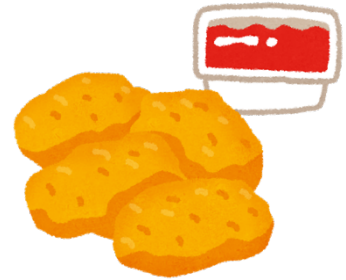


## 初等整数論への招待状✉

日本大学文理学部数学科 教授 大関一秀

突然ですが、問題です！皆さんはナゲット好きが集まるあるグループに所属しているとします。そのグループは3個入りと5個入りのナゲットを何箱でも買えるものとします。ただし、次の3つのルールを守らなければいけません。



1. 一人一個まで食べることができる
2. グループ全員が食べなくてはいけない
3. ナゲットの余りをだしてはいけない

これらのルールの下で、何人のグループであればナゲットを食べることができるでしょうか？

例えば、1人や2人のグループの場合は、3個入りでも5個入りでも余りが出てしまいます。3人であれば、3個入りを1箱買えば全員でナゲットを食べることができます。4人の場合は、3個入りではナゲットが1つ不足、5個入りでは2個のナゲットの余りが出てしまいます。6人の場合は、3個入りを2箱買えば全員で食べることができます。このように数えていくと、7人では食べることができませんが、8人以上であれば何人であってもナゲットを食べることができると分かります。(この他にも、硬貨や切手を用いた同様の問題があります。)

上のナゲットの問題を踏まえて「フロベニウス数」を紹介します。

いくつかの整数  $a_1, a_2, \dots, a_n$  に対して

$$k_1 a_1 + k_2 a_2 + \dots + k_n a_n \quad (\text{ただし, } k_i \geq 0 \text{ は整数})$$

という形で表すことができない最大の数を「フロベニウス数」と呼び、 $F(a_1, a_2, \dots, a_n)$ と表します。

例えば、先ほどのナゲットの問題にて、3個入りと5個入りをどのように組み合わせても食べることができない最大のグループ人数を考えると、 $F(3, 5) = 7$  となります。他にも、 $F(4, 6, 7) = 9$  や  $F(5, 6, 9, 13) = 8$  などとなります。皆さんも、好きな数字を適当に選んでフロベニウス数を計算してみてください。

フロベニウス数は、ドイツの数学者 G. F. Frobenius (1849~1917) に因んで名付けられたものと言われていて、現在でも研究が行われています。

まず、 $a_1, a_2, \dots, a_n$  の最大公約数が 1 となるとき、フロベニウス数が存在します。そして、最大公約数が 1 となる二つの整数  $a, b (\geq 2)$  に対し、

$$F(a, b) = ab - a - b \quad (\text{シルベスターの定理})$$

という公式が証明されています。実際、 $F(3, 5) = 15 - 3 - 5 = 7$  となります。これに対して、3 つの整数  $a, b, c$  の最大公約数が 1 となるとき、 $F(a, b, c)$  を求める公式は、まだ発見されていません。2 つの場合では大変綺麗な公式があるにも係らず、3 つ (以上) の場合で未知なる世界へと誘われることとなります。

前半は、整数の話題としてフロベニウス数を紹介しました。

後半は、素数に関する話題を紹介します。

素数は「整数  $P (\geq 2)$  が、1 と  $P$  自身以外の正整数で割り切れないとき、素数である。」と定義されます。

「素数がどのように存在するか？」について人類は何千年も前から考え続けて来ましたが、様々なアイデアが生み出されてきましたが、その中で「整数  $a$  に対して、 $a^n - 1$  という形の素数を探す。」という方法があります。例えば  $a=2$  の場合、 $2^2 - 1 = 3$ 、 $2^3 - 1 = 7$ 、 $2^4 - 1 = 15$ 、 $2^5 - 1 = 31$  計算すると、4 つのうち 3, 7, 31 の 3 つが素数となりますので良いアイデアに思えます。(尚、 $2^n - 1$  という形の素数は「メルセンス素数」と呼ばれ、これもまた有名な素数です。)

これに対して、フランスの数学者 P. Fermat (1607~1665) は「素数  $P$  が正整数  $a$  を割り切らないとき、 $a^{P-1} - 1$  は  $P$  で割り切ることができる。」というフェルマーの定理 (小定理) を証明しました。フェルマーの定理を使えば、2 を除いたすべての素数  $P$  に対して、 $2^{P-1} - 1$  は  $P$  で割り切れる、つまり素数ではないことが分かります。このようにして、素数ではないものを大量に見つけ出すことができますが、これは素数を探し出す上でも大変有効です。また、フェルマーの定理は合同式  $\equiv$  を使って簡潔に表すことができます。さらに、暗号理論においても活躍しています。

素数やフロベニウス数の魅力は、定義が非常にシンプルであり、初等的な数学を使って誰でも考えることができることです。多くの方が「数学の未解決問題は難解であり、手の届かないものである。」と考えているかも知れません。確かに、その通りの部分があります。しかし、素数の存在やフロベニウス数の様に、定義や問い自体はシンプルな身近な数学の中にも未知の世界からの招待状は潜んでいます。これを機に、数学の未解決問題に挑戦しては如何でしょうか！