〔論　文〕

数論とIT

江戸川大学メディアコミュニケーション学部情報文化学科　石田　義明

1. 数論

数論とは数を扱う数学の一分野であるが、「数論は数学の女王」（ガウス）と呼ばれるくらい数学では基本的なものであり、重要な役割をしてきた。しかしながら、実用性の観点からは、数論は遠い存在であった。最近、数論で特に注目されたものは、フェルマーの最終定理の証明である。1994年にワイルズにより証明された。それは「自然数X、Y、Z、m に対し、$X^m+Y^m=Z^m$ を満たす 3 以上の整数 m は存在しない 」というものである。フェルマーの「証明できるが、それを書く余白が無い」という有名な言葉から 350 年ぶりに証明された。その証明にはフェルマーの時代より遥かに高度な数学が必要で、現在では、フェルマーは証明できなかったと考えられている。証明は直接的なものではなかった。フライ・セールにより m が 3 以上のフェルマーの式が存在すると、モジュラでない楕円曲線が作成でき、谷山・志村予想と矛盾が起きることが示された。結局、フェルマーの最終定理は谷山・志村予想を証明することに帰された。このパズルのラストピースはワイルズによって嵌めこまれた。しかしながら、ワイルズがこの研究を秘密にしてきて、突然発表したり、最初の証明に誤りがあり、全世界の数学者やマスコミの注視の中で、一年後、劇的に解決されたことなどで、多くの人々に強い関心を持たせ、その顛末はいろいろな本に書かれている。これまでも証明できたと公表し、結局証明に誤りがあったことが何例も知られていたので、「ワイルズもダメだったのか」という空気が蔓延していた中で、最後には解決してしまったということは大きなインパクトを与えたが、実用性という点では数学以外の分野には直接的には伝搬しなかった。ワイルズの仕事の中には、谷山・志村予想、岩澤理論など日本人の数学者の名前が頻繁に出てくるので一般の日本人の中でも多くの関心を呼んだ。このように数論というものは元来、他の分野ではなかなか直接的に使われてこなかった。ところが、インターネット上ではパスワードなどの暗証番号をネット経由でやりとりしなければならなくなり、セキュリティ上、素数というものが重要な役割を演じるようになり、数論と IT が密接な関係をもつようになった。

2. 素数定理

数の中で一番身近なものといえばそれは自然数であろう。自然数の集合を N とすれば

$$N=\{1,2,3,4,5,\cdot\cdot\}$$

しかし自然数より基本的な存在である数がある。それは素数である。素数とは「1 と自分自身以外に約数を持たない自然数」である。素数の集合を P とすると

$$P=\{1,2,3,4,5,\cdot\cdot\}$$

なぜ基本的かというと、自然数は素数の積に分解されるからである。

$$12=2\times2\times3 \qquad \text{(素因数分解)}$$

素数はかなり昔から知られており、あの幾何学で有名なエウクレイディス (ユークリッド) の「原論」の中で素数に関する定理が証明されている。一つ目は「素数は無限個ある」というもので、背理法によって巧妙に証明されている。二つ目は「自然数は素数に分解され、その分解の仕方はユニー

クである」。つまり自然数の素因数分解の仕方は一通りしかないということである。代数学にはガウスにより証明された代数学の基本定理「ｎ次代数方程式はｎ個の解が存在する」があるが、この素因数分解の唯一性は初等整数論の基本定理と呼ばれる程重要で基本的な定理である。このように、自然数は素数から構成されているという意味で、素数は数の中でも最も根源的なものと考えられる。物理学において、いろいろな物質は原子からできていて、原子は更に素粒子から構成されている。物理における素粒子に素数が対応しているのかもしれない。そこで根源的な存在である素数には遥か昔から大きな関心が寄せられてきた。では素数とはなんであろうか？

素数の並び方はでたらめにみえ、そこには何の規則性もみられない。最も基本的な数である素数の規則性を求めることは、数学上最も大きな問題の一つである。ある自然数が素数であるかどうかの判定は簡単にできるのであろうか。一番古いシステマチックなやり方はエラストテスのふるいと呼ばれている方法である。それはまず２の倍数でないかチェック、次に３の倍数、５の番数・・とやっていき、素数以外の数を次々に落としていく。しかしながら、このやり方は数が大きくなると、とてつもなく長い時間がかかり、結局不可能になってしまう。スーパーコンピューターを使っても現実的な時間内には素数であるか判別できないような自然数がすぐに出現する。いろいろな数学者は素数の式を提案してきたが、完全なものはなかった。素数を完全に表現する式ではないが有名なものでは

