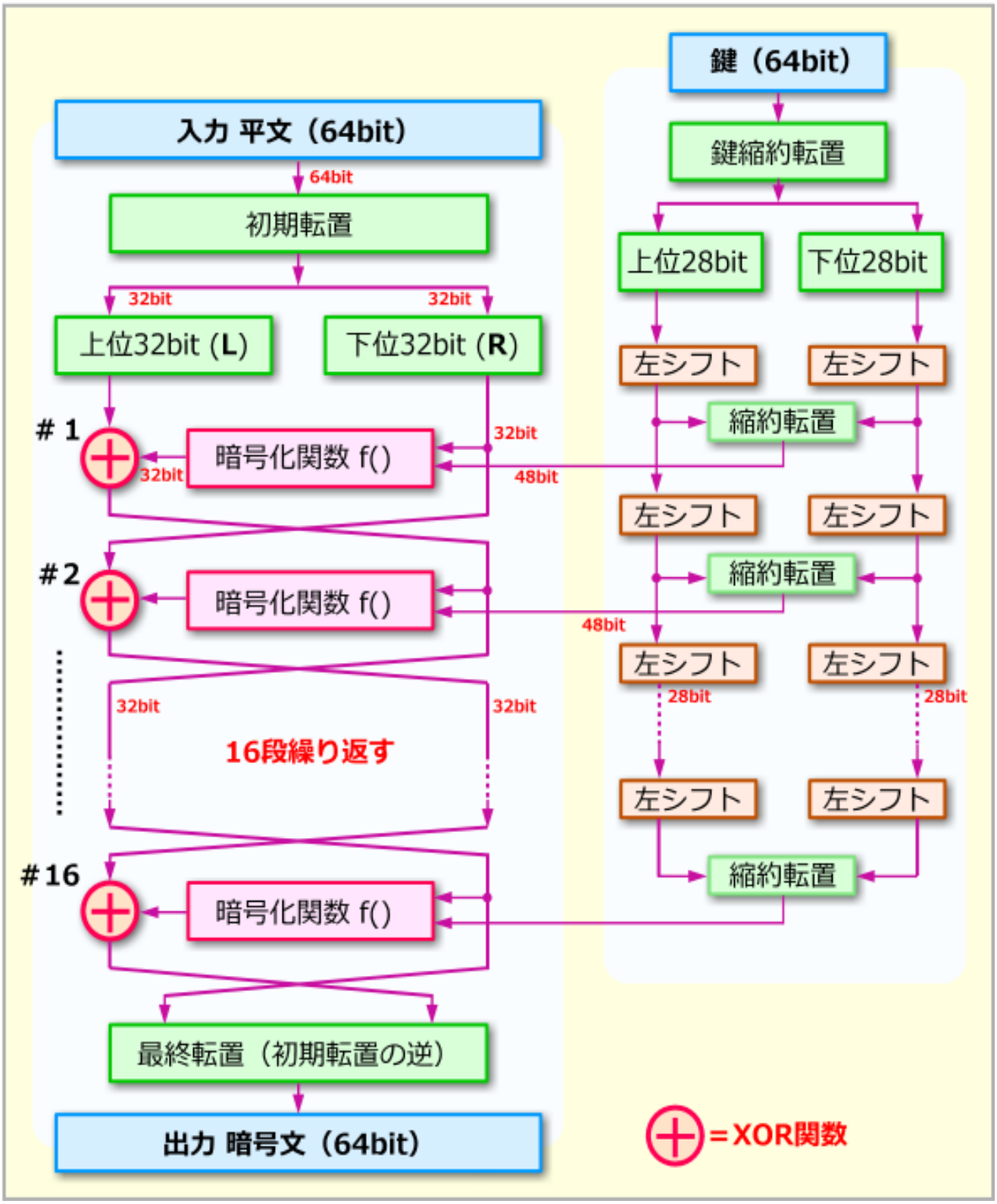
「3以上の自然数において $X^n+Y^n=Z^n$ をみたす自然数 X,Y,Z は存在しない」というもの。フランスの数学者ピエール・ド・フェルマー（1607~1655）が書き残したものである。彼は、「私はこの定理に関して真に驚くべき証明を見つけたが、この余白はそれを書くには狭すぎる」と書き残し、結局証明を書かないまま亡くなってしまう。その後300年に渡り、アマチュアから数学者まで数多くの人が証明に挑んだが失敗に終わった。1999年にイギリスの大学教授アンドリュー・ワイルズにより、ついに証明がなされた。

