数学集中講義

ABC 予想が証明された？

吉田　信夫

大学への数学　13 年 3 月号　掲載

“ABC 予想” は，1985 年に Joseph Oesterle と David Masser によって提起された予想であり，それを京都大学数理解析研究所の望月新一教授が証明した，と話題になっている．4 編 500 ページほどからなる論文により，Inter−universal Teichmüller Theory（宇宙際タイヒミュラー理論）というオリジナルの理論を展開し，ABC 予想が従うような大きな定理を証明した（今後の審査をパスして初めて証明された，と認定されることになる）．では，ABC 予想とは何なのか？

【ABC 予想】

互いに素な自然数 a，b，c が $a+b=c$，$a<b$ を満たすとする．積 abc の互いに異なる素因数全体の積を R とおく．任意の正数 ε に対し，$c>R^{1+\varepsilon}$ となる a，b，c の組は有限個しか存在しない．

ここで，例えば $a=4$，$b=15$，$c=19$ のとき，

$$R=2\cdot 15\cdot 19=570$$

である．R は c よりもずっと大きな値となり，すべての正数 ε に対して $c\leqq R^{1+\varepsilon}$ となっている．特殊な a，b，c でなければ，通常は $c<R$ となるので，ABC 予想はレアケースがどの程度まで起こるかを考えていることになる．ちなみに，$c<100$ の範囲で $c>R$ となる a，b，c の組はわずか 6 組しかなく，$c<1000$ の範囲でも 31 組しかないようである．

さらに，この予想の仲間として

【ABC 予想の仲間】

上記の a，b，c，R に対し，$c<R^2$ が成り立つ．

という予想もある．つまり，$\varepsilon\geqq 1$ であれば，“有限個” の部分が “0 個” になるのではなかろうか，という予想である．

望月教授の論文を見ると，【ABC 予想】は証明されているようであるが，【ABC 予想の仲間】が示されているのかは，私には分からなかった．最新の数学理論なので，専門家の見解を待ちたい．“有限個” を考えるべき範囲が分かっていれば，精査することで示されているのかも知れないが，私の守備範囲を大きく越えているので，これ以上の深入りは避けておきたい．

さて，大きな定理が証明されると，それに関連する問題が出題されることがある．最近では，フェルマーの最終定理「$n\geqq 3$ のとき，$x^n+y^n=z^n$ を満たす自然数の組 $(x,\ y,\ z)$ は存在しない」が示されたが，それにまつわる問題が出題されている．例えば，2010 年の福島県立医科大学に，$n=4$ の場合を考えさせる問題がある．

他には，ペレルマンによってポアンカレ予想が証明された (4 次元空間での球と曲線の関係)．この分野では最短経路が重要な役割を果たすが，1 つ次元を下げた普通の球 (普通の球と曲線に関する低次元のポアンカレ予想の成立はずっと前から知られていた) 上での最短経路の問題が京都大学で出題されている（2008 年理系）．また，2011 年のガロア生誕 200 年を受けてか，2012 年の京都大学ではガロア理論のテーマに近い問題が出題されている ($\sqrt[3]{2}$ を解にもつ有理数係数の方程式に関する問題)．ちなみにガロアは，20 歳の若さで女性を巡る決闘で命を落としたというエピソードで有名な天才数学者である．

偶然か深読みし過ぎかも知れないが，問題を作成する数学者も時事ネタには少なからず関心をもっているはずなので，多少は意識していると考えて良いのではないか．

では，ABC 予想に関わる問題を考えてみよう．

素因数分解や登場する素因数の積に関して問うものはあまり見かけないが，そんな中で，素因数の積を正面から扱う問題があるので，紹介しておこう．2003 年の大阪大学の文系前期の問題である．

問題 1.　自然数 m に対して，m の相異なる素因数をすべてかけあわせたものを $f(m)$ で表すことにする．たとえば $f(72)=6$ である．ただし，$f(1)=1$ とする．

