フェルマー商に関係する数論

神戸大学大学院理学研究科数学専攻

山崎正

Fermat(フェルマー) (1601–1665)

○ Fermat は 1637 年頃次の定理が成立すると書いた.

Fermat の最終定理 (Wiles 1995)　$n \geqq 3$ のとき方程式

$$x^n + y^n = z^n, \quad xyz \neq 0$$

は整数解をもたない.

○ $n = mp$ のとき上の方程式は

$$(x^m)^p + (y^m)^p = (z^m)^p$$

と書けるので, n のときに解があれば p のときにも解があるがことになる. 従って n が 4 の場合と奇素数の場合が問題.

○ 整数係数の多項式で定まる方程式の整数解を求める問題やその一般化を, 不定方程式とか Diophantus 問題という.

Fermat の小定理　p を素数とし, a は整数で $a \not\equiv 0 \bmod p$ とする. このとき

$$a^{p-1} \equiv 1 \bmod p$$

が成り立つ.

○ 合同式

$m > 0$ は自然数, a, b は整数とする. a と b を m で割ったときの余りが一致するとき a と b は m を法として合同であるといい $a \equiv b \bmod m$ と書く.

これは $a - b$ が m で割れる, すなわち m の倍数になることと同じ.

a と b が m を法として合同でないとき $a \not\equiv b \bmod m$ と書く.

例えば

$$3 \equiv 24 \bmod 7, \quad 4 \not\equiv 24 \bmod 11$$

また $a_1 \equiv a_2 \bmod m,\ b_1 \equiv b_2 \bmod m$ なら

$$a_1 + b_1 \equiv a_2 + b_2 \bmod m, \quad a_1 b_1 \equiv a_2 b_2 \bmod m$$

が成立する.

補助定理 1　p を素数とし a, b を整数とする. p が積 ab を割るとき p は a または b のどちらかを割る.

補助定理 2　p を素数とし a は整数で $a \not\equiv 0 \bmod p$ とする. このとき数

$$a,\ 2a,\ 3a,\ \cdots, (p-1)a \bmod p$$

は数

$$1,\ 2,\ 3,\ \cdots, p-1 \bmod p$$

と順序を除いて一致する.

$1 \leqq i < j \leqq p-1$ のとき補助定理 1 より $(j-i)a \not\equiv 0 \bmod\ p$. 従って $ia \not\equiv ja \bmod\ p$ となり補助定理 2 がわかる.

補助定理 2 の最初の数たちの積は $a^{p-1}(p-1)!$ で補助定理 2 より

$$a^{p-1}(p-1)! \equiv (p-1)! \bmod\ p$$

$$(a^{p-1} - 1)(p-1)! \equiv 0 \bmod\ p$$

$(p-1)!$ は p で割れないので補助定理 1 より Fermat の小定理を得る.

○ Fermat 商
整数 $a \geqq 2$ と a を割らない素数 p に対し

$$q_p(a) = \frac{a^{p-1} - 1}{p}$$

を底 a の Fermat 商という.

Fermat 商 $q_p(a)$ 自身は一般に非常に大きな数で, それを p で割った余り $q_p(a) \bmod p$ が問題.

記録の残っている最初の例は Abel (1802–1829) によるもの.

問題 (Abel 1828)　素数 p と $1 < a < p$ なる整数に対して $a^{p-1} - 1$ が p^2 で割れることがあるか.

つまり $q_p(a) \equiv 0 \bmod p$ となることがあるかを問題とした.

定理 (Wieferich 1909)　奇素数 p に対し方程式

$$x^p + y^p + z^p = 0, \quad xyz \not\equiv 0 \bmod p$$

が解を持てば $2^{p-1} \equiv 1 \bmod p^2$ が成立する.

上の定理で言っている

$$x^p + y^p + z^p = 0, \quad xyz \not\equiv 0 \bmod p$$

が解を持たないというのが Fermat の最終定理の第 1 の場合である.
従って $q_p(2) \equiv 0 \bmod p$ が成立しなければ Fermat の最終定理の第 1 の場合が証明できたことのなる.

○ $q_p(2) \equiv 0 \bmod p$ となる素数 p を Wieferich 素数という. Wieferich 素数は 1913 年に 1093 が, 1922 年に 3511 が発見された. 現在 $p < 1.25 \times 10^{15}$ の範囲でこの 2 個以外には無いことが確認されている.