2　研究の目的

今回は各項の三乗 (n = 3 の時) に限って、惜しいフェルマーの最終定理 $X^n+Y^n=Z^n\pm1$ を満たす組み合わせの規則性を研究する。フェルマーの最終定理に 1 だけ足りなかったり、1 だけ多かったりする自然数 X, Y, Z がターゲットとなる。もし、これらの組に規則性を見つけることができれば、±1の違いに新たな数学的な意味を持たせられるのではないか。そして、様々な定理の周りの世界を研究することで、数学をさらに深められるのではないか。

また、この「惜しいフェルマーの最終定理」をセキュリティー分野にも応用できるのではないかと考えた。この定理を使った新しい形式の暗号を作るのだ。情報社会である現代は、個人のクレジットカードや、企業のデータバンク、インターネット回線など身の回りのあらゆる通信のセキュリティに暗号が用いられている。そしてそのような暗号の形式というのは、伝えたい文を特定の工程（鍵という）を繰り返して、暗号化する。暗号化の際に経た過程は、暗号の送信者と受信者にしか分からないようになっており、文を秘密裏に送ることができる。

私達は、この工程の一番最初、平文の順番を入れ替える工程（初期転置）に惜しいフェルマーを満たす X, Y, Z の組の羅列を用い、独自の暗号を作ることを考えている。



3　実験方法

```
list=[]
for x in range(1,100000):
  for y in range(2,x+1):
    i=x**3+y**3
    tmm_z=int(i**(1/3))
    for z in range(tmm_z-1,tmm_z+2):
      o=z**3
      if i-o==1:
        print(x,y,z)
        list.append(x+y+z)
      elif i-o==-1:
        print(x,y,z)
        list.append(x+y+z)
print(len(list))
```

図 1

$X^n+Y^n = Z^n \pm 1$ を満たす組み合わせをgooglecolaboratory（以下colab）でプログラミング、算出し、それをもとに規則性を考察する。また同様にcolabで散布図などのグラフ化を目指す。図 1 は今回用いたプログラミング式である。

```
[ ]  for x in range(1,100000):
       for y in range(1,100000):
         for z in range(1,100000):
           if x**3+y**3==z**3+1:
             if x<y<z:
               print(x,y,z)
           elif x**3+y**3==z**3-1:
             if x<y<z:
               print(x,y,z,'dec')
```

図2

図2は図1の修正前である。図2時点で範囲の限界によって算出できない組が出てくる。for文処理に時間がかかり効率が悪い。などの改善点が挙げられ、前者はxのみ範囲づけy、zはそれに対応するxの式で範囲づけた。後者は伴って改善された。

4 結果と考察

まず、n = 3 として、$X^3+Y^3=Z^3\pm1$ を考えた。1 から 10万までの中で、条件を満たす(X,Y,Z) の組み合わせは、次に示す 78 組が見つかった。

8 6 9, 10 9 12, 94 64 103, 138 71 144, 138 135 172, 144 73 150, 235 135 249

426 372 505, 438 334 495, 486 426 577, 720 242 729, 729 244 738, 812 791 1010

823 566 904, 1207 236 1210, 1537 368 1544, 1738 1033 1852, 1897 1010 1988

2292 575 2304, 2304 577 2316, 2820 1938 3097, 3230 2676 3753, 3518 3097 4184

4528 3753 5262, 5610 1124 5625, 5625 1126 5640, 5984 2196 6081, 6702 1943 6756

8343 4083 8657, 8675 1851 8703, 9036 5856 9791, 9735 3987 9953 11468 11161 14258,

11646 1943 11664, 11664 1945 11682, 11903 7676 12884, 16806 3318 16849,

17328 10866 18649, 19386 13294 21279, 21588 3086 21609, 21609 3088 21630,

24965 3453 24987, 27630 17328 29737, 31180 10876 31615, 31212 28182 37513,

33412 27238 38599, 33857 25765 38239, 34566 31212 41545, 35385 27784 40362,

35442 16617 36620, 36840 4607 36864, 36864 4609 36888 , 37887 10230 38134,

38782 5700 38823, 41167 11767 41485, 44521 26914 47584 46212 34199 51762,

49409 7251 49461, 50920 49193 63086, 51762 38305 57978, 56503 54101 69709,

59022 6560 59049, 59049 6562 59076, 64165 51293 73627, 66167 29196 68010,

66198 15218 66465, 67402 65601 83802, 69479 32882 71852, 72629 27835 73967,

76903 35131 79273, 78244 17384 78529, 80020 50313 86166, 83692 7364 83711,

87383 58462 95356, 89559 84507 109747, 89970 8999 90000, 90000 9001 90030,

94904 75263 108608

見つけた 78 組を見渡して、何かしらの特徴がないか考察した。すると、複数の組にまたがって出現する数が存在することに気付いた。例えば、78 組中の 1 組目と 2 組目、どちらの組にも 9 が出現する。さらに、この 2 組はいずれも z が 3 の倍数になっていることにも気付いた。

