東京大学
玉原国際セミナーハウス
2005 年 8 月 19 日

「フェルマーの小定理」についての問題

[1] 自然数 n にたいし、$\varphi(n) = 12$ が成り立つとする。

(1) $n = 2^e p^a q^b$ または $n = 2^e p^a$ ($p, q > 2$ は素数) とかけることを示せ。

(2) n は次のいずれかであることを示せ：$3 \cdot 7,\ 2 \cdot 3 \cdot 7,\ 2^2 \cdot 3^2,\ 2^2 \cdot 7,\ 13,\ 2 \cdot 13$

ヒント：$n = 2^e p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ を n の素因数分解とすると

$$\varphi(n) = 2^{e-1} p_1^{a_1-1} p_2^{a_2-1} \cdots p_r^{a_r-1} (p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

[2] フェルマーの定理を使って次の事実を示せ。
x を自然数として、素数 $p > 2$ が $x^2 + 1$ の約数なら $p \equiv 1 \mod 4$ である。

ヒント：仮定より $x^2 \equiv -1 \mod p$ である。これより $x^4 \equiv 1 \mod p$ となる。一方、$t = 1, 2, 3$ にたいしては、$x^t \not\equiv 1 \mod p$ である（なぜなら、たとえば $x \equiv 1 \mod p$ なら $x^2 \equiv 1 \mod p$ となり、$1 \equiv -1 \mod p$ となるが、$p > 2$ ならこれは矛盾である)。ここで、$p - 1$ を 4 で割った商を q、あまりを r $(0 \le r \le 3)$ とすれば、$p - 1 = 4q + r$ である。フェルマーの定理より、

$$(x^4)^q x^r = x^{p-1} \equiv 1 \mod p$$

が成り立つので、$x^4 \equiv 1 \mod p$ とあわせて $x^r \equiv 1 \mod p$ が従う。よって先に注意したことから $r = 0$ でなくてはならない。

[3] [2] を使って次の事実を示せ。
$p \equiv 1 \mod 4$ を満たす素数 p が無限個存在する。

ヒント：背理法により示す。$p \equiv 1 \mod 4$ を満たす素数が有限個しか存在しないと仮定して、それらを $p_1,\ p_2,\ \ldots, p_r$ とする。$x = (2p_1 p_2 \cdots p_r)^2 + 1$ とおき、q を a の素因子とする。[2] より $q \equiv 1 \mod 4$ が成り立つ。さらに、a が $p_1,\ p_2,\ \ldots, p_r$ で割れないことを示し、よって q はこれらのいずれとも異なるので、$p_1,\ p_2,\ \ldots, p_r$ のとり方に矛盾する。