メルセンヌ素数：$Mn = 2^n - 1$

フェルマー素数：$Fn = 2^{2^n} - 1$

素数に関するいろいろな定理がフェルマー、オイラー等によって導かれたが、素数に関する直接的な大きな進歩はユークリッドから 1500 年以上たったあの数学の巨人ガウスを待たねばならなかった。彼は洞察力だけでなく計算力も並はずれた能力があった。電卓がない時代にすさまじい計算をした。ガウスは数論に関して重要概念を発見し、多数の定理を導いた。その初めての数論の著書はその後の著名な数学者たちに大きな影響を与えた。ガウスが若干 15 歳のとき、持っていた素数の表をみながら、素数の分布を考えた。それはある数 x 以下の素数の個数、いわゆる分布関数である。素数がどのような順番で出現するかも全く分からない状態で分布関数を出そうとする直観にも驚かされる。ガウスはその式の証明をしなかったが、後に素数定理として大勢の数学者が挑戦をした。それは充分大きい x に対して、素数の分布関数 $\pi(x)$ は

$$\pi(x) \simeq \frac{x}{\log x}$$

この式は非常に良い近似式になっていることがわかる（図-１）。

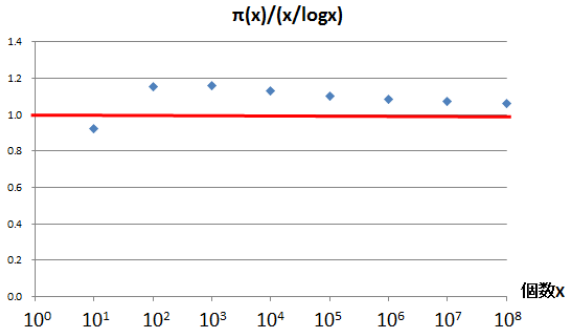

図-1：素数定理を実測値で検証

3. リーマンのゼータ関数ζ(s) (文献1,2,3)

素数の研究において、大きな変革はリーマンによってもたらされた。それは 1859 年に出版した唯一の数論の 10 頁程度の短い論文であった。当初はリーマンの研究はそれほど重要視されなかったようだ。リーマンの素数に関する仕事は、後で述べる素数定理が 37 年後に証明されたとき大きな役割をしたが、本当の深い意味は 70 年後のジーゲルによるリーマン研究によるところが多い。

オイラーは素数によるゼータ関数の表現を導いた。もともとの $\zeta(s)$ は

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

この式は $s>1$ の場合のみ収束する。$s \leq 1$ では

発散してしまう。オイラーはζ関数を次のような素数の積の形に導いた（オイラー積）。

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

s＞1 ではζ(s)≠0 となる。

オイラーの時代はまだ複素関数論が確立しておらず、素数に関して更に進んだ研究には至らなかった。リーマンは素数の積で表現されたζ関数に注目した。コーシーやリーマンにより定式化された複素関数論を使い、s＞1 でしか意味を持たなかったζ関数を複素平面全体に解析接続し、ζ関数が複素平面上で取り扱えるようになり、数論から解析的整数論という分野が生まれ新しい段階に達した。ゼータ関数の積分表示は

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx \quad （第一積分表示）$$

Γ(s)はガンマ関数で $\Gamma(s) = \int_0^\infty e^{-x} x^{s-1} dx$ 。

s を複素数に拡張したとき、ζ(s)は Re(s)＞1 のときのみ収束する。ζ(s)を書き換えると

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^1 \left(\frac{x^{s-1}}{e^x - 1} - \frac{x^{s-1}}{x} \right) dx + \frac{1}{\Gamma(s)} \int_1^\infty \frac{x^{s-1}}{e^x - 1} dx + \frac{1}{\Gamma(s)} \frac{1}{s-1}$$

この式は $0 < \mathrm{Re}(s) \leq 1$ で収束する。これを続けていくと複素平面全体に対して解析接続ができる。更に第二積分表示に変形すると s と 1−s に対称な

