

科学・技術の世界 – Fermat の大定理を巡って –

第三回 平成17年4月26日(火)

三次方程式の解法 (1/7)

t に関する三次式

$$(t - \alpha)(t - \beta)(t - \gamma)$$

を展開すると,

$$t^3 - (\alpha + \beta + \gamma)t^2 + (\alpha\beta + \beta\gamma + \gamma\alpha)t - \alpha\beta\gamma$$

となる. これを参考に

$$(t - u - v)(t - \omega u - \omega^2 v)(t - \omega^2 u - \omega v)$$

を展開する. ただし $\omega = (-1 + \sqrt{3}i)/2$ である.

三次方程式の解法 (2/7)

t^2 の係数は

$$\begin{aligned} & -\{(u+v) + (\omega u + \omega^2 v) + (\omega^2 u + \omega v)\} \\ & = -(1 + \omega + \omega^2)u - (1 + \omega + \omega^2)v = 0 \end{aligned}$$

t の係数は

$$\begin{aligned} & (u+v)(\omega u + \omega^2 v) + (\omega u + \omega^2 v)(\omega^2 u + \omega v) \\ & + (\omega^2 u + \omega v)(u+v) \\ = & \{\omega u^2 + (\omega + \omega^2)uv + \omega^2 v^2\} \\ & + \{u^2 + (\omega + \omega^2)uv + v^2\} \\ & + \{\omega^2 u^2 + (\omega + \omega^2)uv + \omega v^2\} \\ = & 3(\omega + \omega^2)uv = -3uv \end{aligned}$$

三次方程式の解法 (3/7)

定数項は

$$-(u + v)(\omega u + \omega^2 v)(\omega^2 u + \omega v)$$

であるが, $\omega^3 = 1$ をかけることにより

$$\begin{aligned} &= -\omega^3(u + v)(\omega u + \omega^2 v)(\omega^2 u + \omega v) \\ &= -(u + v)\{\omega^2(\omega u + \omega^2 v)\}\{\omega(\omega^2 u + \omega v)\} \\ &= -(u + v)(u + \omega v)(u + \omega^2 v) \\ &= -u^3 - v^3 \end{aligned}$$

となる.

三次方程式の解法 (4/7)

以上をまとめると

$$(t-u-v)(t-\omega u-\omega^2 v)(t-\omega^2 u-\omega v) = t^3 - 3uvt - u^3 - v^3$$

を得る. 次に方程式 $t^3 - t = 0$ を解くことを考える.
上の式と係数比較をすると,

$$\begin{cases} -1 = -3uv \\ 0 = u^3 + v^3 \end{cases}$$

上をみたす u, v を見付けることが出来れば, 因数分解の形から $t^3 - t = 0$ の解は以下ようになる.

$$t = u + v, \omega u + \omega^2 v, \omega^2 u + \omega v$$

三次方程式の解法 (5/7)

ここで二次方程式の解と係数の関係を思いおこそう.

$$(s - \alpha)(s - \beta) = s^2 - (\alpha + \beta)s + \alpha\beta.$$

u^3, v^3 は $u^3 + v^3 = 0, u^3 v^3 = 1/27$ であることから
二次方程式

$$s^2 + \frac{1}{27} = 0$$

の解となる. よって $u^3 = i/3\sqrt{3}, v^3 = -i/3\sqrt{3}$.

三次方程式の解法 (6/7)

$i^3 = -i, (-i)^3 = i$ より $u = -i/\sqrt{3}, v = i/\sqrt{3}$ となるので, 求める解は

$$u + v = -\frac{i}{\sqrt{3}} + \frac{i}{\sqrt{3}} = 0$$

$$\omega u + \omega^2 v = \frac{-i(1 + \sqrt{3}i)}{2\sqrt{3}} + \frac{i(1 - \sqrt{3}i)}{2\sqrt{3}} = 1$$

$$\omega^2 u + \omega v = \frac{-i(1 - \sqrt{3}i)}{2\sqrt{3}} \frac{i(1 + \sqrt{3}i)}{2\sqrt{3}} = -1$$

三次方程式の解法 (7/7)

発展として以下の式を用いて任意の四次方程式を解くことが出来る.

