フェルマーの小定理について

担当：大矢 浩徳 (OYA Hironori)

本資料では，第 3 回講義資料で解説した $\mathbb{Z}/n\mathbb{Z}$ における和および積の応用の 1 つとしてフェルマーの小定理を紹介する．さらに，フェルマーの小定理の一般化・応用例についても解説を行う．

まず，フェルマーの小定理を示すために，以下の命題を準備する．

命題

p を素数とする．このとき，任意の $a, b \in \mathbb{Z}$ に対し，

$$([a]_p + [b]_p)^p = ([a]_p)^p + ([b]_p)^p$$

ここで p 乗は，$\mathbb{Z}/p\mathbb{Z}$ における $\times$ を p 回繰り返し行うという意味である．

証明.

$$\begin{aligned}([a]_p + [b]_p)^p &= ([a+b]_p)^p \\ &= [(a+b)^p]_p \\ &= \left[a^p + {}_p\mathrm{C}_1 a^{p-1}b + {}_p\mathrm{C}_2 a^{p-2}b^2 + \cdots + {}_p\mathrm{C}_{p-1}ab^{p-1} + b^p\right]_p \quad \text{(二項定理)}.\end{aligned}$$

ここで，${}_p\mathrm{C}_k = \dfrac{p!}{k!(p-k)!}$ $(k = 1, \ldots, p-1)$ である．いま，p は素数なので，$k = 1, \ldots, p-1$ のとき，$k!(p-k)!$ は p では割り切れない．一方で，$p!$ は p で割り切れることに注意すると，${}_p\mathrm{C}_k$ は $k = 1, \ldots, p-1$ のとき，p の倍数であることがわかる．これより，$\mathbb{Z}/p\mathbb{Z}$ における同一視のルールから，

$$\left[a^p + {}_p\mathrm{C}_1 a^{p-1}b + {}_p\mathrm{C}_2 a^{p-2}b^2 + \cdots + {}_p\mathrm{C}_{p-1}ab^{p-1} + b^p\right]_p = [a^p + b^p]_p.$$

以上より，$([a]_p + [b]_p)^p = [a^p + b^p]_p = ([a]_p)^p + ([b]_p)^p$ となる． □

以下がフェルマーの小定理 (Fermat's little theorem)[*1]と呼ばれる定理である．

定理 (フェルマーの小定理)

p を素数する．このとき，任意の $a \in \mathbb{Z}$ に対し，

$$[a^p]_p = [a]_p.$$

さらに，a が p の倍数でないとき (つまり $[a]_p \neq [0]_p$ のとき)，

$$[a^{p-1}]_p = [1]_p.$$

証明. まず $[a^p]_p = [a]_p$ を示す．$a = 0$ のとき，$[0]_p = [0]_p$ となって成立する．

[*1] フェルマーの「小」定理と呼ばれているのは，有名なフェルマーの最終定理 (Fermat's last theorem) との区別のためである．フェルマーの最終定理とは「$n \geq 3$ のとき，$x^n + y^n = z^n$ を満たす正の整数 x, y, z は存在しない」という定理で，P.Fermat(1607–1665) がこの主張を述べてから 350 年以上かかって A.Wiles によって 1995 年に証明された．

$a > 0$ のとき，命題を繰り返し用いると，

$$\begin{aligned}[a^p]_p = ([a]_p)^p = ([1]_p + [a-1]_p)^p &= ([1]_p)^p + ([a-1]_p)^p \\ &= ([1]_p)^p + ([1]_p + [a-2]_p)^p = ([1]_p)^p + ([1]_p)^p + ([a-2]_p)^p \\ &\cdots \\ &= \underbrace{([1]_p)^p + ([1]_p)^p + \cdots + ([1]_p)^p}_{a\text{ 個}} = \underbrace{[1]_p + [1]_p + \cdots + [1]_p}_{a\text{ 個}} = [a]_p\end{aligned}$$

$a < 0$ のとき，

$$[a^p]_p = [(-1)^p(-a)^p]_p = (-1)^p[(-a)^p]_p = (-1)^p[-a]_p \quad (-a > 0 \text{ なので上で示したことよりわかる})$$