（1）m，n を自然数，d を m，n の最大公約数とするとき $f(d)f(mn)=f(m)f(n)$ となることを示せ．

（2）2 つの箱 A，B のそれぞれに 1 番から 10 番までの番号札が 1 枚ずつ 10 枚入っている．箱 A，B から 1 枚ずつ札を取り出す．箱 A から取り出した札の番号を m，箱 B から取り出した札の番号を n とするとき $f(mn)=f(m)f(n)$ となる確率 p_1 と $2f(mn)=f(m)f(n)$ となる確率 p_2 を求めよ．

解　（1）d の素因数を

$$p_1,\ p_2,\ \cdots\cdots,\ p_i$$

とおく（$d=1$ になる場合もあるが，それは $i=0$ と考えることにする）．すると m，n の素因数をそれぞれ

$$p_1,\ p_2,\ \cdots\cdots,\ p_i,\ q_1,\ q_2,\ \cdots\cdots,\ q_j$$

$$p_1,\ p_2,\ \cdots\cdots,\ p_i,\ r_1,\ r_2,\ \cdots\cdots,\ r_k$$

とおける（$j=0$ や $k=0$ と考えることもある）．すると，

$$f(m)=(p_1\cdot p_2\cdot\cdots\cdots\cdot p_i)\cdot(q_1\cdot q_2\cdot\cdots\cdots\cdot q_j),$$

$$f(n)=(p_1\cdot p_2\cdot\cdots\cdots\cdot p_i)\cdot(r_1\cdot r_2\cdot\cdots\cdots\cdot r_k),$$

$$f(d)=p_1\cdot p_2\cdot\cdots\cdots\cdot p_i$$

であり，

$$f(mn)=(p_1\cdot p_2\cdot\cdots\cdots\cdot p_i)\cdot(q_1\cdot q_2\cdot\cdots\cdots\cdot q_j)\cdot(r_1\cdot r_2\cdot\cdots\cdots\cdot r_k)$$

より，$f(d)f(mn)=f(m)f(n)$ が成り立つ．

⇨注　本問では指数は考える必要がないので，素因数分解をおいて考えると煩雑になる：

$$m=p_1^{a_1}\cdot p_2^{a_2}\cdot\cdots\cdots\cdot p_i^{a_i}\cdot q_1^{b_1}\cdot q_2^{b_2}\cdot\cdots\cdots\cdot q_j^{b_j},$$

$$n=p_1^{c_1}\cdot p_2^{c_2}\cdot\cdots\cdots\cdot p_i^{c_i}\cdot r_1^{d_1}\cdot r_2^{d_2}\cdot\cdots\cdots\cdot r_k^{d_k}$$

$$d=p_1^{e_1}\cdot p_2^{e_2}\cdot\cdots\cdots\cdot p_i^{e_i}$$

$$(e_k=\min\{a_k,\ c_k\}\ (1\leqq k\leqq i))$$

（2）取り出し方の総数は

$$10\cdot 10=100\text{（通り）}$$

である．

$f(mn)=f(m)f(n)$ とは，$f(d)=1$ つまり「m，n が互いに素」ということである．そのような取り出し方は

・$m=1$ のとき $n=1\sim 10$　…10 通り

・$m=2$，4，8 のとき n は奇数　…5 通り

・$m=3$，9 のとき n は 3 の倍数でない　…7 通り

・$m=5$ のとき n は 5 の倍数でない　…8 通り

・$m=6$ のとき n は 2，3 の倍数でない　…3 通り

・$m=7$ のとき n は 7 の倍数でない　…9 通り

・$m=10$ のとき n は 2，5 の倍数でない　…4 通り

なので，全部で 63 通りある．よって

$$p_1=\frac{\mathbf{63}}{\mathbf{100}}$$

である．

$2f(mn)=f(m)f(n)$ とは，$f(d)=2$ つまり「m，n の最大公約数 d が 2，4，8」ということである．そのような取り出し方は

・m が奇数のとき不適　…0 通り

・$m=2$，4，8 のとき n は偶数　…5 通り

・$m=6$ のとき n は 6 以外の偶数　…4 通り

・$m=10$ のとき n は 10 以外の偶数　…4 通り

なので，全部で 23 通りある．よって

$$p_2=\frac{\mathbf{23}}{\mathbf{100}}$$

である．

＊　　＊

ABC 予想においては，自然数 a，b，c が互いに素なので，$R=f(abc)=f(a)f(b)f(c)$ である．

ちなみに，a，b が互いに素で $a+b=c$ であれば，c は a および b と互いに素である．証明は簡単である：

a と c の最大公約数を d とおくと，$b=c-a$ も d の倍数になる．a，b が互いに素なので，$d=1$ である．よって，a，c は互いに素である．同様に b，c も互いに素である．