$$(t+u+v+w)(t-u-v+w)(t+u-v-w)(t-u+v-w)$$

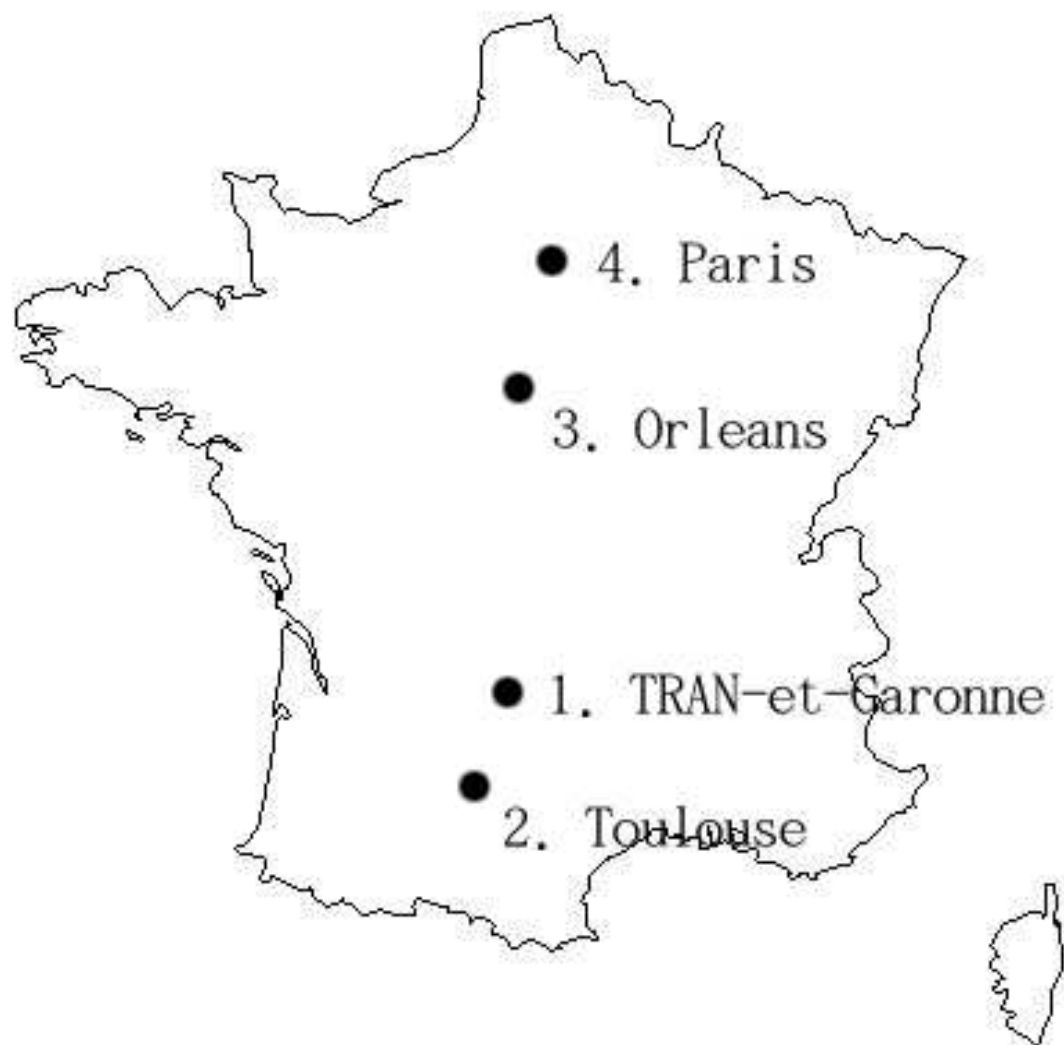
四次方程式の解の公式は16世紀までに得られた. 当然次は五次方程式の解の公式がないか? という問題が考えられるが, これはなかなか解けず, 19世紀になって解決された. 答は

一般の五次方程式の解の公式は存在しない.
というものであった.

Fermat の生涯 (1/3)

- 1601 年誕生.
- 1631 年, 民法学士の学位取得. Toulouse 高等法院の法官となる.
- 1636 年 Mersenne への手紙がヨーロッパで話題となる.
- 1637 – 38 年 Descarte との論争.
- 1648 年 Toulouse 地方議会の勅撰議員となる.
- 1653 年 そのころ流行していた疫病にかかる.
- 1654 年頃 Pascal と確率について議論.
- 1657 年 Wallis らにあてて挑戦状を出す.
- 1665 年 死去.