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \int_1^\infty \varphi(x) \left(x^{\frac{s}{2}} + x^{\frac{1-s}{2}} \right) \frac{dx}{x}$$

が導け、これから関数等式が得られる。

$$\zeta(1-s) = \zeta(s) \frac{2}{(2\pi)^s} \Gamma(s) \cos\left(\frac{\pi s}{2}\right)$$

これによりζ(s)の零点は s ＝−2、−4、−6 ・・・と $0 \leq \mathrm{Re}(s) \leq 1$ にのみ限定される。

またリーマンはゼータ関数ζ(s) と同時に素数の分布関数π(x) の明示公式も導いた。

$$\pi(x) = \sum_{m=1}^{\infty} \frac{\mu(m)}{m} \left(Li\left(x^{\frac{1}{m}}\right) - \sum_\rho Li\left(x^{\frac{\rho}{m}}\right) + \int_{x^{\frac{1}{m}}}^\infty \frac{du}{(u^2-1)u\log u} - \log 2 \right),$$

$\sum_\rho$ はゼータ関数の零点（ζ(ρ)＝0 ）の和。

$Li(x)$は対数積分で

$$Li(x) = \int_0^x \frac{du}{\log u} 。$$

μ(m)はメビウス関数と呼ばれ

$$\mu(m) = \begin{cases} 1 \cdots m \text{ は偶数個の相異なる積または} 1 \\ -1 \cdots m \text{ は奇数個の相異なる積} \\ 0 \cdots \text{その他} \end{cases}$$

そこでは素数の和からゼータ関数の零点の和に変わっている。プーサンとアダマールは独立に 1896 年にリーマンのゼータ関数を使って素数定理を証明した。これがリーマンの仕事の後の大きな成果であった。そのときゼータ関数の零点の領域は $0 < \mathrm{Re}(s) < 1$ の範囲にわずかながら縮まった。

4. リーマン予想

リーマンは素数分布関数π(x)を導いた際、$\sum_\rho$ のρの和の取り方にもっと強い制限を付けた。それは、ζ(s)の零点ρの実数部分は

$$\mathrm{Re}(\rho) = \frac{1}{2}$$

となるであろうという予想である。これは全ての零点が実数軸に垂直な直線上にあるということである（図-2）。素数に関しての規則性が初めて示されたのである。

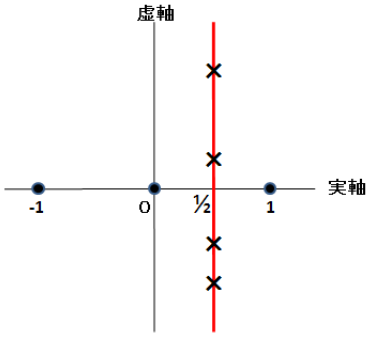

図-2：リーマン予想によるζ(s)の零点分布

このリーマン予想は 1900 年パリの国際数学者会議において、ヒルベルトにより 23 の問題の一つとして、20 世紀に向けて提出されたが、リーマンから 150 年後の 21 世紀の現在でもまだ解決されず、数学界でもっとも重要な未解決問題の 1 つ

となっている。リーマン以後の直接的な進歩としては、前述した素数定理の解決、1914 年ハーディにより Re(ρ)＝1/2 の直線上に無限個の零点があることが証明されたが、全ての零点があるかは証明できなかった。しかしながら後でわかったことであるが、リーマンはその 55 年前に既にハーディの証明を行っていたことがわかった。現在までには零点のうち 40%がリーマン予想を満たしていることが証明されているが 100%にはなっていないし、その割合を上げるやり方には限界があった。コンピューターを使った数値計算では、図-3 に示したように、1000 億個以上の零点がリーマン予想に従っていることがわかっている。(文献 4)

