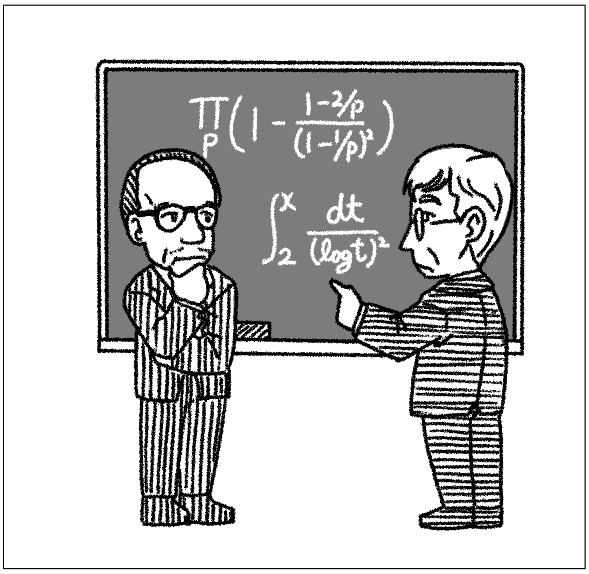
『数学セミナー』2019 年 12 月号「高校数学ではじめる整数論」

連載●第 9 回

推測する　付録

谷口 隆◎神戸大学大学院理学研究科



※ 式番号は本誌 2019 年 12 月号の連載と通しで振っています．

◎——1　関数 $\mathrm{li}_2(x)$ について

まず $\mathrm{li}_2(x)$ について，細かいことですが補足です．4 節の (10) の積分 $\int_2^x \frac{dt}{(\log t)^2}$ ですが，n が t ぐらいの大きさのとき，$n+2$ は $t+2$ ぐらいの大きさだから，この積分は

$$\int_2^x \frac{dt}{\log t \log(t+2)}$$

の方がより正確では？ と感じた人もいるかも知れません．もしそうなら，(2) の $\mathrm{li}_2(x)$ も，こちらの積分に $2c$ を乗じた関数の方がよいのでは，ということになります．

これはもっともな感覚なのですが，実際には次の命題に示すように，2 つの積分の値は僅かの差しかありません．したがって，$\pi_2(x)$ を近似的に見積もる関数を与えることが目的であれば，どちらを選んでも，違うというほどの違いはありません．$\int_2^x \frac{dt}{(\log t)^2}$ の方が表示が単純なため，通例こちらが用いられます．

命題 5　任意の $x > 2$ で

$$0 < \int_2^x \frac{dt}{(\log t)^2} - \int_2^x \frac{dt}{\log t \log(t+2)} < \frac{9}{4} \tag{15}$$

が成り立つ．　□

証明　(15) の真ん中の項の関数を $f(x)$ とおく．$\log t < \log(t+2)$ より $f(x) > 0$ である．また，

$$f(x) = \int_2^x \frac{\log(t+2) - \log t}{(\log t)^2 \log(t+2)} dt < \int_2^x \frac{\log(t+2) - \log t}{(\log t)^3} dt = \int_2^x \log\left(1 + \frac{2}{t}\right) \frac{1}{(\log t)^3} dt$$

である．$a>0$ で $\log(1+a)<a$ であるから，

$$f(x)<\int_2^x \frac{2}{t(\log t)^3}dt$$

である．$u=\log t$ で置換積分すると，

$$f(x)<\int_{\log 2}^{\log x}\frac{2}{u^3}du=\left[-\frac{1}{u^2}\right]_{\log 2}^{\log x}=\frac{1}{(\log 2)^2}-\frac{1}{(\log x)^2}<\frac{1}{(\log 2)^2}=(\log_2 e)^2<\frac{9}{4}$$

が得られる．ただし最後は $e<2\sqrt{2}$ を用いた． ■

◎——2　$\mathrm{li}_f(x)$ の導出

5 節で出てきた

$$\mathrm{li}_f(x):=c_f\int_2^x\frac{dt}{2\log t},\qquad c_f:=\prod_{p\geqq 3}\left(1-\frac{\chi_4(p)}{p-1}\right)$$

の導出方法を説明します．

n が t ぐらいの大きさのときに，$f(n)=n^2+1$ が「素数である確率」を考えましょう．まず，$n^2+1\fallingdotseq n^2$ ぐらいの大きさのランダムな整数 m が素数である「確率」は，本誌の (★) により，$\dfrac{1}{\log(n^2)}=\dfrac{1}{2\log n}$ です．