Fermat の生涯 (2/3)



1. 誕生地
2. 勤務地
3. 大学所在地

Fermat の生涯 (3/3)

ヨーロッパの出来事

日本の出来事

1603 徳川幕府成立

1616 家康没

1610 ~ 1643 ルイ 13 世

1639 鎖国令

1643 ~ 1715 ルイ 14 世

1651 家光没

Fermat の人となり (1/2)

17世紀にはまだ数学の論文を発表する集会や雑誌がなく, 得られた研究成果は本にして出版するか, 文通によって広められた. このような文通サークルで後にパリ・アカデミーの母体となるものを運営していたのが Mersenne 神父である.

1636年に Fermat の同僚が Paris に栄転し, Fermat のことを Mersenne 神父に紹介した. Mersenne は Fermat に招待状を送り, 自分達のサークルに勧誘した. これに Fermat が答えて, Descartes や Pascal との交流が始まったのである.

Fermat の人となり (2/2)

Fermat が出した数学上の問題は数論だけではなく、幾何学に関するものもかなりあった。どちらの分野の出題にも共通して言えることは非常に難しい問題が多かったということで、しかも Fermat は解答や証明をほとんど送らなかった。

また、Fermat は生前、自分の名前を公にすることを完全に拒否した匿名主義者であった。何故 Fermat がこのような態度を取りつづけたのかは今となってはわからない。が、こうした態度は当然人から疎まれ、いろいろと噂をたてられた。

Fermat の小定理 (1/7)

1640 年 Fermat は Frenicle 宛の手紙に次の内容を記した.

定理 1 p を素数としたとき, 任意の自然数 n に対して $n^p - n$ は p で割り切れる.

前述したとおり, Fermat は結果だけ記し, 証明は残していない. が, この定理は現在 Fermat の小定理と呼ばれている.

Fermat の小定理 (2/7)

定理の証明のために二項展開を復習する.

$$\begin{aligned}(a + b)^m &= \sum_{i=0}^m {}_m C_i a^i b^{m-i} \\ &= a^m + (ma^{m-1}b + \cdots + mab^{m-1}) \\ &\quad + b^m\end{aligned}$$

と展開できる. ここで m が素数であるとき, 上の括弧の中は m で割り切れることに注意する.

Fermat の小定理 (3/7)

定理を帰納法を用いて証明する.

まず $n = 1$ のとき明らかに定理は成り立つ.

次に $n = k$ のとき定理が成立すると仮定する. このとき

$$\begin{aligned}(k+1)^p &= k^p + ({}_pC_1 k^{p-1} + \cdots + {}_pC_{p-1} k) + 1 \\ &= k^p - k + (pk^{p-1} + \cdots + pk) + \\ &\quad + k + 1\end{aligned}$$

と展開される.

Fermat の小定理 (4/7)

前項の式を次のように書き替える.

$$(k+1)^p - (k+1) = k^p - k + (pk^{p-1} + \cdots + pk)$$

- $k^p - k \cdots$ 帰納法の仮定から p で割り切れる.
- 上の括弧の中 $\cdots p$ で割り切れる.

よって $(k+1)^p - (k+1)$ も p で割り切れることがわかる.

Fermat の小定理 (5/7)

Fermat の小定理を用いてある数が素数でないことを判定できる. まず Fermat の小定理を以下のように変形する.

定理 2 n, p を互いに素な自然数とする. このとき p が素数であれば, $n^{p-1} - 1$ は p で割り切れる.

これの対偶を取ると次のようになる.

系 1 n, p を互いに素な自然数とする. $n^{p-1} - 1$ が p で割り切れないのであれば, p は素数ではない.

Fermat の小定理 (6/7)

問題 1 511 は素数でないことを証明せよ.

解答 511 は奇数なので, 互いに素な数として 2 が取れる.

そこで $2^{510} - 1$ を考える. $511 = 512 - 1 = 2^9 - 1$ であるので

$$\begin{aligned} 2^{510} - 1 &= (2^9)^{56} \times 2^6 - 1 \\ &= (511 + 1)^{56} \times 2^6 - 1 \end{aligned}$$

となる.

Fermat の小定理 (7/7)

二項定理を用いて展開すると

$$\{(511^{56} + 56 \times 511^{55} + \cdots + 56 \times 511) + 1\} \times 2^6 - 1$$

となり丸括弧の中は 511 で割り切れる. よって $2^{510} - 1$ を 511 で割った余りは $2^6 - 1 = 63$ で 0 とはならず, 511 は素数ではない.