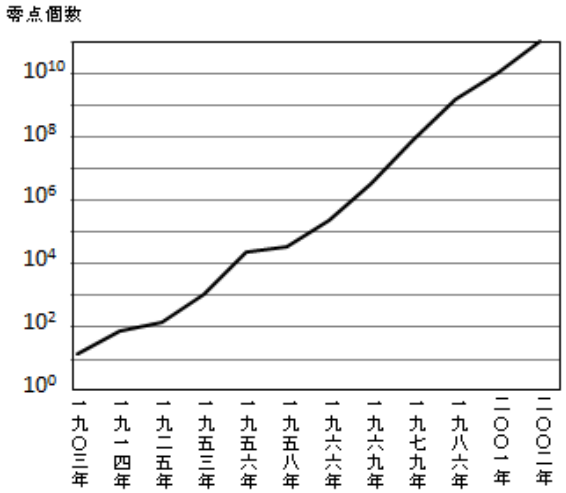

図-3：リーマン予想を満たす零点の個数

リーマンゼータ関数から数学上重要なゼータ関数が次々に発見された。合同ゼータ関数上ではハッセ、ヴェイユ、ドリーニュらによりリーマン予想が証明され、セルバーグによりセルバーグゼータ関数上でリーマン予想が証明され、数学上大きな進歩があった。またあの奇才、スキーム理論のグロタンディークも合同ゼータ関数で重要な寄与をし、非可換幾何のコンヌなどもリーマン予想の解決に参戦してきた。フェルマーの最終定理やポアンカレ予想と並んで、いまやリーマン予想は TV にも取り上げられ、世界中の数学者から注目されているホットな話題になっているのである。ただ解決するかどうかは全く未知である。リーマン予想が完全に解決される頃には素数に関する理解度も格段に進歩しているかもしれないのである。その素数論の発展が IT の世界に大きな影響を及ぼしかねない状況にある。

5. RSA と数論 (文献5)

前節まで、現在の素数の研究の現状を述べてきたが、素数の性質が明らかになるとサイバースペース上では大騒ぎになることは間違いない。なぜなら素数がインターネットビジネスや個人情報の保護のためのセキュリティに決定的な役割をしているからである。筆者はオンラインショッピングにネットバンキングを利用する。ショップに対してクレジット番号は余り使う気になれないのである。その際、銀行にログインするときも、銀行からショップに振り込むときもパスワードを要求される。

そのときパスワード処理に要求されるものは、簡単にパソコン内で暗号化処理でき、かつ送信途中で絶対に解読されず、受信側で簡単に復元できるということである。素朴な考えでは、あらかじめ二人の間で暗号化の規則を決めて、それから暗号化通信を始める。第二次大戦中の無線通信は暗号コードブックでおこなっていた。しかしながらコードブックが第三者の手に渡れば、情報が筒抜けになってしまうという致命的な欠陥があったし、コードブックを変えるとなると多数の相手がいる場合などでは危険だし、殆ど不可能であった。またインターネット上でもコードブックの存在はハッキングなどで危険極まりなく、操作も面倒であるので現実的でない。それに代わるものとして公開鍵暗号を使うシステムが出現した。1976 年スタンフォード大学のディフィーとヘルマンにより提案された。それは二種類の鍵を使う。暗号化する鍵 A と解読する鍵 B である。これの長所は鍵 A が分かっても暗号が解読できないということである。(図-4 参照)

