

数学集中講義

素数の秘密 $x^2 \equiv -1$ を解こう！

吉田 信夫

大学への数学 14 年 6 月号 掲載

素数 p について考えるとき、 $(p-1)!$ が重要な役割を演じることをご存じだろうか？本稿では、これに関連する有名なウィルソンの定理を導いた後、

$$x^2 \equiv -1 \pmod{p}$$

を解き、最終的には、4 で割って 1 余る素数と 3 余る素数の違いを明確にすることを目標にする。

まず、余りに関する重要性質から、

問題 1. 素数 p と自然数 k ($1 \leq k \leq p-1$) につ

いて考える。

(1) $p > 2$ とする。 $1 \leq i < j \leq p-1$ を満たす任意の自然数 i, j に対し、 ki, kj を p で割った余りが異なることを示せ。

(2) フェルマーの小定理： $k^{p-1} \equiv 1 \pmod{p}$ を示せ。

解 (1) $kj - ki = k(j-i)$ において、 $1 \leq k \leq p-1$ 、 $1 \leq j-i \leq p-2$ であり、 p は素数であるから、 $k(j-i)$ が p の倍数になることはない。よって、 ki, kj を p で割った余りは異なることが示された。

(2) $p=2$ のとき、 $k=1$ しかないので、

$$k^{p-1} \equiv 1 \pmod{2}$$

は成り立つ。

$p > 2$ のとき、(1) から、

$$k, 2k, 3k, \dots, (p-1)k$$

を p で割った余りはすべて異なる。つまり、これらの中に、 p で割って 1 余るものがただ 1 つ存在し、また、2 余るもの、 $\dots$ 、 $p-1$ 余るものもそれぞれただ 1 つずつ存在する。よって、すべてかけると

$$k \cdot 2k \cdot 3k \cdot \dots \cdot (p-1)k$$

$$\equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$$

$$\therefore k^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

となる。 $(p-1)!$ は p の倍数でないので、

$$k^{p-1} \equiv 1 \pmod{p}$$

となることが分かる。以上で示された。

*

*

論証の鍵は $(p-1)!$ であった。今回はこれが p の倍数にならない、という性質を利用して、フェルマーの小定理を示すことができた。本問では、 $1 \leq k \leq p-1$ しか考えていないが、「 p と互いに素な任意の整数 k 」とできることはすぐに分かる (k を p で割った余りを考えれば、 $1 \leq (\text{余り}) \leq p-1$ となるので、

$$k^{p-1} \equiv (\text{余り})^{p-1} \equiv 1 \pmod{p}$$

となるからである)。

本問 (1) の結果は、「マスター・オブ・整数」の 62 ページに、図を使ってイメージをとらえることができる解説が載っているので、ぜひ、参考にしてもらいたい。

さて、(1) の結果は、フェルマーの小定理ということでも面白いことを教えてくれた。それは、 k^{p-1} を p で割った余りが 1 になるというものであった。例えば $p=5$ のとき、 $k=3$ とすると、

$$k^{p-1} = 3^4 = 81 \equiv 1 \pmod{5}$$

となるが、これが任意の素数 p と p と互いに素な k で成り立つのである。

では、(2) の証明の流れに沿って $3^4 \equiv 1 \pmod{5}$ が成り立つことを確認しよう。

3 に 1, 2, 3, 4 をかけていくと

$$1 \cdot 3 = 3, 2 \cdot 3 \equiv 1, 3 \cdot 3 \equiv 4, 4 \cdot 3 \equiv 2$$

となり、5 で割った余りがすべて異なっている。すると、すべてかけると

$$(1 \cdot 3)(2 \cdot 3)(3 \cdot 3)(4 \cdot 3) \equiv 3 \cdot 1 \cdot 4 \cdot 2$$

$$\therefore 3^4 \cdot 4! \equiv 4! \pmod{5}$$

となるのである。ゆえに、 $(3^4 - 1)4!$ が 5 の倍数になり、 $4!$ が 5 の倍数でないことから、 $3^4 - 1$ が 5 の倍数になる。つまり、

$$3^4 \equiv 1 \pmod{5}$$

が成り立つのである。集合として

$$\{1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3 \text{ を } 5 \text{ で割った余り}\}$$

$$= \{1, 2, 3, 4\}$$

となったので、すべてかけた値に注目したのである。

さて、(1)からは、さらに面白いことも分かる。 $(p-1)!$ を p で割った余りについてである。 $p=2, 3, 5, 7$ で実

集中講義～素数の秘密～

試してみると

$$1! \equiv 1 \pmod{2} \quad 2! \equiv 2 \pmod{3}$$

$$4! \equiv 24 \equiv 4 \pmod{5} \quad 6! \equiv 720 \equiv 6 \pmod{7}$$

となる。どんな法則が成り立ちそうだろうか？

問題 2. 素数 p について考える。ただし、必要ならば、**問題 1** の結果を用いて良い。

(1) 自然数 k ($1 \leq k \leq p-1$) に対し、 $kl \equiv 1 \pmod{p}$ となる自然数 l ($1 \leq l \leq p-1$) がただ 1 つ存在することを示せ。

