応用

フェルマーの小定理を利用したフェルマーテストの失敗確率を考える.

定理. カーマイケル数でない奇数の合成数 n.

$$a^{n-1} \equiv 1 \pmod{n} \qquad (*)$$

をみたす整数 $a \in \{1, 2, \ldots n-1\}$ の個数は $(n-1)/2$ 以下.

証明. $Z_n^* = \{i \in Z_n \mid \gcd(i, n) = 1\}$

（ただし $Z_n = \{0, 1, 2, \ldots, n-1\}$）とおき，演算 $\otimes_n$ を

$x \otimes_n y = xy$ を n で割った余り

と定義すると，$(Z_n^*, \otimes_n)$ が群になることはすでに確かめた.

なお，条件 $\gcd(i, n) = 1$ より $i \neq 0$ だから $Z_n^* \subseteq Z_n \setminus \{0\}$ であり，従って $|Z_n^*| \leq n-1$.

まず，整数 a $(1 \leq a < n)$ が $(*)$ をみたすならば $a \in Z_n^*$ であることを示す．a は $(*)$ をみたすから $a \cdot a^{n-2} \equiv 1 \pmod{n}$. よって合同方程式 $ax \equiv 1 \pmod{n}$ は解 a^{n-2} を持つ．従って，$\gcd(a, n) \mid 1$ だから $\gcd(a, n) = 1$. すなわち $a \in Z_n^*$ がいえた.

次に $(*)$ をみたす Z_n^* の要素すべての集合

$$B = \{b \in Z_n^* \mid b^{n-1} \equiv 1 \pmod{n}\}$$

を考える．$1 \in B$ だから $B \neq \emptyset$ であり，また明らかに有限集合.

さらに，$\forall x, y \in B,\ (xy)^{n-1} \equiv x^{n-1}y^{n-1} \equiv 1 \cdot 1 \equiv 1 \pmod{n}$ だから $x \otimes_n y \in B$. すなわち B は演算 $\otimes_n$ に関して閉じている; i.e., $(B, \otimes_n)$ は性質 (S0) をみたす．よって $(B, \otimes_n)$ は $(Z_n^*, \otimes_n)$ の部分群．n はカーマイケル数ではない合成数なので，

$\exists c \in Z_n^*,\ c^{n-1} \not\equiv 1 \pmod{n}$. すなわち $c \in Z_n^* \setminus B$ だから $B \neq Z_n^*$ (i.e., $(B, \otimes_n)$ は有限群 $(Z_n^*, \otimes_n)$ の真の部分群). よって，上述の

系より $|B| \leq |Z_n^*|/2 \leq (n-1)/2$. □

フェルマーテストは，$2 \leq a < n$ からランダムに選んだ整数 a に対して条件 $(*)$ および $\gcd(a, n) = 1$ のいずれかが成り立たなければ「n は合成数」と出力するものであった．以上の定理より，フェルマーテストがカーマイケル数でない合成数 n に対して $1/2$ 以上の確率で「n は合成数」と出力することが確認できた．