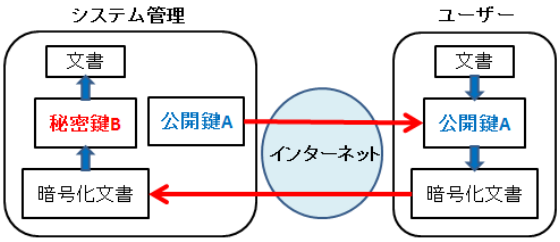

図-4：公開鍵暗号システム

そのために鍵Aは誰にでも公開できるという新しい考え方で、公開鍵Aはいつでも変えられ、従来に比べて画期的なものであった。しかしながら、乱数表のようなコードブックが要らないということでは素晴らしいものであるかもしれないが、このシステムを使ったからと言って安全であるわけではない。なぜなら公開鍵を与えてパスワードを暗号化しても、その解読が難しいかどうかは公開鍵暗号システムとは別なことである。やがて何回か試行錯誤され、このような公開鍵は上手く作成できないのではないかという空気が漂い始めた。そのようなとき、ディフィーとヘルマンの論文に触発されたMITの情報科学専門のリヴェスト(R)に、暗号専門のシャミア(S)と数論専門のアーデルマン(A)が加わり、三人によってRSAという暗号システムが完成された。それは公開鍵と数論を上手く組み合わせたもので、三人は世界中から注目され、この功績によって2002年のチューリング賞を受賞した。実践的な応用とはおよそ無縁であった数論が将にRSAの根幹をなしている。その一番目の特徴は、二つの異なる巨大な素数p、qの積n＝p×qを考える。このとき、nを素因数分解して元の素数とpとqを求めようとすると、最新鋭スーパーコンピューターでさえも莫大な計算時間を必要とするということである。二番目の特徴は「フェルマーの小定理」を使うと、第三者が元の痕跡を辿りにくくできるが、復元は秘密鍵で簡単にできる。そしてこの二つの特徴は素数という共通の性質を使うため、公開鍵暗号システムと数学的な整合性が非常にあったということである。今やインターネット上の取引は殆どRSAによって暗号化されている。RSAでは70桁以上の二つの巨大な近い素数p、qを必要とする。その積をnとすると

$$n = p \times q$$

このnを公開鍵とする。前述したように、nを公開してもその素因数分解の計算にはスーパーコンピューターでも莫大な時間がかかり、事実上計算不可能と考えられ、素数p、qは秘密のままにできる。次にこの素数とフェルマーの小定理を使って暗号化する。フェルマーの小定理は

「pが素数で、pとxが互いに素なら

$$x^{p-1} \equiv 1 \ (mod\ p)$$

（$x\ mod\ y$：xをyで割った余り）」

オイラーはこの定理を更に一般化し、n＝p×q（p、q素数）の二次元上でφ(n)＝(p−1)×(q−1)とすると

$$x^{\varphi(n)} \equiv 1 \ (mod\ n)$$

を証明した。一般に $a^b = c\ (mod\ n)$ において a^b からcを求めるのは簡単であるが、aとcからbを求めるのは難しい。かつ $mod\ n$ によってbを乗しても桁数は大きくならない。このことで公開鍵暗号システムが最適な理由となった。これをわかりやすいイメージにすると、トランプをφ(n)+1回シャッフルすると元に戻るということになる。一番上のカードを記憶し、m回シャッフルするとそのカードはどこに行ったかわからない(暗号化)。ところが更にシャッフルして合計φ(n)+1回シャッフルすると先頭に記憶したカードが戻ってくる（復号化）。

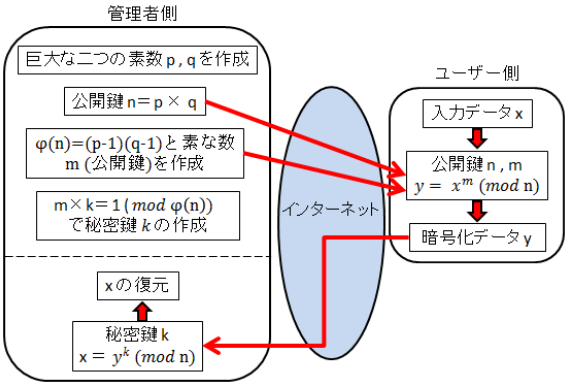

図-5：暗号化システムRSAの仕組み （文献6）

実際の手順は、暗号管理者側の準備として

(1) 70 桁以上の二つの大きな素数 p、q を考え、その積 n＝p×q を公開鍵の 1 つとする。

(2) オイラーの関数 φ(n) ＝ (p－1)×(q－1)と素な数 m (1 以外の約数を持たない) を公開する。

(3) m×k ＝ 1 ($mod\ \varphi(n)$) なる k を求める。m、n は公開鍵で p、q、k は秘密鍵となる。

ユーザー側のパソコンで x を暗号化し y を作成。

(4) $x^m \equiv y\ (mod\ n)$ で暗号化する。計算は簡単であるが、y → x の復元は難しい。

（m 回シャッフルしてカードを隠す）

(5) 管理者側で秘密鍵 k を使って y → x に復元。

x ＝ $y^k\ (mod\ n)$ （計算簡単）

（k 回シャッフルすると元のカードが現れる）

この暗号を破るには n を素因数分解できればよい。しかしながら n ＝ p×q を求めるのが極めて困難であるということをこれまで述べてきた。ベル研究所のポメランスは素因数分解に強い関心を持っていた。ポメランスは素因数分解にはフェルマーの因数分解法が最も高速であることを知った。そして「二次ふるい法」という手法を発見した。これは前述したエラトステネスのふるいに似たところがあったが、ガウスの時計計算機を使い、その時間を変えながら素数でない数を落としていくのというものである。1980 年代には、この発見はまだ実用的ではなかった。しかしながら 1990 年代にインターネットが登場すると状況は変わった。

