**定理.** オイラーの規準 (Euler's criterion)

3以上の素数 $p$ と任意の $c \not\equiv 0 \pmod p$ について

$$\left(\frac{c}{p}\right) \equiv c^{\frac{p-1}{2}} \pmod p.$$

**証明.** $\forall a, c \in X = \{1, 2, \ldots, p-1\}$,

$$ab \equiv ba \equiv c \pmod p$$

をみたす $b \in X$ がただ1つ存在（$f_a$ は全単射だから）.

このようなペアで相異なるものの全てを $(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)$ と記す（対称的なので $a_i \le b_i$ を仮定）. すなわち,

$\forall i,\ a_i, b_i \in X$ かつ $a_i b_i \equiv c \pmod p$

$i \neq j \Rightarrow a_i \neq a_j$ (すると自動的に $b_i \neq b_j$ かつ $a_i \neq b_j$)

$\{a_1, \ldots, a_k, b_1, \ldots, b_k\} = X$.

#$a_i \neq b_j$ も自動的に成り立つ理由: $\exists i \neq j,\ a_i = b_j$ ならば $a_i b_i \equiv b_j b_i \equiv c$ となるが, $ab_j \equiv b_j a \equiv c$ をみたす $a$ の一意性より $b_i = a_j$. すると $a_i \le b_i = a_j \le b_j = a_i$ より $a_i = a_j$ となり矛盾.

- $c$ が $p$ を法として平方非剰余であるとき

  $\forall i,\ a_i \neq b_i$ なので, $a_1, \ldots, a_k, b_1, \ldots, b_k$ は全て相異なる.

  よってこれらの中に $X$ の各整数が丁度一度ずつ出現.

  このことから $k = |X|/2 = (p-1)/2$. また, $a_i b_i \equiv c$ の両辺を $i = 1, 2, \ldots, k$ について積をとると, 左辺は $a_1 b_1 \cdots a_k b_k = (p-1)!$, 右辺は $c^k$ なので, 結局 $(p-1)! \equiv c^{\frac{p-1}{2}}$.

- $c$ が $p$ を法として平方剰余であるとき

  $(*)$ の解を $\alpha\ (\in X)$, $-\alpha\ (\equiv p - \alpha)$ とする.

  $\alpha \not\equiv -\alpha$（$p$ は奇数なので $\alpha$ と $p - \alpha$ の偶奇は異なる）.



一般性を失うことなく $a_1 (= b_1) = \alpha$, $a_2 (= b_2) = p - \alpha$.

解はこれ以外に存在しないから $\forall i = 3, 4, \ldots, k$, $a_i \neq b_i$.

よって $a_1, a_2, a_3, \ldots, a_k, b_3, b_4 \ldots, b_k$ の中に $X$ の各整数が丁度一度ずつ出現.

従って $2k - 2 = |X|$ だから $k = (|X| + 2)/2 = (p+1)/2$.

$$a_1 a_2 = \alpha(p - \alpha) \equiv \alpha(-\alpha) \equiv -\alpha^2 \equiv -c \pmod p.$$

であるが, この式に $a_i b_i \equiv c \pmod p$ を $i = 3, 4, \ldots, k$ に対してかけあわせると, 左辺は

$$(a_1 a_2)(a_3 b_3 \cdots a_k b_k) = (p-1)!,$$

右辺は $-c \cdot c^{k-2} = -c^{\frac{p-1}{2}}$. よって

$$(p-1)! \equiv -c^{\frac{p-1}{2}} \pmod p. \qquad (**)$$

$c = 1$ ならば $(*)$ は解 $\pm 1$ を持つから, $(**)$ に代入して

$$(p-1)! \equiv -1 \pmod p. \qquad \square$$