ただしここでも，n^2+1 は,「ランダムな整数」にはなりません．たとえば n^2+1 を法 3 で考えてみましょう．すると，$n\equiv 0,1,2 \pmod 3$ に応じて，$n^2+1\equiv 1,2,2 \pmod 3$ です．したがって，n^2+1 は絶対に 3 の倍数にはなりません.「ランダムな整数」のときは，3 で割った余りは $0,1,2$ になることが等しい確率で起きる，とするので，n^2+1 の形の整数であることは，3 の倍数にはならないという点では「素数である確率」を上げることになります．一方，同じことを法 5 で考えると，$n\equiv 0,1,2,3,4 \pmod 5$ に応じて $n^2+1\equiv 1,2,0,0,2 \pmod 5$ なので，5 の倍数でない確率は $\dfrac{3}{5}$ と，ランダムな $\dfrac{4}{5}$ より低めです．

そこで一般に各素数 p について，次の二つの確率を考えます．

$a'_p:=$ (ランダムに選ばれた整数 m が p の倍数でない確率)
$b'_p:=$ (整数 n がランダムに選ばれたとき，n^2+1 が p の倍数でない確率)

すると，n がランダムに選ばれたとき，n^2+1 が素数である確率は，だいたい

$$\frac{1}{2\log n}\prod_{p:\ \text{素数}}\frac{b'_p}{a'_p} \tag{16}$$

ではないかと考えることができます．

本誌で述べたように，整数 n が「ランダムに選ばれる」の意味は，n を p で割ったときの余りが $0,1,\cdots,p-1$ の p 通りのどれになるかが等確率だということと考えます．すると明らかに $a'_p=1-\dfrac{1}{p}$ です．また b'_p は，合同方程式 $f(n)=n^2+1\equiv 0 \pmod p$ の法 p での解 n の個数を $N_f(p)$ とすれば，$b'_p=1-\dfrac{N_f(p)}{p}$ です．

$$N_f(p)=\begin{cases}1 & p=2\ \text{のとき}\\ 2 & p\equiv 1 \pmod 4\ \text{のとき}\\ 0 & p\equiv 3 \pmod 4\ \text{のとき}\end{cases}$$

から，b'_p が求められます．(この $N_f(p)$ は，これまでの連載で扱った内容に基づいて求めることができます．詳細は皆さんにお任せします．考えてみてください．)

$p=2$ のときは $a'_2=b'_2=\dfrac{1}{2}$ なので，$\dfrac{b'_2}{a'_2}=1$ です．$p\neq 2$ のとき，$N_f(p)-1=\chi_4(p)$ であることに注意して，

$$\frac{b'_p}{a'_p}=\frac{p-N_f(p)}{p-1}=1-\frac{N_p(f)-1}{p-1}=1-\frac{\chi_4(p)}{p-1}$$

です．よって (16) は $\dfrac{c_f}{2\log n}$ となります．これで $\mathrm{li}_f(x)$ の式の意味が明らかになりました．

◎——3　素数の個数のヒューリスティック

他にもいろいろな場合に，このようなヒューリスティックによって，素数の個数を近似する式を作ることができます．もう二つ紹介しましょう．一つはソフィー・ジェルマンの素数で，もう一つは n^2+n+41 の形の素数です．

3.1　ソフィー・ジェルマンの素数

p が素数であり，また $2p+1$ も素数であるとき，p をソフィー・ジェルマンの素数といいます．$\pi_{\mathrm{SG}}(x)$ で，x 以下のソフィー・ジェルマンの個数を表します．ヒューリスティックによって得られる $\pi_{\mathrm{SG}}(x)$ の近似式は

$$\mathrm{li}_{\mathrm{SG}}(x):=2c\int_2^x\frac{dt}{\log t\log(2t)}$$

です．ただし c は，双子素数のときに考えた (1) の定数です．値を比較すると次のようで，やはりよい近似であることが観察されます．

x	10^4	10^6	10^8	10^{10}
$\pi_{\mathrm{SG}}(x)$	195	7811	423295	26568824
$\mathrm{li}_{\mathrm{SG}}(x)$	190	7746	423140	26569515
差	5	65	155	691

