離散数学 講義資料 (8)

8.1 素数

本節は，教科書 3.3 節の後半 (pp.140–147) に対応する．

補題 8.1 p を素数とし，a を $a \not\equiv 0 \pmod p$ なる整数とし，$Z_p^\times = \{1, 2, \ldots, p-1\}$ とする．このとき，関数 $f_a : Z_p^\times \to Z_p^\times$ が以下で定義可能であり，さらに，f_a は全単射となる．

$$f_a(i) \stackrel{\text{def}}{=\!=} ai \bmod p$$

証明

- 最初に，$f_a(i) = ai \bmod p$ によって関数 $f_a : Z_p^\times \to Z_p^\times$ の定義が与えられることを示す．具体的には，任意の $i \in Z_p^\times$ に対し $ai \bmod p \in Z_p^\times$ を示せば十分．

  ある $i \in Z_p^\times$ に対し $ai \bmod p \notin Z_p^\times$ と仮定する．mod の定義より $0 \le ai \bmod p < p$ であるので $ai \bmod p = 0$，すなわち $p \mid ai$．これは，$(p, a) = (p, i) = 1$ に矛盾．

- 次に f_a が単射であることを示す．

$$\begin{aligned} f_a(i) = f_a(j) &\Rightarrow ai \bmod p = aj \bmod p \\ &\Rightarrow ai \equiv aj \pmod p \\ &\Rightarrow i \equiv j \pmod p \qquad ((a,p) = 1 \text{ より}) \\ &\Rightarrow i = j \end{aligned}$$

- 最後に f_a が全射であることを示す．f_a は単射なので，$f_a(1), f_a(2), \ldots, f_a(p-1)$ は全て異なる値をとる．よって，$|f_a(Z_p^\times)| = p - 1$．ここで，$|Z_p^\times| = p - 1$ なので，$f_a(Z_p^\times) = Z_p^\times$．　□

定理 8.2 (**フェルマーの小定理** (Fermat's Little Theorem))
p を 2 以上の整数とし，a を $(a, p) = 1$ となる整数とする．

$$p \text{ が素数} \implies a^{p-1} \equiv 1 \pmod p$$

証明 $Z_p^\times = \{1, 2, \ldots, p-1\}$ とし，$f_a : Z_p^\times \to Z_p^\times$ を補題 8.1 で定義した関数とする．f_a の定義から，各 i で

$$ai \equiv f_a(i) \pmod p$$

が成立．f_a は全単射なので $f_a(1) f_a(2) \cdots f_a(p-1) = (p-1)!$ であることを考えて，各 $i = 1, 2, \ldots, p-1$ に対する上式を片々掛け合わせると

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

となる．$((p-1)!,\ p) = 1$ であることを考えて両辺を $(p-1)!$ で割ると $a^{p-1} \equiv 1 \pmod p$ となり求める合同式が得られる．　□

アルゴリズム 8.3 (フェルマーテスト) 入力として整数 n をとる．$2 \leq a < n$ となる整数 a をランダムに生成して，

$$a^{n-1} \equiv 1 \pmod{n}$$

をチェック．もし，この合同式が成立しないならば n は合成数，成立するならば素数の可能性大． □

NOTE: 何故，上記のフェルマーテストの出力の部分が「素数の可能性大」と書いているかというと，フェルマーの小定理の逆は一般には成立しない，すなわち $a^{p-1} \equiv 1 \pmod{p}$ だとしても p が合成数の場合があるのである．実際，

$$2^{341-1} \equiv 1 \pmod{341}$$

であるが，341 は素数でない ($341 = 11 \times 31$)．このような数を擬素数と呼ぶ．

NOTE: 通常フェルマーテストは繰り返し適用する事により判定確率を高める．このような判定法のことを一般に確率的素数判定法と呼ぶ．他にもいろいろ開発されている．実用上はそれなりに有用．