となる．ここで，$p = 2$ のとき，$[-a]_2 = [a]_2$ なので，$(-1)^2[-a]_2 = [a]_2$．$p > 2$ のとき，p は奇数なので，$(-1)^p[-a]_p = -[-a]_p = [a]_p$．これより，いずれの場合も，

$$[a^p]_p = (-1)^p[-a]_p = [a]_p$$

が成立する．以上で，任意の $a \in \mathbb{Z}$ に対し，$[a^p]_p = [a]_p$ が示された．

次に，$[a]_p \neq [0]_p$ のとき，第 3 回講義資料命題 2.9 より (p.12 の観察も参考にせよ)，$[a]_p^{-1}$ が存在することがわかる．よって，$([a]_p)^p = [a^p]_p = [a]_p$ の両辺に $[a]_p^{-1}$ を掛けて，

$$([a]_p)^{p-1} = [a^{p-1}]_p = [1]_p$$

を得る． □

例 1.

$$[1^4]_5 = [1]_5 \qquad [2^4]_5 = [16]_5 = [1]_5 \qquad [3^4]_5 = [81]_5 = [1]_5 \qquad [4^4]_5 = [256]_5 = [1]_5$$

$$[2^{30}]_{31} = [1073741824]_{31} = [31 \times 34636833 + 1]_{31} = [1]_{31}$$

フェルマーの小定理の一般化：オイラーの定理. フェルマーの小定理は，以下のような形で p が素数でない場合に一般化される．これはオイラーの定理 (Euler's theorem) と呼ばれる．

定理 (オイラーの定理)

n が正の整数，$a \in \mathbb{Z}, \gcd(a, n) = 1$ のとき，

$$[a^{\varphi(n)}]_n = [1]_n.$$

オイラーの定理で n を素数とすると，a が n の倍数でさえなければ $\gcd(a, n) = 1$ となり，しかも $\varphi(n) = n-1$ となるので (第 3 回講義資料 p.12 参照)，確かにこの定理はフェルマーの小定理を特別な場合として含んでいる．オイラーの定理は群論を学ぶと，群論における一般的な定理から直ちに証明することができる．今後の講義内で扱うので楽しみにしていてほしい．

例 2. $\varphi(12) = 4$ なので，

$$[5^4]_{12} = [625]_{12} = [1]_{12} \qquad [7^4]_{12} = [2401]_{12} = [1]_{12} \qquad [11^4]_{12} = [14641]_{12} = [1]_{12}$$

フェルマーの小定理と素数判定. フェルマーの小定理の主張において，p が素数であるという仮定は本質的である．例えば，n が 4 以上の素数でない自然数のとき，a を $\gcd(a, n) > 1$ となる数 (つまり a は n と互いに素でない．例えば a が n の 1 でない約数) とすると，必ず

$$[a^{n-1}]_n \neq [1]_n$$

となる．なぜなら，$[a^{n-1}]_n = [1]_n$ であるとすると，$[a^{n-2}]_n$ が $[a]_n$ の $\times$ に関する逆元であるということになるので，とくに $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ となるが，これは第 3 回講義資料命題 2.9 に反するためである．これより，以下がわかる．

定理

2 以上の自然数 n に対し，以下は同値である．

(1) n は素数である．
(2) $1 \leq a \leq n-1$ なる全ての自然数 a について，$[a^{n-1}]_n = [1]_n$ となる．
(3) $1 \leq q \leq n-1$ なる全ての素数 q について，$[q^{n-1}]_n = [1]_n$ となる．

証明. (1) と (2) の同値性については，上で述べた通りである．(2) $\Rightarrow$ (3) は自明なので，(3) $\Rightarrow$ (2) のみ示せば良いが，これは，$[a^{n-1}]_n = [1]_n, [b^{n-1}]_n = [1]_n$ のとき，$[(ab)^{n-1}]_n = [1]_n$ となることからわかる． □

