Fermat ちゃんと Euler 君

Articled by kymst. 20110720

Fermat's Theorem

Let p be a positive prime.
If $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof.
$A = \{1, 2, \ldots, p-1\}$ とすれば，A の要素の個数 $\sharp A = p - 1$. $i \in A$ について，ai を p で割った余りを r_i とすれば，

$$ai \equiv r_i \pmod{p}.$$

$f(i) = r_i$ とすれば，f は A から A への写像である．f が単射であることを示す．$\pmod{p}$ を fix する．$f(i) = f(j)$ とすれば $ai \equiv aj$ となり，$(a, p) = 1$ より $i \equiv j$ である．$i, j \in A$ より $i = j$. 確かに f は A から A 自身への単射であるが，A は有限集合だから，f は全単射になる．

そこで

$$\begin{aligned} a \cdot 1 &\equiv r_1, \\ a \cdot 2 &\equiv r_2, \\ &\vdots \\ a \cdot \overline{p-1} &\equiv r_{p-1} \end{aligned}$$

の辺々を乗じて

$$a^{p-1} \prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} r_i.$$

ところが，$1, 2, \ldots, p-1$ と $r_1, r_2, \ldots r_{p-1}$ は全体として一致するから

$$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} r_i$$

であり，p: prime であるから，この積は p と互いに素である．よって両辺これで割ることができて，

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

となり，証明された． ■

Fermat ちゃん
Fermat, Pierre de (1601-1665)

Euler's Theorem

Let m be a positive integer.
If $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof.
$A = \{k_1, k_2, \ldots, k_{\varphi(m)}\}$ とすれば，A の要素の個数 $\sharp A = \varphi(m)$. $k_i \in A$ について，ak_i を m で割った余りを r_i とすれば，

$$ak_1 \equiv r_i \pmod{m}.$$

$f(k_i) = r_i$ とすれば，f は A から A への写像である．f が単射であることを示す．$\pmod{m}$ を fix する．$f(k_i) = f(k_j)$ とすれば $ak_i \equiv ak_j$ となり，$(a, m) = 1$ より $k_i \equiv k_j$ である．$k_i, k_j \in A$ より $k_i = k_j$. 確かに f は A から A 自身への単射であるが，A は有限集合だから，f は全単射になる．

そこで

$$\begin{aligned} a \cdot k_1 &\equiv r_1, \\ a \cdot k_2 &\equiv r_2, \\ &\vdots \\ a \cdot k_{\varphi(m)} &\equiv r_{\varphi(m)} \end{aligned}$$

の辺々を乗じて

$$a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} k_i \equiv \prod_{i=1}^{\varphi(m)} r_i.$$

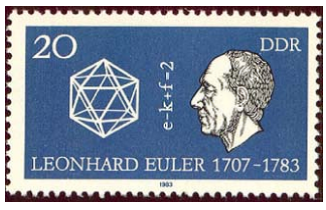
ところが，$k_1, k_2, \ldots, k_{\varphi(m)}$ と $r_1, r_2, \ldots r_{\varphi(m)}$ は全体として一致するから

$$\prod_{i=1}^{\varphi(m)} k_i = \prod_{i=1}^{\varphi(m)} r_i$$

であり，$(k_i, m) = 1$ であるから，この積は m と互いに素である．よって両辺これで割ることができて，

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

となり，証明された． ■



Euler くん
Euler, Leonhard (1707-1783)

The pdf version of this docu is DLable from http://kymst.net/mjk
Version 201207. Bug fixed: Tue Jul 17 11:12:03 2012.