問題１０

p と q を素数とし、$p \neq q$ とすると、どのような負でない２つの整数 m と n をもちいても $x = pm + qn$ とは表すことができない正の整数 x は有限個である。これを証明せよ。

［(類）大阪大学（2000）前期理系第３問（$p = 3, q = 5$)］
［(類）甲陽学院中学校（1997）第２日第３問（$p = 3, q = 5$)］

（解答例１）$p < q$ とし、q を p で割ったときの余りを r とすると、

$$0 < r < p$$

である。まず、

$$r,\ 2r,\ 3r,\ \ldots,\ (p-1)r$$

のそれぞれを p で割ったときの余りはすべて異なることを示す。

実際、$0 < i < j < p$ とし、ir を p で割ったときの余りと jr を p で割ったときの余りが一致すれば、$(j-i)r$ は p で割り切れる。しかし、p が素数であることと、

$$0 < j - i < p,\ \ 0 < r < p$$

から、$j - i$ も r も p で割り切れないから、$(j-i)r$ は p で割り切れない。

すると、ir を p で割ったときの余りを a_i とすると、$a_1, a_2, \ldots, a_{p-1}$ を適当に並べ替えると、$1, 2, \ldots, p-1$ となる。これより

$$0,\ q,\ 2q,\ 3q,\ \ldots,\ (p-1)q$$

のそれぞれを p で割ったときの余りはすべて異なり、しかも、それら p 個の余りを適当に並べ替えると $0, 1, 2, \ldots, p-1$ となる。

いま、正の整数 $x \geq (p-1)q$ を p で割ったときの余りを s とし、iq を p で割ったときの余りが s となるような $0 \leq i < p$ を選ぶと、$x - iq$ は p で割り切れるから、$x - iq = kp$ とすると、$k \geq 0, x = kp + iq$ となる。

以上から、正の整数 $x \geq (p-1)q$ は $x = pm + qn$ と表すことができる。■

（解答例２）p と q は互いに素であるから、

$$a'p + b'q = 1$$

となる整数 a' と b' が存在する。いま、$a' > 0, b' < 0$ とし、$a = a', b = -b'$ とする。すると、$ap - bq = 1$ であるから、

$$ap - 1 = bq$$

である。負でない 2 つの整数 m と n をもちいて $x = pm + qn$ と表すことができる正の整数 x の全体の集合を A とする。いま、$0 \leq i \leq p-1$ とすると

$$(p-1)ap - i = i(ap-1) + ((p-1)-i)ap \in A$$

である。$c = (p-1)ap \geq p$ とすると、連続する p 個の正の整数

$$c,\, c-1,\, c-2,\, \ldots,\, c-(p-1)$$

は A に属する。

以上から、正の整数 $x \geq c-(p-1)$ は A に属する。■