(2) $k^2 \equiv 1 \pmod{p}$ となる自然数 k ($1 \leq k \leq p-1$) を求めよ。

(3) ウィルソンの定理: $(p-1)! \equiv -1 \pmod{p}$ を示せ。

解 (1) $p=2$ のときは $k=1$ だけであり、 $l=1$ が存在する。

$p > 2$ のとき、**問題 1** (1) より、

$$k, 2k, 3k, \dots, (p-1)k$$

を p で割った余りはすべて異なるので、これらの中に、 p で割って 1 余るものがただ 1 つ存在する。それを kl とおけば、 $kl \equiv 1 \pmod{p}$ か $1 \leq l \leq p-1$ が成り立つ。

以上で示された。

$$(2) \quad k^2 \equiv 1 \iff (k-1)(k+1) \equiv 0 \pmod{p}$$

において、 p が素数で、 $k-1=0, 1, \dots, p-2$ と $k+1=2, 3, \dots, p$ から、求める k は

$$k-1=0 \quad \text{または} \quad k+1=p$$

$$\therefore k=1, p-1$$

である。

(3) $p=2$ のときは、

$$(p-1)! \equiv 1 \equiv -1 \pmod{2}$$

より、成り立つ。

$p=3$ のときも、

$$(p-1)! \equiv 2 \equiv -1 \pmod{3}$$

より、成り立つ。

$p > 3$ のとき、 p は奇数であるから、 $p-1$ は偶数である。

(1)、(2) より、 $k=2, 3, 4, \dots, p-2$ に対して、 $kl \equiv 1 \pmod{p}$ となる自然数 l ($1 \leq l \leq p-1$) が存在するが、それは $l \neq k, p-1$ である。つまり、 $p-3$ 個 (偶数) の数

$$2, 3, 4, \dots, p-2$$

は、 $kl \equiv 1 \pmod{p}$ となるよう 2 個ずつを選んでペアを作ることができるのである ($\frac{p-3}{2}$ 組のペアができる)。

よって、積を計算すると

$$2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2)$$

$$\equiv 1 \cdot 1 \cdot \dots \cdot 1 \quad \left(\frac{p-3}{2} \text{ 個の積} \right)$$

$\equiv 1 \pmod{p}$ である。よって、

$$(p-1)! \equiv 1 \cdot \{2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2)\} \cdot (p-1)$$

$$\equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}$$

が成り立つ。

以上で示された。

*

*

先ほどは $(p-1)!$ が p の倍数にならないことを利用しただけだったが、本問では、 $(p-1)!$ を p で割った余りも求めることができた。これがウィルソンの定理である。

一般論で示すことができたので、成立することは分かった。実は、具体例でみると面白い。

$p=11$ として考えよう。

$$(p-1)! = 10! = 3628800$$

であるが、11 で割ると

$$3628800 = 329890 \cdot 11 + 10$$

$$\equiv 10 \equiv -1 \pmod{11}$$

となる。確かに成り立つようだ。これを、解答の証明の意味が分かるようにすると、以下ようになる。

mod 11 で

$$2 \cdot 6 = 12 \equiv 1, \quad 3 \cdot 4 = 12 \equiv 1, \quad 5 \cdot 9 = 45 \equiv 1,$$