1970 年 RSA 作成者の三人は「129 桁の数を 2 つに素因数分解せよ」という懸賞 RSA129 を世界に提出した。これには世界中の多くの人が注目した。ポメランスの「二次ふるい法」の出番がやってきたのである。レンストラとマッスルはポメランスのやり方を「多重多項式ふるい法」に拡張して、インターネットで使えないかと考えた。それは多数のパソコンによる分散処理である。インターネットに繋がれた 1600 台もの各パソコンに、時間の違う時計計算機を割り当てて、独立に解を捜索させたのである。その結果、14 年後の 1994 年についに解が求まったのである。時間はまだ結構かかっているが、従来考えられてきた天文学的な時間ではなかったことが重要なのである。パソコンの計算能力は急速に向上しているので、暗号システム側も現状維持だけでは生き延びられないことがわかった。素数の桁数を少し上げるだけで計算時間が極端に長くできるので、コンピューターの進歩にも対応できているのが現状であるが、リーマン予想の研究の進歩により、素数に対する理解が深まり、また独創的なアルゴリズムで素因数分解が超高速で可能になったり、今後の予想はつきにくい。他に楕円関数を使った暗号システムなども実用化されている。

6. 結論

「素因数分解が困難」→「RSA 暗号の解読も困難」という関係は証明されているわけではない。「RSA 暗号を解読しようとすると、素因数分解が必要なので、RSA 暗号の解読も難しい」という事が根拠になっているに過ぎない。 つまり、今のところ素因数分解は難しいが、その素因数分解をしないで RSA 暗号を解読してしまう方法が存在するかもしれない。現状では現実的ではないかもしれないが、RSA 暗号 にはそういう欠点がある。ところが NTT は、「素因数分解の困難」と「暗号解読の困難」が等価であることと、強秘匿であるということが数学的に証明された公開鍵暗号、EPOC（エポック）を発明した。その結果、「素因数分解が難しい」ならば「EPOC 暗号の解読も難しい」ということが証明されていて、 素因数分解の効率的なアルゴリズムを見つける以外には、この暗号を短時間で解読する方法がないということになった。安全性の証明が見つけられた暗号という点では、RSA 暗号システムより完成度が高いシステムであるということになる。

このようにインターネット上のセキュリティで重要な役割をしている素数に対し、アメリカの国家安全保障局のような機関も数論に強い関心を持ち、それが国家の安全にとって重大な危機にな

るかどうかの詳しい検討をするようになり、例えば巨大な素数の輸出にはストップをかけたりしてきた。国家の重要機密ということであろう。研究費の取りにくかった数論の分野の専門家は、セキュリティという言葉を使用することによって、予算が取りやすくなったという話も聞いたりする。リーマン予想というのは数学上でも重要な課題であり、天才的な数学者が次々に挑戦しているので、素数に対する理解もどんどん深まることであろう。またセキュリティを破ろうと世界中のハッカーが虎視眈々と新しいアルゴリズムを作成している。

今後の急激な進展は、おそらく予測のつかないものになるであろうことだけは理解できる。

参考文献

(1)黒川信重（2009）「リーマン予想の 150 年」岩波書店 、1,2,3,7 章

(2)黒川信重、小山信也(2009)「リーマン予想のこれまでとこれから」日本評論社、3,4,5 章

(3)リーマン(1859)「与えられた限界以下の素数の個数について」リーマン論文集（足立、杉浦、長岡　訳）より（2004）朝倉書店

(4) John Derbyshire(2003)「Prime Obsession-Bernard Riemann and the Great Unsolved Problem in Mathematics」, Joseph Henry Press

(5) Marcus du Sautoy(2003)「The Music of the Primes」Harper Perennial; Chap.10

(6) 芹沢正三(2002)「素数入門」講談社