1 組目 (X, Y, Z) = (8, 6, 9)　　2 組目 (X, Y, Z) = (10, 9, 12)

この 2 組をペアにすると、同様の特徴をもつ組のペアが 10 ペア見つかった。

表 1

ﾍﾟｱNo	x	y	z	z÷3	階差1	階差2	階差3	階差4	階差5
1	8	6	9	3	1				
	10	9	12	4		44			
2	138	71	144	48	2		149		
	144	73	150	50		193		180	
3	720	242	729	243	3		329		72
	729	244	738	246		522		252	
4	2292	575	2304	768	4		581		72
	2304	577	2316	772		1103		324	
5	5610	1124	5625	1875	5		905		72
	5625	1126	5640	1880		2008		396	
6	11646	1943	11664	3888	6		1301		72
	11664	1945	11682	3894		3309		468	
7	21588	3086	21609	7203	7		1769		72
	21609	3088	21630	7210		5078		540	
8	36840	4607	36864	12288	8		2309		72
	36864	4609	36888	12296		7387		612	
9	59022	6560	59049	19683	9		2921		72
	59049	6562	59076	19692		10308		684	
10	89970	8999	90000	30000	10		3605		
	90000	9001	90030	30010					

Z の値は、いずれも 3 の倍数であることに着目し、各組の Z の値を 3 で割ってみる（表 1 の 5 列目の数値 ： 以下、(Z÷3)値とする）。この (Z÷3)値に様々な考察を加えて得られた結果を以下に挙げる。

・ペア内の 2 組で (Z÷3)値の階差をとると、1, 2, 3, 4, … と増える自然数の列が見つかった。（表 1 の 6 列目:階差 1）。

・隣接 2 ペア間のうち、先行ペアの (Z÷3)値の最大値と、後続ペアの (Z÷3)値の最小値の差をとる（表 1 の 7 列目:階差 2 ）。例えば、表 1 において赤色で示した値は、ペア 1 の最大値、ペア 2 の最小値、それらの値の差である。階差 2 の階差数列 3、階差数列 3 の階差数列 4 ･･･を繰り返していくと、階差 5 の値が すべて 72 となって出てくる。

以下、次ページより各階差数列の一般項を求めていく式:階差数列の公式

$$a_n = a_1 + \sum_{k=1}^{n-1} b_k$$

数学Bの教科書に記載されている上式を用いて求める。

各階差数列の一般項について

表 1 の階差 4, 階差 3, 階差 2, それぞれの数列を $\{c_n\}$, $\{b_n\}$, $\{a_n\}$ として、一般項を求める。

まず、$\{c_n\}$ は初項 180、公差 72 の等差数列であるから、

$c_n = 180+72(n-1) = 72n+108$

次に、$\{b_n\}$ は階差 c_n 、初項149 の数列であるから、、

n = 1のとき、$b_1 = 149$

n ≧ 2のとき

$b_n = 149+\Sigma c_k = 36n^2+72n+41$･･･① （※Σは k = 1 から k = n−1 の和）

n = 1のとき、$b_1 = 36+72+41 = 149$ となり、n = 1 のときも①が成り立つ。

∴n≧1のとき

$b_n = 36n^2+72n+41$

最後に、$\{a_n\}$ は階差b_n 、初項44 の数列であるから、

n = 1のとき、$a_1 = 44$

n ≧ 2のとき

$a_n=44+\Sigma b_n = 12n^3+18n^2+11n+3$・・・② （※Σは k = 1 から k = n−1 の和）

n = 1のとき、12+18+11+3=44 となり、n = 1 のときも②が成り立つ。

∴n≧1のとき

$a_n=12n^3+18n^2+11n+3$

以上の結果より、局所的ではあるものの「惜しいフェルマーの最終定理」を満たす自然数 X, Y, Z の組み合わせについて、ひとつの規則性を発見できたということになる！しかし、この数列 $\{c_n\}$, $\{b_n\}$, $\{a_n\}$ が独自の暗号作成の材料となり、助けになるのかどうか、現在も考察の途中である。

5 今後の展望

・Z を3で割った余りが 1 または 2 となる (X,Y,Z) の組でグループ化し、そのグループ内またはグループ間における数列の一般項を考察する。

・数値をもとに、図形的に解析する。

・3D散布図を phython によって作成して考察する。

・「惜しいフェルマーの最終定理」を使った暗号を作る。

6 謝辞

これまでご協力いただいた秋田県立大学の廣田千明先生、ご指導くださった横手高校の千葉将仁先生、高橋寿彦先生、佐々木一也先生ありがとうございました。

7 引用・参考文献

「フェルマーの最終定理」 サイモン・シン著 新潮社