この定理は素数判定に用いることができる．n を 2 以上の自然数とする．$a \in \mathbb{Z}_{>0}$ に対し，

$$[a^{n-1}]_n = [1]_n$$

が成立するとき，n は底 a について**フェルマーテスト**にパスしたという．この言葉を用いれば，n が $1 \leq q \leq n-1$ なる全ての素数 q についてのフェルマーテストにパスする場合，n は素数であると言える．上で考察したように，n が合成数 (素数でない数) のとき，q が n の約数となる素数である場合，n は底 q についてフェルマーテストにパスしない．合成数で，その約数とならない全ての素数についてフェルマーテストにパスする数を**絶対偽素数**，あるいは**カーマイケル数**という．絶対偽素数は小さい方から $561, 1105, 1729, \ldots$ と続き，無限に存在することが知られている．

フェルマーの小定理と RSA 暗号. フェルマーの小定理は **RSA 暗号**と呼ばれる暗号の基本原理にもなっている．これは Ron Rivest, Adi Shamir, Leonard Adleman の 3 名によって 1977 年に考案された公開鍵暗号と呼ばれる暗号の 1 つである．その仕組みをここで簡単に説明しよう．

私が A さんから情報を貰いたいとする．このとき，私は以下のものを準備すればよい．

- (大きな) 相異なる素数 p, q.
- $(p-1)(q-1)$ と互いに素な自然数 e.

ここで，私は A さんに

$$n = pq, e$$

のみを伝える．この 2 つが**公開鍵**と呼ばれる情報になる．それに対して，素数 p と q が**秘密鍵**である．その名の通り，公開鍵は第三者に見られても良い情報，秘密鍵は他の人に見せてはいけない情報である．「$n = pq$ が公開鍵なのだから n を知っていればそれを因数分解すれば p や q がわかるではないか」と思われるかもしれないが，実は p と q が非常に大きな素数の場合，n を因数分解して p, q を見つけるというのはコンピュータでも膨大な時間がかかる問題となる．このため，「実質 n からはわからない」情報になる．このため，もしどんなに大きい整数でもその因数分解が簡単に計算できるようなアルゴリズムが発明されてしまったら，今から説明する暗号は破綻してしまう．

さて，n と e を知った A さんは，1 以上 n 未満の x を私に暗号化して伝えることができる[*2]．それは以下のようにする．

$$[x^e]_n = [r]_n$$

を満たす $0 \leq r < n$ を計算し (つまり x^e を n で割った余り)，その r を私に伝える．

つまり，この r が x を暗号化した数字である．この r から元の x(つまり $\mathbb{Z}/n\mathbb{Z}$ における “e 乗根”) を p, q の情報を知らずに n と e だけを使って計算するのが一般には難しいということがこの暗号の安全性の根拠と

[*2] 「数字じゃなくて文章を送りたい」と思うかもしれないが，その場合は単に文字を数字に対応させれば良いので，問題にはならない．また，ここでは数字の大きさに制限を付けたが，それより大きい数字も数字の桁でいくつかに区切って送れば良いので，送れないというわけではない．

なっている．さて，p, q の情報を用いてどのように x が計算できるだろうか．これは次のようにすれば良い．$L \coloneqq (p-1)(q-1)$ とする．まず，$\gcd(e, L) = 1$ だったことを思い出し，第 3 回講義資料 2.3 節の方法を用いて，

$$ed - Lf = 1$$

を満たす整数 (d, f) を求めておく．ここで，第 3 回講義資料 p.6 に述べたこの方程式の一般解の形を見ると，d, f は必ず正の値のもので取れることがわかるので，正の値になるように取っておく．このとき，上の r に対し，以下が成立する．

次のように x が復元される．

$$[r^d]_n = [x]_n$$

ここで，x は 1 以上 n 未満としていたので，r^d からただ 1 つに定まることに注意する．

証明. $1 = ed - Lf = ed - (p-1)(q-1)f, d > 0, f > 0$ に注意すると，

$$[r^d]_p = [x^{ed}]_p = [x^{1+(p-1)(q-1)f}]_p = [x]_p([x^{p-1}]_p)^{(q-1)f}$$
$$[r^d]_q = [x^{ed}]_q = [x^{1+(p-1)(q-1)f}]_q = [x]_q([x^{q-1}]_q)^{(p-1)f}$$