定義 8.4 n を 2 以上の合成数とする．$(a, n) = 1$ となる整数 a に対して $a^{n-1} \equiv 1 \pmod{n}$ となるとき，n を a を底とする**擬素数** (pseudoprime) と呼ぶ．特に，n と互いに素な $1 < a < n$ となる全ての整数 a に対し $a^{n-1} \equiv 1 \pmod{n}$ となるとき，n を**カーマイケル数** (Carmichael number) と呼ぶ． □

NOTE: カーマイケル数が無限個存在するかどうかは長い間，未解決問題 (Open Problem) であった．しかし，ごく最近 (1992 年)，Alford, Granville, Pomerance によって肯定的に解決された．すなわち，カーマイケル数は無限個存在するのである．だが一方，カーマイケル数は非常に稀にしか存在しないことが知られている．実際，10000 以下のカーマイケル数は

$$561,\ 1105,\ 1729,\ 2465,\ 2821,\ 6601,\ 8911$$

の 7 個しか存在しない．さらにいうと，100 億 ($= 10^{10}$) 以下で考えると，素数は 455052511 個あるが，2 を底とする擬素数は 14887 個しか存在せず，カーマイケル数はたったの 1547 個しか存在しない．

NOTE: 注意してほしいのは,「素数判定」と「素因数分解」が異る問題であるという事である．さらに言うと，素数判定は比較的容易に行えるようになったが，素因数分解を行うのは (少なくとも現時点では) 非常に難しいのである．なお，素因数分解を容易に (実行可能な程度で) 実行できるアルゴリズムが開発されたら，現代の暗号のほとんどは使い物にならなくなってしまう．

最後に教科書で紹介されていた定理を 2 つ紹介しておく．

定理 8.5 (オイラーの定理 (Euler's theorem))
関数 ϕ を以下で定義する (オイラー関数と呼ばれる)．

$$\phi(n) = |\{i \mid 1 \leq i < n,\ (n, i) = 1\}|$$

このとき，$(a, n) = 1$ ならば以下が成立.

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

証明 (概略のみ) 集合 $Z_p^{\times} = \{1, 2, \ldots, p-1\}$ を集合 $\{i \mid 1 \leq i < n,\ (n, i) = 1\}$ に置き換えることにより，定理 8.2 と同様な方法で証明できる． □

NOTE: 和算家の久留島義太 (よしひろ) はオイラーより先にオイラー関数を見つけていた．そのため，(日本の) 一部の文献ではオイラー関数を久留島-オイラー関数と呼んだりもする.

定理 8.6 (**ウィルソンの定理** (Wilson's Theorem)) 2 以上の任意の整数 p に対して

$$p \text{ が素数} \iff (p-1)! \equiv -1 \pmod{p}$$

証明

- p を素数とする．フェルマーの小定理より $1, 2, \ldots, p-1$ は合同方程式 $x^{p-1} - 1 \equiv 0 \pmod{p}$ の解．しかし，この合同式は法 p に関してその次数より多くの解を持つことはできない (教科書 135 頁の定理 3.11 参照)．また，教科書 134–135 頁の因数分解に関する議論をふまえて，

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

  p は素数なので，$p = 2$ または奇数であることを考えて，定数項を比較することにより

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

- p を合成数とする．$p = ab,\ 1 < a < b < p$ と分解できる場合は，$ab \mid (p-1)!$ なので，

  $$(p-1)! \equiv 0 \not\equiv -1 \pmod{p}$$

  $p = a^2,\ 2 < a$ と分解できるときも，$1 < a < 2a < p$ なので，同様の議論により $(p-1)! \not\equiv -1 \pmod{p}$ が示せる．最後に $p = 2^2 = 4$ のときは，$(p-1)! \equiv 6 \not\equiv -1 \pmod{4}$ となる． □

演習課題

問 8.1 p を奇素数 (奇数でかつ素数) とし a を $(a, p) = 1$ となる整数とする．このとき，

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

となることを示せ.
(ヒント：$(x-1)(x+1)$ が p の倍数ならば $(x-1)$ か $(x+1)$ のどちらかが p の倍数)