○ 実験結果 ($2 \leqq a \leqq 20$, $p \leqq 179424673$ で $q_p(a) \equiv 0 \bmod p$ となるもの)

a	p
2	1093, 3511
3	11, 1006003
4	1093, 3511
5	20771, 40487, 53471161
6	66161, 534851, 3152573
7	5, 491531
8	3, 1093, 3511
9	11, 1006003
10	3, 487, 56598313
11	71
12	2693, 123653
13	863, 1747591
14	29, 353
15	29131
16	1093, 3511
17	3, 46021, 48947
18	5, 7, 37, 331, 33923, 1284043
19	3, 7, 13, 43, 137, 63061489
20	281, 46457, 9377747, 122959073

実験した $2 \leqq a < 1000$, $p \leqq 179424673$ の範囲で調べてみると

○ $q_p(a) \equiv 0 \bmod p$ となる組 (a, p) の個数は

- $a \leqq 100$ となるものは 241 個,
- $a < 1000$ となるものは 2557 個.

○ 各 a に対し $q_p(a) \equiv 0 \bmod p$ となる p の個数を見てみると, 最小が 0 で最大が 8. 0 から 8 の各数 b に対し $q_p(a) \equiv 0 \bmod p$ となる素数の個数が b となる a がどれだけあるかを数えてみると

0	1	2	3	4	5	6	7	8
69	176	271	232	151	64	27	7	1

8 個持つのは $a = 476$ のときでそれらは

$$3,\ 5,\ 37,\ 109,\ 337,\ 401,\ 5527,\ 1169759$$

○ 大体各 a に対して平均 2.5 個程度の p に対して $q_p(a) \equiv 0 \bmod p$ のなっている.

○ 素数 p 固定して考える. 例えば $p = 5$ のときは次のようになる.

a	$q_5(a)$	$\bmod 5$	a	$q_5(a)$	$\bmod 5$
1	0	0	13	5712	2
2	3	3	14	7683	3
3	16	1	16	13107	2
4	51	1	17	16704	4
6	259	4	18	20995	0
7	480	0	19	26064	4
8	819	4	21	38896	1
9	1312	2	22	46851	1
11	2928	3	23	55968	3
12	4147	2	24	66355	0

$\bmod 5$ で見ると, 0 から 4 までそれぞれ 4 回現れる.

一般に $\bmod p^2$ で考えると, 1 から p^2 までの整数 a で p で割れない数は $p^2 - p$ 個. それらの $q_p(a) \bmod p$ らは 0 から $p-1$ がちょうど $p-1$ 回現れる.

a を固定すると, 素数 p が $q_p(a) \equiv 0 \bmod p$ を満たす確率は $\dfrac{1}{p}$ と思われる.

従って N 以下の素数 p で $q_p(a) \equiv 0 \bmod p$ を満たすものの個数は

$$\sum_{p \leqq N} \frac{1}{p} \sim \log(\log(N))$$

程度と思われる. 一方

$$\log(\log(179424673)) = 2.94472\cdots$$

○ 自然数 n の素因数分解 $n = p_1^{e_1} \cdots p_k^{e_k}$ を取る. このとき n の根基 (radical) を

$$\mathrm{rad}(n) = p_1 \cdots p_k$$

で定める.

***ABC* 予想** (Masser-Oesterlé 1986)　任意に実数 $\varepsilon > 0$ を取ると, $\varepsilon > 0$ のみにより定まる定数 $K(\varepsilon)$ が存在して次が成立する. A, B, C が互いに素な零でない整数で $A + B = C$ を満たせば

$$\max(|A|, |B|, |C|) \leqq K(\varepsilon)(\mathrm{rad}(ABC))^{1+\varepsilon}$$

多冪数 自然数 n が多冪数であるとは, 素数 p が n を割るなら p^2 も n を割ること. いいかえると, 自然数 n を $n = p_1^{e_1} \cdots p_k^{e_k}$ と素因数分解したとき $e_1 \geqq 2, \cdots, e_k \geqq 2$ となること.
連続する 2 個の多冪数は存在する.

$$(8, 9), \quad (288, 289), \quad (675, 676), \quad (9800, 9801), \quad (12167, 12168)$$

$$(235224, 235225), \quad (332928, 332929), \quad (465124, 465125)$$

$$235224 = 2^3 \cdot 3^5 \cdot 11^2, \quad 235225 = 5^2 \cdot 97^2$$

$$332928 = 2^7 \cdot 3^2 \cdot 17^2, \quad 332929 = 577^2$$

Erdös の 予想 (1975)　連続した 3 個の多冪数は存在しない.

定理　ABC 予想が正しければ $2^{p-1} \not\equiv 1 \bmod p^2$ となる素数が無限個ある.

