数チャレ 第109回(2010年2月)

奇数 m について，$a^2 \equiv 2 \pmod{m}$ を満たす整数 a が存在するならば，

$$m \equiv \pm 1 \pmod{8}$$

であることを m についての数学的帰納法で示せ。

解答

$m = 1$ のとき題意は成り立ち，$m = 3$ のとき題意は成り立たない。

$$a^2 = 2 + bm \qquad \cdots\cdots (*)$$

を満たす整数 $a,\ b$ が存在するような奇数 m について，m より小さい奇数はすべて題意を満たすものとする。

$$(a-m)^2 \equiv a^2 \pmod{m}, \quad a - m \not\equiv a \pmod{2}$$

であるから，

$$a \text{ は奇数}, \ 3 \leqq a < m$$

として一般性を失わない。このとき b も奇数であり，$0 < b < m$ である。

b の任意の素因数(奇素数)を q とすると，$(*)$より

$$a^2 \equiv 2 \pmod{q}$$

であり，$q < m$ より

$$q \equiv \pm 1 \pmod{8}$$

が成り立つ。したがって，それらの積についても

$$b \equiv \pm 1 \pmod{8}$$

が成り立つ。a は奇数で $a^2 \equiv 1 \pmod{8}$ であるから，$(*)$より

$$1 \equiv 2 \pm m \pmod{8}$$

であるが，これを満たすには $m \equiv \pm 1 \pmod{8}$ の場合に限られ，2が平方剰余となるすべての奇数 m について成り立つ。 (証明おわり)

© 早稲田数学フォーラム