もちろん，a，c が互いに素であれば，a，b および b，c も互いに素であることが分かる．

また，$f(a)=a$ となるのは，a が「1，素数または異なるいくつかの素数の積」であるときである．

＊　　＊

では，**問題 1** に登場する範囲内（1 以上 10 以下）で，ABC 予想について検証してみよう．

$$1+2=3<R=6,$$

$$1+3=4<R=6,$$

$$\cdots\cdots$$

などで，ほぼすべての組で $c<R$ となる．しかし，1 組だけ $c>R$ となるものがある．分かるだろうか？

c と比べて R を小さくするには，a，b，c のいずれかが「(素数)$^{(\text{大きい指数})}$」という形を含まなければならないことがわかる．この範囲では

$$1+8=9>R=6$$

である．このとき，$c=R^{\log_R c}$ において

$$\log_6 9=1.2262\cdots\cdots$$

であるから，$\varepsilon<0.2262$ のときの“有限個の例外”の 1 つになっていることが分かる．

では，例外を少し探してみよう．まずは，一瞬で例外でないと判断できるものから．

問題 2.　互いに素な自然数 a，b，c が $a+b=c$，$a<b$ を満たすとする．積 abc の互いに異なる素因数全体の積を R とおく．

$a\geqq 2$ で，b が素数であるか，異なるいくつかの素数の積であるとき，$c<R$ となることを示せ．

解　**問題 1** の記号を使うと

$$f(a)\geqq 2,\ f(b)=b,\ f(c)>1$$

$$\therefore\quad R=f(a)f(b)f(c)>2f(b)=2b$$

である．すると，$c=a+b<2b$ より，

$$R-c>2b-2b=0 \quad \therefore \quad c<R$$

が成り立つ．

＊　　＊

これが上記の『c と比べて R を小さくするには，a，b，c のいずれかが「(素数)$^{(\text{大きい指数})}$」という形を含まなければならない』というイメージの元である．そのような組を具体的にいくつか探してみよう．

問題 3. 互いに素な自然数 a，b，c が $a+b=c$，$a<b$ を満たすとする．積 abc の互いに異なる素因数全体の積を R とおく．$c=64$，81 に対して，$c>R$ となるような a，b，c の組を求めよ．

解 $c=64$ のとき，a，b $(a<b)$ は奇数であるから，

$a=1$，3，5，……，29，31

の 16 個を調べる必要がある．仮定より，a，b，c は互いに素なので，**問題 1** の記号を使うと

$$R=f(a)f(b)f(c)=2f(a)f(b)$$

である．

問題 2 を使って調べると，考えるべきは

$(a,\ b)=(1,\ 63)$，$(15,\ 49)$，$(19,\ 45)$

のみであることが分かる．それぞれ

$R=2f(1)f(3^2\cdot 7)=2\cdot 3\cdot 7=42<64=c$，

$R=2f(3\cdot 5)f(7^2)=2\cdot 3\cdot 5\cdot 7=210>64=c$，

$R=2f(19)f(3^2\cdot 5)=2\cdot 3\cdot 5\cdot 19=570>64=c$

であるから，$\boldsymbol{(a,\ b,\ c)=(1,\ 63,\ 64)}$ のみが適する．

$c=81$ のとき，a，b $(a<b)$ は 3 の倍数でないから，

$a=1$，2，4，……，38，40

の 27 個を調べる必要がある．仮定より，a，b，c は互いに素なので，**問題 1** の記号を使うと

$$R=f(a)f(b)f(c)=3f(a)f(b)$$

である．

問題 2 を使って調べると，考えるべきは

$(a,\ b)=(1,\ 80)$，$(5,\ 76)$，$(13,\ 68)$，$(17,\ 64)$，
$(25,\ 56)$，$(29,\ 52)$，$(31,\ 50)$，
$(32,\ 49)$，$(37,\ 44)$

