数チャレ 第６回（2001年７月）

(1)　$a,\ b$を互いに素な自然数とするとき，

$$ax+by=1$$

を満たす整数$x,\ y$が存在することを証明せよ。

(2)　2以上の整数pに対して，

$$p\text{が素数} \iff (p-1)!+1\text{が}p\text{で割り切れる}$$

を証明せよ。

解答

(1)　$by=1-ax$を満たす整数$x,\ y$を見つけるために，b個の整数

$$1-a,\ 1-2a,\ \cdots\cdots,\ 1-ba$$

を考える。ここから，任意の2つの数$1-am,\ 1-an\ (1\leqq m<n\leqq b)$を選ぶとき，$0<n-m\leqq b-1<b$および$a$と$b$は互いに素であることより，

$$(1-am)-(1-an)=a(n-m)$$

はbで割り切れない。したがって，上のb個の整数はbで割った余りがすべて異なり，1つだけはbの倍数である。そのbの倍数を$1-ax$（xは整数）とすると，

$$by=1-ax\ \text{すなわち}\ ax+by=1$$

を満たすyも整数である。

（おわり）

（別証明）aとbが互いに素な整数であるとき，集合

$$S=\{ax+by\,|\,x,\ y\text{は整数}\}$$

が整数全体の集合Zと一致することを示せばよい。

$ax_1+by_1,\ ax_2+by_2\in S$に対して

$$(ax_1+by_1)\pm(ax_2+by_2)=a(x_1\pm x_2)+b(y_1\pm y_2)\in S$$

であるから，Sは和と差について閉じている。また，$ax+by\in S,\ k\in Z$に対して

$$k(ax+by)=a(kx)+b(ky)\in S$$

であるから，Sは整数倍について閉じている。

いま，dをSに属する正の最小数とする。任意の$n\in S$に対して

$$n=dq+r,\quad 0\leqq r<d\quad (q,\ r\text{は整数})$$

と表されるが，上に述べたSの性質より

$$r=n-dq\in S$$

dの最小性より

$$r=0,\quad n=dq$$

したがって，SはSに属する正の最小整数dの倍数の集合である。

$$a=a\times1+b\times0\in S,\quad b=a\times0+b\times1\in S$$

であるから，$a,\ b$はともにdの倍数，すなわちdはaとbの公約数である。ところが，aとbは互いに素であるから$d=1$となり，

$$S=\{\,d=1\text{の倍数}\}=Z$$

（おわり）

(2) $\Longrightarrow$: pが奇素数のとき,

$$k \in \{1,\ 2,\ \cdots\cdots,\ p-1\}$$

に対してkとpは互いに素であるから，(1)より

$$kx_k + py_k = 1$$

を満たす整数x_k，y_kが存在する。任意の整数mに対して

$$kx_k + py_k = k(x_k + mp) + p(y_k - mk)$$

であるから，適当にy_kを調節することにより

$$x_k \in \{1,\ 2,\ \cdots\cdots,\ p-1\}$$

であるとしてよい。

ここで,

$$kx_k + py_k = kx_k{}' + py_k{}' \quad (x_k,\ x_k{}' \in \{1,\ 2,\ \cdots,\ p-1\},\ \ y_k,\ y_k{}'\text{は整数})$$

とすると$k(x_k - x_k{}') = p(y_k{}' - y_k)$は$p$で割り切れ，$k$と$p$は互いに素であるから

$$x_k - x_k{}'\text{は}p\text{の倍数}$$

ところが，$|x_k - x_k{}'| \leqq (p-1) - 1 < p$であるから,

$$x_k = x_k{}'$$

したがって，kに対してx_kは$\{1,\ 2,\ \cdots,\ p-1\}$において一意に定まる。

(i) $k = x_k$のとき

$$kx_k - 1 = k^2 - 1 = (k+1)(k-1)$$

はpの倍数であるから，$1 \leqq k \leqq p-1$では

$$k = 1 \text{ または } k = p-1$$

(ii) $k \neq 1,\ p-1$のとき

$k \neq x_k$であり，kとx_kの$\dfrac{p-3}{2}$組で2以上$p-2$以下のすべての整数をとり尽くすことができる。その$\dfrac{p-3}{2}$組を

$$k^{(1)},\ x_k{}^{(1)},\ k^{(2)},\ x_k{}^{(2)},\ \cdots\cdots,\ k^{(\frac{p-3}{2})},\ x_k{}^{(\frac{p-3}{2})}$$

とすると,

$$k^{(i)}x_k{}^{(i)} = 1 - py_k{}^{(i)} \quad \left(y_k{}^{(i)}\text{は整数},\ i = 1,\ 2,\ \cdots,\ \frac{p-3}{2}\right)$$

と表されて,

$$(p-2)! = \prod_{i=1}^{\frac{p-3}{2}} (1 - py_k{}^{(i)}) = 1 + (p\text{の倍数})$$

(i), (ii)より

$$(p-1)! = (p-2)! \times (p-1) = (p\text{の倍数}) - 1$$

$p = 2$のときは，$(p-1)! + 1 = 2$であるから成り立つ。

$\Longleftarrow$: $(p-1)! + 1$がpの倍数ならば，$(p-1)!$はpと互いに素である。したがって，1以上$p-1$以下のすべての整数がpと互いに素であるから，pは素数である。

(おわり)

(注) (2)を「ウィルソンの定理」という。