$$7 \cdot 8 = 56 \equiv 1$$

となるので、

$$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$$

$$= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10$$

$$\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1)$$

$$\equiv -1$$

となる。

これが (3) の解答の意味である。 $kl \equiv 1 \pmod{p}$ と

なる $\frac{p-3}{2}$ 組のペアができ、それらを利用して計算した。

そして、 $\frac{p-3}{2}$ 組のペアが必ず作れることを (1)、(2) で示したのである。

*

*

では、次が本稿のメインテーマ。

$$x^2 \equiv -1 \pmod{p}$$

の解法について考えてみよう。ただし、自然数 x は

$1 \leq x \leq p-1$ の範囲で探していこう。もちろん、 $x=i$ (虚数) を解としてはならない！

まず、 $p=2$ のときは、 $x=1$ が解である。これは

$$x^2 = 1 \equiv -1 \pmod{2}$$

集中講義～素数の秘密～

より、成り立つことが分かる。もちろん、他にはない。

では、それ以外の素数、つまり奇数の素数について考えてみよう。奇数の素数は、4で割った余りで分類できる。それぞれ考えてみよう

問題 3. p が 4 で割って 3 余る素数のとき、

$$x^2 \equiv -1 \pmod{p} \quad (1 \leq x \leq p-1)$$

を満たす x が存在しないことを示せ。ただし、必要ならば **問題 1** の結果を用いて良い。

解 $x^2 \equiv -1 \pmod{p} \quad (1 \leq x \leq p-1)$

となる自然数 x が存在すると仮定する。

$p = 4m + 3$ とおくと、フェルマーの小定理から

$$x^{p-1} = x^{4m+2} \equiv 1 \pmod{p}$$

である。一方、仮定から

$$x^{4m+2} = (x^2)^{2m+1} \equiv (-1)^{2m+1} = -1 \pmod{p}$$

である。ゆえに、

$$1 \equiv -1 \quad \therefore 2 \equiv 0 \pmod{p}$$

となる。これでは 2 が p の倍数となってしまう、不合理である。

よって、仮定は誤りで、

$$x^2 \equiv -1 \pmod{p} \quad (1 \leq x \leq p-1)$$

となる自然数 x が存在しないことが示された。

* * *

例えば、4 で割って 3 余る素数 $p = 7$ のとき、 $1 \leq x \leq 6$ の自然数 x で $x^2 \equiv -1 \pmod{7}$ となることはない。実際、 $\text{mod } 7$ で

$$1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 2, 4^2 = 16 \equiv 2,$$

$$5^2 = 25 \equiv 4, 6^2 = 36 \equiv 1$$

となる。

では、4 で割って 1 余る素数 $p = 13$ のときはどうだろうか？ $\text{mod } 13$ で

$$1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 \equiv 3,$$

$$5^2 = 25 \equiv -1, 6^2 = 36 \equiv 10, 7^2 = 49 \equiv 10,$$

$$8^2 = 64 \equiv -1, 9^2 = 81 \equiv 3, 10^2 = 100 \equiv 9,$$

$$11^2 = 121 \equiv 4, 12^2 = 144 \equiv 1$$

である。 $x^2 \equiv -1$ となる x として $x = 5, 8$ が見つかった！

しかし、上記の計算には無駄が多かった。7 以降は

$$7^2 \equiv (-6)^2 \equiv 10$$

などと簡単に計算できたのである。

さて、具体的な p で x を求めることができたからといって、一般論がどうなるか、まだ不明である。実は、 x を求める公式が存在する。次の問題で確認してみよう。

問題 4. p が 4 で割って 1 余る素数のとき、

$$x = \left(\frac{p-1}{2}\right)!$$

とおくと、 $x^2 \equiv -1 \pmod{p}$ であることを示せ。ただし、必要ならば **問題 2** の結果を用いて良い。

解 $p-1$ が 4 の倍数であるから、

$$\begin{aligned} x &= 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} \\ &\equiv \{-(p-1)\} \cdot \{-(p-2)\} \cdot \dots \cdot \left\{-\left(p - \frac{p-1}{2}\right)\right\} \\ &\quad \pmod{p} \\ &= (-1)^{\frac{p-1}{2}} \frac{p+1}{2} \cdot \dots \cdot (p-2) \cdot (p-1) \\ &= \frac{p+1}{2} \cdot \dots \cdot (p-2) \cdot (p-1) \end{aligned}$$