双子素数の問題と同様，ソフィー・ジェルマンの素数が無限個あるかどうかもまだ分かっていません．(もし $\displaystyle\lim_{x\to\infty}\frac{\pi_{\mathrm{SG}}(x)}{\mathrm{li}_{\mathrm{SG}}(x)}=1$ が正しければ，無限個あることになります．)

3.2　オイラーの多項式

オイラーが注目した多項式，$g(n)=n^2+n+41$ を知っていますか．$n=0,1,\cdots,39$ での $g(n)$ はそれぞれ

$$41,43,47,53,61,71,83,97,113,131,151,173,197,223,251,281,313,347,383,421,461,503,$$
$$547,593,641,691,743,797,853,911,971,1033,1097,1163,1231,1301,1373,1447,1523,1601$$

です．なんと，実はこれらはすべて素数です．これだけの連続した整数について素数になる多項式はなかなか類例がありません．$n=40$ では素数ではなく，$g(n)$ が常に素数になるわけではないのですが，割合を調べて

みると，たとえば $1 \leqq n \leqq 10^4$ のうち，半数にも迫る 4148 個の n で素数になります．$f(n) = n^2 + 1$ のときは同じ範囲では 841 個であり，この頻度の多さも，群を抜くものです．

$\pi_g(x)$ で，x 以下の正の整数 n で，$g(n)$ が素数になるものの個数を表します．これを近似する関数 $\mathrm{li}_g(x)$ を，$f(n)$ のときとまったく同様の考え方で構成できます．合同方程式 $g(n) \equiv 0 \pmod p$ の法 p での解 n の個数を $N_g(p)$ とします．そして，

$$c_g := \prod_{p \geqq 2} \left(1 - \frac{N_g(p) - 1}{p - 1}\right) \tag{17}$$

として，

$$\mathrm{li}_g(x) := c_g \int_2^x \frac{dt}{2 \log t}$$

を考えることができます．c_g の数値は $c_g = 6.6395463549428 \cdots$ で，二つの関数の値を較べてみると，やはりよい近似になっています．

x	10^4	10^6	10^8	10^{10}
$\pi_g(x)$	4148	261080	19132652	1510676802
$\mathrm{li}_g(x)$	4133	261022	19129225	1510681420
差	15	58	3427	4618

表の数値では $\pi_g(x)$ は $\pi_f(x)$ よりは大幅に大きく，$g(n) = n^2 + n + 41$ は $f(n) = n^2 + 1$ よりも，素数になることがずっと多いことが見て取れます．$\mathrm{li}_g(x)$ と $\mathrm{li}_f(x)$ は，積分は同じ式で，定数 c_f と c_g だけが違います．$c_g = 6.639 \cdots$ が，$c_f = 1.372 \cdots$ よりずっと大きいのです．

この定数の違いは，関数 $N_g(p)$ の特殊な振る舞いが原因です．小さな素数で，$N_f(p)$ と $N_g(p)$ の値を較べてみましょう．

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	$\cdots$
$N_f(p)$	1	0	2	0	0	2	2	0	0	2	0	2	2	0	0	2	0	2	0	0	2	0	$\cdots$
$N_g(p)$	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	0	2	0	2	0	0	$\cdots$

$N_f(p)$ は 0 になったり 2 になったりがなんとなくランダムですが，$N_g(p)$ は 37 までの p でズラッと 0 が並んでいます．(17) の右辺の積の因子

$$1 - \frac{N_p(g) - 1}{p - 1}$$

は，$N_g(p) = 0$ のときは > 1 で，$N_g(p) = 2$ のときは < 1 であり，また p が大きくなるほど 1 に近い値をとることに注意してください．小さな素数で連続して $N_g(p) = 0$ となっていることが，c_g の数値が大きいことの原因です．数値実験をすると分かるのですが，整数係数の 2 次多項式 $h(n) = an^2 + bn + c$ で，法 p での $h(n) \equiv 0 \pmod p$ の解 n の個数がこれだけ連続して 0 になるものはなかなか見つかりません．これがオイラーの多項式 $n^2 + n + 41$ のもつ特徴です．

(なお，無限個の n で $n^2 + n + 41$ が素数になるかどうかは，やはり未解決の問題です．)

[たにぐち たかし]
[絵／森脇かみん]