のみであることが分かる．それぞれ

$R=3f(1)f(2^4\cdot 5)=3\cdot 2\cdot 5=30<81=c$，

$R=3f(5)f(2^2\cdot 19)=3\cdot 2\cdot 5\cdot 19=570>81=c$，

$R=3f(13)f(2^2\cdot 17)=3\cdot 2\cdot 13\cdot 17=1326>81=c$，

$R=3f(17)f(2^6)=3\cdot 2\cdot 17=102>81=c$，

$R=3f(5^2)f(2^3\cdot 7)=3\cdot 2\cdot 5\cdot 7=210>81=c$，

$R=3f(29)f(2^2\cdot 13)=3\cdot 2\cdot 13\cdot 29=2262>81=c$，

$R=3f(31)f(2\cdot 5^2)=3\cdot 2\cdot 5\cdot 31=930>81=c$，

$R=3f(2^5)f(7^2)=3\cdot 2\cdot 7=42<81=c$，

$R=3f(37)f(2^2\cdot 11)=3\cdot 2\cdot 11\cdot 37=2442>81=c$

であるから，$\boldsymbol{(a,\ b,\ c)=(1,\ 80,\ 81),\ (32,\ 49,\ 81)}$ が適する．

＊　　＊

登場する素因数の種類が少ないときしか $R<c$ とはならないようである．ここで，$(a,\ b,\ c)=(1,\ 63,\ 64)$，$(1,\ 80,\ 81)$，$(32,\ 49,\ 81)$ のとき，$c=R^{\log_R c}$ において，

$\log_{42}64=1.1126\cdots\cdots$，

$\log_{30}81=1.2920\cdots\cdots$，

$\log_{42}81=1.1757\cdots\cdots$

である．

【ABC 予想】および【ABC 予想の仲間】が正しいような気がしてくる結果である．もちろん，上記の a，b，c，R に対しても，$c<R^2$ が成り立っている．ちなみに，現在までに $c<10^{20}$ くらいまでが調べられているらしく，$\log_R c=1.63$ くらいになる例までは見つかっているそうである．

シラミつぶしで調べていくのは，なかなか大変である．c を決めたときに，「c 以下で c と互いに素な自然数」の分だけ調べることになる．その個数は，整数論において重要なテーマである．オイラーの関数 $\varphi(c)$ と名前が付けられており，c の素因数分解が

$$c=p_1^{a_1}\cdot p_2^{a_2}\cdot\cdots\cdots\cdot p_i^{a_i}$$

のとき，c 以下で c と互いに素な自然数の個数 $\varphi(c)$ は

$$\varphi(c)=c\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\cdots\left(1-\frac{1}{p_i}\right)$$
$$=\frac{c(p_1-1)(p_2-1)\cdots\cdots(p_i-1)}{p_1p_2\cdots\cdots p_i}\cdots\cdots(*)$$

であることが知られている（マスター・オブ・整数などを参照せよ）．

この値については，$c\geqq 3$ において偶数になることが容易に分かる ((*) の分子に注目せよ)：

$c=2^a$ という形以外では，奇素数を素因数にもつので，(奇素数)-1 が偶数になる．$c=2^a$ $(a\geqq 2)$ という形では $\varphi(2^a)=2^{a-1}$ となり，偶数である．

$\varphi(1)=\varphi(2)=1$ のみ例外である．しかし，いま考えている $a+b=c$，$a<b$ という状況では，$c\geqq 3$ なので，$\varphi(c)$ は必ず偶数であり，a，b として考えられる組の個数は $\dfrac{\varphi(c)}{2}$ 通りになる．**問題 3** で調べた個数も確認せよ．

【ABC 予想】や【ABC 予想の仲間】が証明されて大騒ぎになる理由はあるのだろうか？高度な理論を用いて証明される定理なので，我々の理解できる範疇で重要性を見ることはできないだろうか？