定理　上の Erdös の予想が正しければ $2^{p-1} \not\equiv 1 \bmod p^2$ となる素数が無限個ある.

定理　ABC 予想が正しければ $n-1, n, n+1$ が多冪数となるような自然数 n は有限個しかない.

定理　ABC 予想が正しければ有限個の n を除いて Fermat の最終定理が成立する.

○ $n-1$, n, $n+1$ が多冪数なら

$$(n^2-1)+1 = n^2$$

に ABC 予想を用いると

$$\begin{aligned} n^2 &\leqq K(\varepsilon)(\mathrm{rad}(n^2(n^2-1)))^{1+\varepsilon} \\ &\leqq K(\varepsilon)(n^{\frac{1}{2}}\sqrt{n-1}\sqrt{n+1})^{1+\varepsilon} \\ &\leqq K(\varepsilon)n^{\frac{3}{2}(1+\varepsilon)} \end{aligned}$$

従って

$$n^{\frac{1}{2}-\frac{3}{2}\varepsilon} \leqq K(\varepsilon)$$

例えば $\varepsilon = \frac{1}{6}$ と取ると

$$n^{\frac{1}{4}} \leqq K(\tfrac{1}{6}) \quad \text{すなわち} \quad n \leqq K(\tfrac{1}{6})^4$$

で n は有界.

○ 複素数係数の多項式全体の集合を $\boldsymbol{C}[t]$ と書く. 多項式の和, 差, 積によりこの集合は「環」といわれるものになる. 同様に整数全体の集合 $\boldsymbol{Z}$ も環である.

$\boldsymbol{C}[t]$ と $\boldsymbol{Z}$ は似ている. 例えば割算ができる.

- $a, m > 0$ が整数のとき

$$a = qm + r \quad 0 \leqq r < m$$

と書ける.

- $a(t), m(t)$ が多項式で $m(t)$ は定数でないとすると

$$a(t) = q(t)m(t) + r(t) \quad 0 \leqq \deg(r(t)) < \deg(m(t))$$

と書ける.

定理 (多項式環の場合の Fermat の最終定理) $n \geqq 3$ を自然数とする. 定数ではない互いに素な多項式 $x(t), y(t), z(t) \in \boldsymbol{C}[t]$ で

$$x(t)^n + y(t)^n = z(t)^n$$

を満たすものは存在しない.

○ 零ではない複素数係数の多項式 $f(t) \in \boldsymbol{C}[t]$ を 1 次式の積に分解して

$$f(t) = c\prod_{i=1}^{r}(t - \alpha_i)^{m_i}$$

と書く. ここで $\alpha_1, \alpha_2, \cdots, \alpha_r$ は $f(t)$ の相異なる解で c は零でない定数. 整数 m_i は解 α_i の重複度で多項式 $f(t)$ の次数は

$$\deg(f(t)) = m_1 + \cdots + m_r$$

また $f(t)$ の相異なる解の個数は r でこれを

$$n_0(f(t)) = r$$

と書くことにする.

$$\deg((x-1)^{1000}) = 1000, \quad n_0((x+1)^{1000}) = 1$$

定理 (Stothers(1981)–Mason(1983))　$f(t)$, $g(t)$, $h(t) \in \boldsymbol{C}[t]$ を定数ではない互いに素な多項式で $f(t)+g(t)=h(t)$ を満たすものとする. このとき

$$\max(\deg(f(t)), \deg(g(t)), \deg(h(t))) \leqq n_0(f(t)g(t)h(t)) - 1$$

が成立する.

○ 上の定理を用いると多項式環に対する Fermat の最終定理が示される.

$x(t)$, $y(t)$, $z(t) \in \boldsymbol{C}[t]$ は定数ではなく互いに素で

$$x(t)^n + y(t)^n = z(t)^n$$

を満たすとする. 次数が最大のものを $x(t)$ とすると,

$$\deg(x(t)^n) = n\deg(x(t)), \quad n_0(x(t)^n) = n_0(x(t)) \leqq \deg(x(t))$$

であるから, Stothers–Mason の定理より

$$\begin{aligned} n \cdot \deg(x(t)) &\leqq \deg(x(t)) + \deg(y(t)) + \deg(z(t)) - 1 \\ &\leqq 3\deg(x(t)) - 1 \end{aligned}$$

従って

$$(n-3)\deg(x(t)) \leqq -1$$

仮定より $\deg(x(t)) > 0$ であるから $n-3 < 0$ で $n \leqq 2$.

おしまい

ありがとうございました