である。よって、**問題 2** のウィルソンの定理より、

$$x^2 \equiv (p-1)! \equiv -1 \pmod{p}$$

である。

* * *

p が 4 で割って 1 余る素数のとき、

$$x^2 \equiv -1 \pmod{p}$$

となる自然数 x が存在することが分かった。 $p = 13$ では $x = 5, 8$ であったが、

$$\left(\frac{13-1}{2}\right)! = 720 \equiv 5 \pmod{13}$$

であり、 $8 \equiv -5 \pmod{13}$ である。一般的に、

$$x^2 \equiv -1 \pmod{p} \quad (1 \leq x \leq p-1)$$

を満たす x として、

$$x \equiv \left(\frac{p-1}{2}\right)!, -\left(\frac{p-1}{2}\right)! \pmod{p}$$

となる 2 つが見つかる。他にはあるのだろうか？

これについて、少し考察してみよう。

* * *

$p > 3$ とし、 $1 \leq x < y \leq p-1$ を満たす自然数 x, y が

$$y^2 \equiv x^2 \pmod{p}$$

を満たすとしよう。すると、

$$(y-x)(y+x) \equiv 0 \pmod{p}$$

となる。 p が素数であるから、

$$1 \leq y-x \leq p-2, 3 \leq y+x \leq 2p-3$$

より、

$$y+x = p \quad \therefore y = p-x \equiv -x \pmod{p}$$

となる。つまり、 $1 \leq x < y \leq p-1$ を満たす自然数 x, y について、 x^2, y^2 を p で割った余りが等しくなるのは、

$$y \equiv -x \pmod{p}$$

集中講義～素数の秘密～

のときのみであることが分かった。

特に、4で割って1余る素数 p に対し、

$$x^2 \equiv -1 \pmod{p} \quad (1 \leq x \leq p-1)$$

を満たす x は2個しか存在しないことが分かった。

$1^2, 2^2, \dots, (p-1)^2$ を p で割った余りは、同じものが2つつ現れる。 p が4で割って3余るときは、その余りの中に-1が現れず、1余るときは-1が現れるのである。

*

*

ここまでから分かったことをまとめておこう。

p が素数のとき、

$$x^2 \equiv -1 \pmod{p} \quad (1 \leq x \leq p-1)$$

を満たす x は、

・ $p=2$ のとき、 $x=1$

・ p が4で割って3余るとき、存在しない

・ p が4で割って1余るとき、

$$x \equiv \left(\frac{p-1}{2}\right)!, -\left(\frac{p-1}{2}\right)! \pmod{p}$$

となる2つの x が解である

*

*

$x^2 \equiv -1 \pmod{p}$ について色々と考えてきたが、実は

問題 3の派生事項として、以下が分かっている。

自然数 x に対し、 x^2+1 は4で割って3余るような素数を素因数にもたない。

言い方を変えると、自然数 x に対し、 x^2+1 は2か「4で割って1余る素数」しか素因数にもたないことが分かったのである。例えば、

$$8^2+1=65=5 \cdot 13$$

$$9^2+1=82=2 \cdot 41$$

などである。特に、(偶数) $^2+1$ という形の自然数は奇数であるから、4で割って1余る素数しか素因数にもたないことが分かる。これはなかなか強力な制限である。この事実を用いると、素数の個数に関する次の事実が分かる。

問題 5. 4で割って1余る素数は無数に存在することを示せ。

解 4で割って1余る素数が n 個しかないとし、それ

らを

$$p_1, p_2, p_3, \dots, p_n$$

とおく。これらを用いて

$$P = (2p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n)^2 + 1$$

とおく。

すると、 P は4で割って1余る素数以外を素因数にもたない。

一方、 P は $p_1, p_2, p_3, \dots, p_n$ のどれとも互いに素である。

これは不合理であり、仮定は誤りである。よって、4で割って1余る素数は無数に存在する。

*

*

ちなみに、4で割って3余る素数も無数に存在する。これは「余り1」よりも簡単に証明できる：

問題 6. 4で割って3余る素数は無数に存在することを示せ。

解 4で割って3余る素数が n 個しかないとし、それらを

$$q_1, q_2, q_3, \dots, q_n$$

とおく。これらを用いて

$$Q = 4(q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_n) - 1$$

とおく。すると、これは $q_1, q_2, q_3, \dots, q_n$ のどれとも互いに素で、しかも奇数である。ゆえに、 Q の素因数は、4で割って1余るものばかりである。すると、 Q は4で割って1余るはずである。

しかし、おき方から、 Q は4で割って3余る数である。これは不合理である。

よって、仮定は誤りで、4で割って3余る素数は無数に存在する。

*

*

4で割って3余る素数の積は、4で割って1余ることもあるので、**問題 5**を**問題 6**のように示せない。

素数はほぼすべてが奇数であるが、4で割って1余る素数も、3余る素数も、無数に存在するのである。そして、深く探っていくと、4で割って1余る素数

$$5, 13, 17, 29, 37, 41, \dots$$

と、4で割って3余る素数

$$3, 7, 11, 19, 23, 31, \dots$$

では、大きく性質が異なっているのである。

素数には秘密がたくさんある。ぜひ探ってもらいたい。

(よしだ のぶお, 予備校講師)