p，q を互いに素な正整数とする。

(1)　任意の整数 x に対して，p 個の整数

$$x-q,\ x-2q,\ \cdots,\ x-pq$$

を p で割った余りは全て相異なることを証明せよ。

(2)　$x>pq$ なる任意の整数 x は，適当な正整数 a，b を用いて

$$x=pa+qb$$

と表せることを証明せよ。

＜ '08 奈良県立医科大 ＞

【戦略】

(1)　**例題の参考で見た【ベズーの補題】の証明中に出てきた**

q，$2q$，$3q$，$\cdots$，$(p-1)q$ **を p で割った余りは全て異なる**

ということの証明と同様の手法を用います。

つまり，$x-iq\equiv x-jq \pmod p$ となる i，j $(1\leqq i<j\leqq p)$ が存在すると仮定します。

(2)　**(1) により，**

$$x-q,\ x-2p,\ \cdots,\ x-pq$$

という p 個の正の整数は p を法として

$$0,\ 1,\ 2,\ \cdots,\ p-1$$

という p 個の整数と 1 対 1 対応します。

つまり，$x-bq\equiv 0 \pmod p$ となるような b の存在が保証されます。

条件から $x-q$，$x-2q$，$x-bq$，$\cdots$，$x-pq$ は正の整数です。

よって，$x-bq$ という正の整数を p という整数で割った商も当然正ということになります。

したがって，$x-bq=pa$ という正の整数 a の存在が保証されます。

すなわち $x=pa+qb$ となるような正整数 a，b の存在が保証されたことになり証明完了です。

【解答】

(1)　$x-iq\equiv x-jq \pmod p$ となるような i，j $(1\leqq i<j\leqq p)$ が存在すると仮定する。

このとき，$(j-i)q\equiv 0 \pmod p$ を得る。

ゆえに，$(j-i)q$ は p の倍数となる。

p，q は互いに素であるため，$j-i$ が p の倍数となるしかない。

$1\leqq i<j\leqq p$ より，j，i の幅である $j-i$ は $p-1$ 以下の p の倍数ということになる。

ゆえに，$j-i=0$ となってしまい，i，j が異なることに矛盾する。

以上から，$x-q$，$x-2q$，$\cdots$，$x-pq$ を p で割った余りは全て異なる。

(2)　(1) より，$x-q$，$x-2q$，$\cdots$，$x-pq$ という p 個の整数を p で割った余りは 0，1，2，$\cdots$，$p-1$ という p 個の整数と 1 対 1 対応する。

ゆえに，$x-bq\equiv 0 \pmod p$ となるような正の整数 b が存在する。

今，条件から $x>pq$ であるため，

$$x-q,\ x-2q,\ \cdots,\ x-bq,\ \cdots,\ x-pq$$

は全て正の整数である。

正の整数 $x-bq$ を正の整数 p で割った商も正であるため

$$x-bq=pa$$

となるような正の整数 a が存在することになる。

以上から，$x=ap+qb$（a，b は正の整数）という形で表すことができることが示された。

【総括】

大阪大学の問題を少し一般化したような問題です。

非負整数ではないものの，正の整数で「確実に」表現できるということを保証できたわけです。

もし，表現できないものを探せと言われた場合，1，2，$\cdots$，$pq-1$ という有限の範囲で考えればよいということになります。

そう考えると，本問の結果はそれなりに価値があると言えましょう。