実は，身近なところで，この予想のパワーを感じることができる．例えば…

$$1+2^m=3^n$$

となる自然数 m，n を考えたいとする．

$$1+2=3,\ 1+8=9$$

は簡単に見つかるが，「他にはあるのだろうか？」ということが気になってくる．

問題 4. $1+2^m=3^n$ となる自然数 m，n をすべて求めよ．

解 $n=1$ のとき，$m=1$ である．

$n=2$ のとき，$m=3$ である．

以下，$n\geqq 3$ とする．$3^n\geqq 27$ より $m\geqq 5$ である．

n が偶数のとき，$n=2N\,(N\geqq 2)$ とおくことができて，

$$3^{2N}-1=(3^N+1)(3^N-1)$$

は連続する偶数の積

$$(2M+2)2M=4M(M+1)\ \ (M\geqq 4)$$

という形になる．M と $M+1$ はいずれかが奇数で，もちろん，1 より大きい．よって，$3^{2N}-1$ が 2^m の形になることはない．

n が奇数のとき，$n=2N+1\,(N\geqq 1)$ とおけて，

$$3^{2N+1}=3\cdot 9^N$$

となる．9 を 8 で割った余りが 1 なので，$3\cdot 9^N$ を 8 で割った余りは 3 である．しかし，$m\geqq 5$ において $1+2^m$ を 8 で割った余りは 1 である．よって，$1+2^m=3^n$ となることはない．

以上から，

$$\boldsymbol{(m,\ n)=(1,\ 1),\ (3,\ 2)}$$

である．

＊　　＊

本問は数自身の性質から，シラミつぶしすることなくすべてを列挙できた．しかし，一般には困難である．

本問を考える際に，もしも【ABC 予想の仲間】が正しいと分かっていたら，どうなるだろうか．

$$a=1,\ b=2^m,\ c=3^n$$

とすると，仮定を満たすので

$$R=f(1)f(2^m)f(3^n)=6$$

$$\therefore\quad c<R^2=36$$

となる．ゆえに，「$c=3$，9，27 を調べれば終わり」と分かるのである．同様に，【ABC 予想】が正しいと分かっているとしたら，例外が起こっても有限個なので，それがどの範囲に入るかが分かれば，シラミつぶしするべき範囲が特定されることになる．

「起こりそうもないことが起こる可能性があるとしたら，この範囲だけ」と教えてくれたら，非常に有用であろう．しかし，「例外が有限個しかない」ということと「例外が存在し得る範囲を具体的に記述できる」ということは別問題である．そういう意味では，【ABC 予想】と【ABC 予想の仲間】では使いやすさが違っている．【ABC 予想の仲間】が証明されている方がありがたい．

例えば，【ABC 予想の仲間】が正しければ，フェルマーの最終定理「$n\geqq 3$ のとき，$x^n+y^n=z^n$ を満たす自然数の組 $(x,\ y,\ z)$ は存在しない」で考えるべき n を，ごくごく限られたものにすることができる：

そんな組があるとする．x，y，z が互いに素でないとき，それらの最大公約数を d として，

$$x=Xd,\ y=Yd,\ z=Zd$$

とおけて，

$$(dX)^n+(dY)^n=(dZ)^n\quad\therefore\quad X^n+Y^n=Z^n$$

となる．よって，互いに素な組を作ることができるので，互いに素な場合のみ考えれば良い．また，互いに素であることと対称性から，$x<y$ として良い．すると，x^n，y^n，z^n は【ABC 予想の仲間】の仮定を満たしている．よって，

$$z^n<R^2$$

である．また，

$$R=f(x^n)f(y^n)f(z^n)\leqq xyz$$

が成り立つ（等号は，x，y，z がそれぞれ「1，素数または異なる素数の積」のときに成り立つ）．すると，

$$z^n<R^2\leqq x^2y^2z^2<z^2z^2z^2=z^6$$

$$\therefore\quad n<6$$

である．よって，$n=3$，4，5 のみ調べたら良いことになる．

$n=3$，4，5 で $x^n+y^n=z^n$ を満たす自然数の組 $(x,\ y,\ z)$ が存在しないことは，ずっと昔から知られている．実際，前述の通り，$n=4$ の場合は大学入試範囲内で証明可能である．このことからも，【ABC 予想】および【ABC 予想の仲間】の重要性が感じられるだろう．

現高 1 からの新課程では「整数」を本格的に教科書で扱っている．それと相まって，今後の入試問題で【ABC 予想】に関わる興味深い問題が出題されるのではないかと予想できる．

（よしだ　のぶお，予備校講師）