研究員の眼

円周率πが現われる世界(2)
－互いに素となる確率－

取締役　保険研究部　研究理事
年金総合リサーチセンター長　　中村　亮一
TEL:　(03)3512-1777　　E-mail：nryoichi@nli-research.co.jp

はじめに

「互いに素（coprime)」という概念については、学生時代に学んだので、多くの人が聞いたことがあるとの認識を有しているものと思われる。具体的には、「２つの整数ａとｂが互いに素である」とは、「a、ｂを共に割り切る正の整数が１のみである（ａとｂの最大公約数が１になる)」ことを言う。

今回は、この「互いに素」に関係して、円周率πが現われてくる世界を紹介する。

互いに素となる確率

具体的には、任意に選ばれた２つの整数ａとｂがあるときに、このａとｂが互いに素である確率を考える。その答えが　６／π^2（＝0.607927…）となり、円周率πが現われることになる。

前回の研究員の眼と同様に、これについても、ここで円周率πが登場してくることについては、何とも不思議な感じがするのではないか。

互いに素となる確率の証明

ａとｂが互いに素であるとは、任意の素数 ｐ に対して、ａとｂの少なくとも一方が ｐの倍数でないこと、と言い換えられる。ｐを固定したとき、この事象は、ａとｂ がともに ｐ の倍数である事象の余事象となる。

ａがｐの倍数である確率は 1／ｐ であり、ｂについても同様である。各ｐに対して、これらの試行は独立なので、求める確率は、

$$\prod_{p:素数} \{1-(1/p)^2\} = 1/\left(\prod_{p:素数} (1-p^{-2})^{-1}\right)$$

となる。この算式の分母は、一般的に「リーマンのゼータ関数」と呼ばれ、ζ(s)と表されるものの

s=2 の場合に相当している。

$$\zeta(s)=\sum_{n=1}^{\infty} 1/n^{s} = \prod_{p:素数} (1-p^{-s})^{-1}$$

ζ(2)の値については、有名なスイスの数学者・天文学者であるレオンハルト・オイラー（Leonhard Euler）によって求められ、$\zeta(2)=\pi^{2}/6$　となっている。この証明をここで説明するのは紙面の都合上大変でもあるし、このコラムの意図するところでもないので、それは専門書等に委ねることにする。ただし、ここで円周率πが現われてくることについては、ゼータ関数ζ(s)の値を求める過程でsinX といった三角関数が使用されることと関係している、とだけ述べておく。πと三角関数の関係については、次回の研究員の眼で触れることにする。

いずれにしても、ここでは結果だけを引用させていただくことにして、求める確率は、

$$6/\pi^{2}=0.607927\cdots$$

となる。

a と b が偶数の場合には、互いに素ではないことから、それらのケースが全体の 1／4 あることを考えると、60.8%というのはかなり高い確率であると考えられる。

3 つ以上の整数が互いに素という概念とその確率

「互いに素」という概念は、3 つ以上の整数に対しても拡張される。例えば、「3 つの整数 a と b と c が互いに素」であるとは、「a と b と c の最大公約数が 1 になる」ことをいう。これに対して、a と b、a と c、b と c が互いに素である場合には、「a と b と c は対ごとに素（pairwise coprime)」であるという。対ごとに素であれば互いに素となるが、互いに素であっても対ごとに素であるとは限らない（例：a =3、b = 5、c = 6)。あるいは、２つの数字が互いに素であれば、それらの２つの数字を含む３つの数字は互いに素となる。

任意に選んだ k 個の整数が互いに素である確率は、２つの数字の場合と同様の考え方により算出され、その結果は 1/ζ(k）で表されることになる。具体的には、以下の通りとなる。

$\zeta(3)=1.20205\cdots$	$1/\zeta(3)=0.83190\cdots$
$\zeta(4)=1.08232\cdots$　$(=\pi^{4}/90)$	$1/\zeta(4)=0.92393\cdots$
$\zeta(5)=1.03692\cdots$	$1/\zeta(5)=0.96438\cdots$

その定義から、当然のことながら、k が大きくなれば、それらが互いに素となる確率も大きくなっていく。

互いに素となる数の性質

「互いに素」の概念については、例えば、以下の事実がある。

①異なる二つの素数 p と q は互いに素であり、連続する二つの整数 n と（n+1）も互いに素である。

②a と b が互いに素である時、$2^a - 1$ と $2^b - 1$ も互いに素となる。

③a と b が互いに素である時、ax + by = 1 を満たす整数 x、y が存在する

（a、b、x、y は整数なのでマイナスの場合もあることに注意）

※ これは、**ベズーの等式**（Bézout's identity）と呼ばれる初等整数論における定理の特別形である。**ベズーの等式によれば、**a と b を 0 でない整数とし、d をそれらの最大公約数とするとき、整数 x と y が存在して、ax + by = d となる。x と y は（a, b）の**ベズー係数**（Bézout coefficients）と呼ばれる。それらは一意的ではない。ベズー係数の組は、拡張ユークリッドの互除法という手法によって計算できる。これについては、学生時代に学んでおり、大学の入学試験問題等に出されることもあるので、ご存知の方もおられると思う。

互いに素の概念の応用

「互いに素」となる整数は、上記の性質③により、RSA 暗号（Rivest-Shamir-Adleman Cryptosystem）の秘密鍵の生成に利用されている。

RSA 暗号とは、桁数が大きい合成数の素因数分解が困難であることから、それを安全性の根拠とした公開鍵暗号の一つである。その仕組みは、大まかに説明すると、以下の通りとなる。

①まずは、２つの素数 p と q から、その積 n=pq を求める。

②e として、(p-1)(q-1)未満の正の整数で、(p-1)(q-1)と**互いに素**な数を選ぶ。

③次に、d を(p-1)(q-1)を法とした e の逆数とする。即ち、de を(p-1)(q-1)で割った余りが 1（あるいは、(de－1)が(p-1)(q-1)の倍数）となるような数とする。

④この時、de を(p-1)(q-1)で割った時の整数部分の商（割り算の結果）を x とすれば、

de+(－x)(p-1)(q-1)=1 が成り立つ。

⑤これにより、n と e を公開鍵として、d を秘密鍵とすることができることになる。

巨大な素数 p と q 及びそれから得られる巨大な整数 n を素数の積に分解することは、コンピューターを使用しても時間がかかる。従って、一般の人がこれを解明することは実際上不可能なことから、暗号化が可能になる。なお、この場合、p と q が漏れると d が計算で求まることになるため、p と q は絶対に知られないようにしておく必要がある。

最後に

学生時代に何となく学んだ「互いに素」という概念であるが、よくよく調べてみれば、なかなか面白い事実があり、実際の社会においても応用され役立っていることがわかる。

学校で、新しい概念や定義を学ぶ時には、それらが社会にどのように役立っており、どのような意味合いを有しているのか、について併せて教えていただければ、学ぶ者の興味もより一層深まっていくのではないか、と感じた次第である。

