ABC 予想とフェルマーの最終定理

abc-triple

自然数の組(a,b,c)が$a+b=c$，$a<b$，aとbは互いに素を満たすとき，

この自然数の組(a,b,c)をabc-triple とよぶ。

また，ある自然数Xを素因数分解したときの素因数の積を$\mathrm{rad}(X)$と表すことにする。

たとえば，

$\mathrm{rad}(6)=\mathrm{rad}(2\cdot 3)=6$

$\mathrm{rad}(16)=\mathrm{rad}(8)=\mathrm{rad}(4)=\mathrm{rad}(2)=2$

$\mathrm{rad}(17)=17$

$\mathrm{rad}(18)=\mathrm{rad}(2\cdot 3^2)=\mathrm{rad}(2\cdot 3)=6$

すると，

$\mathrm{rad}(a\cdot b\cdot c)<c$を満たす$abc$-triple は無限個あり，

たとえば，$(a,b,c)=\left(1,\ 3^{2^n}-1,\ 3^{2^n}\right)$はこれを満たす。（証明は後述）

ABC 予想

abc-triple (a,b,c)のすべてが$c<\{\mathrm{rad}(abc)\}^2$を満たすという予想

ABC 予想とフェルマーの最終定理

フェルマーの最終定理

nを自然数とすると，$x^n+y^n=z^n$は$n\geq 3$のとき，自然数解(x,y,z)をもたない。

ABC 予想が成り立つとした上でのフェルマーの最終定理の証明

$n\geq 3$のとき，$x^n+y^n=z^n$を満たす自然数解(x,y,z)が存在すると仮定し，

xとyの最大公約数をgとすると，$x=x'g$，$y=y'g$（x'とy'は互いに素）より，

$x^n+y^n=g^n\left(x'^n+y'^n\right)=z^n$となるから，$z$も$g^n$で割り切れる。

よって，この仮定を，$n\geq 3$のとき，$p^n+q^n=r^n$を満たす自然数解(p,q,r)，

（$p<q$，pとqは互いに素）が存在するとしてよい。

すると，$\left(p^n,q^n,r^n\right)$について，$p^n<q^n$，p^nとq^nは互いに素が成り立つから，

$\left(p^n,q^n,r^n\right)$はabc-triple である。

よって，$r^n<\left\{\mathrm{rad}\left(p^nq^nr^n\right)\right\}^2=\{\mathrm{rad}(pqr)\}^2\leq (pqr)^2<\left(r^3\right)^2=r^6$

ゆえに，nが 3 以上 5 以下の自然数のとき，

$x^n+y^n=z^n$を満たす自然数解(x,y,z)が存在する。

ところが，$n=3,4,5$のとき$x^n+y^n=z^n$を満たす自然数解(x,y,z)が存在しないことが，

それぞれオイラー（$n=3$のとき，1753 年），フェルマー（$n=4$のとき，1640 年），

ディリクレとルジャンド（$n=5$のとき，1825 年）により証明されている。

よって，$n\geq 3$のとき，$x^n+y^n=z^n$を満たす自然数解(x,y,z)は存在しない。

$(a,b,c)=\left(1,\,3^{2^n}-1,\,3^{2^n}\right)$が $\mathrm{rad}(abc)<c$ を満たすことの証明

$$
\begin{aligned}
b&=3^{2^n}-1\\
&=3^{2\cdot 2^{n-1}}-1\\
&=\left(3^{2^{n-1}}\right)^2-1\\
&=\left(3^{2^{n-1}}+1\right)\left(3^{2^{n-1}}-1\right)\\
&=\left(3^{2^{n-1}}+1\right)\left(3^{2^{n-2}}+1\right)\left(3^{2^{n-2}}-1\right)\\
&=\left(3^{2^{n-1}}+1\right)\left(3^{2^{n-2}}+1\right)\left(3^{2^{n-3}}+1\right)\left(3^{2^{n-3}}-1\right)\\
&\qquad\vdots\\
&=\left(3^{2^{n-1}}+1\right)\left(3^{2^{n-2}}+1\right)\left(3^{2^{n-3}}+1\right)\cdots\cdot\left(3^{2^k}+1\right)\cdots\cdot\left(3^{2^0}+1\right)\cdot\left(3^{2^0}-1\right)
\end{aligned}
$$

ここで $3^{2^k}+1$ （$0\le k\le n-1$）は n 個あり，いずれも偶数であることと，

$3^{2^0}+1=3^1+1=4=2^2$ であることから，

$\left(3^{2^{n-1}}+1\right)\left(3^{2^{n-2}}+1\right)\left(3^{2^{n-3}}+1\right)\cdots\cdot\left(3^{2^k}+1\right)\cdots\cdot\left(3^{2^0}+1\right)\cdot\left(3^{2^0}-1\right)$は 2^{n+1} で割り切れる。

これと $3^{2^0}-1=3^1-1=2$ より， $b=3^{2^n}-1$ は 2^{n+2} で割り切れる。

よって，

$$
\begin{aligned}
\mathrm{rad}(abc)&=\mathrm{rad}\left(1\cdot\left(3^{2^n}-1\right)\cdot 3^{2^n}\right)\\
&=\mathrm{rad}\left(2^{n+2}\cdot\frac{3^{2^n}-1}{2^{n+2}}\cdot 3^{2^n}\right)\\
&=\mathrm{rad}\left(2\cdot\frac{3^{2^n}-1}{2^{n+2}}\cdot 3\right)\\
&\le\frac{3}{2^{n+1}}\left(3^{2^n}-1\right)\\
&=\frac{3}{2^{n+1}}(c-1)\\
&<\frac{3}{2^{n+1}}c\\
&\le\frac{3}{4}c\\
&<c
\end{aligned}
$$

フェルマー予想と ABC 予想

http://www.math.tohoku.ac.jp/~ytakao/papers/abc.pdf

を読んで自分なりに理解しまとめました。