ここで，p, q は素数なので，フェルマーの小定理より，$[x^{p-1}]_p = [1]_p, [x^{q-1}]_q = [1]_q$．よって，

$$[r^d]_p = [x]_p \quad \text{かつ} \quad [r^d]_q = [x]_q.$$

このとき，$r^d - x$ は p でも q でも割り切れるということになるので，p, q は相異なる素数であるから，$r^d - x$ は $n = pq$ でも割り切れるということがわかる．よって，

$$[r^d]_n = [x]_n.$$

□

注意 1. ここで，いくつかの注意を述べておこう．

- RSA 暗号において行った操作のみを要約すると，
  - $1 \leq x < n$ を送りたいとき，$[x^e]_n = [r]_n$ $(1 \leq r < n)$ として，r を送信.
  - r を受信した側は $[r^d]_n = [x]_n$ $(1 \leq x < n)$ として，x を復元.

  となる．これを見ると，一旦 d を求めてしまえば，p, q, L はもう使用しないということがわかる．よって，これらは安全に廃棄してしまっても構わない.
- ここでは簡単のために，$L = (p-1)(q-1)$ とおいたが，証明中に用いたのは，e と L が互いに素 ($1 = ed - Lf$ なる $d, f > 0$ が求まる)，L が $p-1, q-1$ で割り切れるという事実のみである．このため，L は $p-1$ と $q-1$ の最小公倍数として取れば問題ない．実際，このようにした方が d としては一般に小さいものが得られるため，最小公倍数を用いて説明されているものも多い.

例 3. $p = 17, q = 31$ としてみよう．このとき，$L = (p-1)(q-1) = 480$ なので，例えば，$e = 37$ ととる．ここで，私は A さんに $n = pq = 527$ と $e = 37$ を伝える (これらは A さん以外に漏れても問題ない)[*3]．一方で，$ed - Lf = 37d - 480f = 1$ を満たす d, f を求めておく．

$$480 = 12 \times 37 + 36 \qquad 37 = 1 \times 36 + 1$$

であるので，

$$\begin{aligned} 1 &= 37 - 1 \times 36 \\ &= 37 + (-1) \times (480 - 12 \times 37) \\ &= 13 \times 37 + (-1) \times 480 \end{aligned}$$

[*3] 527 の因数分解はすぐに計算できるので，この例は実際の暗号としての意味はない．これはただ様子を説明するための例である.

より，$(d, f) = (13, 1)$ が $37d - 480f = 1$ を満たす整数の組の例である ($d > 0, f > 0$ も成立しているのでこれをそのまま使えば良い).

さて，A さんが私に 12 という数字を暗号化して送りたかったとしよう．A さんは私から $e = 37$ と聞いているので，12^{37} を

$$12^{37} = 850562249982110214457613168411482993459 2$$

と計算し，これを $n = 527$ で割った余り 241 を私に送信する[*4].

241 を受け取った私は，先ほど計算した $d = 13$ を用いて，241^{13} を

$$241^{13} = 92517002510467100946797213599 21$$

と計算する．すると，これを $n = 527$ で割った余りを計算することで，12 が復元される．

[*4] ちなみにここではコンピュータを用いて 12^{37} を計算しているが，$[12^{37}]_{527}$ のみ求めればよいので，12^{37} を実際に計算する必要はない．例えば，$12^3 = 1728$ なので，$[12^3]_{527} = [147]_{527}$．$147^2 = 21609$ なので，$[12^6]_{527} = [147^2]_{527} = [2]_{527}$．$2^6 = 64$ なので，$[12^{36}]_{527} = [2^6]_{527} = [64]_{527}$．$64 \times 12 = 768$ なので，$[12^{37}]_{527} = [64 \times 12]_{527} = [241]_{527}$ というようにすれば，普通の電卓でも簡単に計算できる．次の 241^{13} についても同様である．