数チャレ 第11回(2001年12月)

pを素数とするとき，次の定理を証明せよ。

(1) pで割り切れない任意の整数aに対して，

$$ax \equiv y \pmod{p},\quad 1 \leqq x < \sqrt{p},\quad 1 \leqq |y| < \sqrt{p}$$

を満たす整数$x,\ y$が存在する。

(2) $a^2+1 \equiv 0 \pmod{p}$を満たす整数aが存在するならば，

$$p = x^2 + y^2$$

を満たす整数$x,\ y$が存在する。

解答

(1) $\sqrt{p}$の整数部分($\sqrt{p}$を越えない最大整数)をnとおくと，

$$n < \sqrt{p} < n+1$$

いま，$x,\ y$をそれぞれ$0,\ 1,\ 2,\ \cdots,\ n$の中から選んで

$$ax - y \quad \big(x,\ y \in \{0,\ 1,\ 2,\ \cdots,\ n\}\big)$$

を考えると，その個数は$(n+1)^2$でpより大きいから，

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p},\quad (x_1,\ y_1) \neq (x_2,\ y_2)$$

を満たす0以上n以下の整数$x_1,\ y_1,\ x_2,\ y_2$が存在する。このとき

$$a(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}$$

となるから，結局

$$x_1 \not\equiv x_2 \pmod{p} \text{ かつ } y_1 \not\equiv y_2 \pmod{p}$$

が成り立つ。

必要ならばx_1とx_2を入れかえて$x = x_1 - x_2 > 0$としてよいから，

$$1 \leqq x = x_1 - x_2 \leqq n < \sqrt{p}$$

であり，さらに$y = y_1 - y_2$とおくと，

$$1 \leqq |y| = |y_1 - y_2| \leqq n < \sqrt{p},\quad ax \equiv y \pmod{p}$$

(おわり)

(2) $a^2+1 \equiv 0 \pmod{p}$を満たす整数aに対して，(1)で定まる整数$x,\ y$を用いると，

$$x^2 + y^2 \equiv x^2 + a^2x^2 \equiv (1+a^2)x^2 \equiv 0 \pmod{p}$$

$1 \leqq x^2 < p,\ 1 \leqq y^2 < p$より$2 \leqq x^2 + y^2 < 2p$であるから，

$$p = x^2 + y^2$$

(おわり)

(注) Wilsonの定理より

$$p\text{が素数} \iff (p-1)! \equiv -1 \pmod{p}$$

であるから，素数pが$p = 4m+1$(mは自然数)と表されるならば，

$$\begin{aligned}(p-1)! = (4m)! &= (2m)! \times (p-2m)(p-2m+1)\cdots(p-1)\\ &\equiv (2m)! \times (2m)! \pmod{p}\end{aligned}$$

となって，$a = (2m)!$は(2)の仮定を満たす。

(1)はThueの剰余定理と呼ばれている。