<table>
<thead>
<tr>
<th>Title</th>
<th>A Further Note on the Generalized Josephus Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal</td>
<td>Tsukuba journal of mathematics</td>
</tr>
<tr>
<td>Volume</td>
<td>31</td>
</tr>
<tr>
<td>Number</td>
<td>2</td>
</tr>
<tr>
<td>Page Range</td>
<td>253-259</td>
</tr>
<tr>
<td>Year</td>
<td>2007</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2241/00143966">http://hdl.handle.net/2241/00143966</a></td>
</tr>
</tbody>
</table>
A FURTHER NOTE ON THE GENERALIZED JOSEPHUS PROBLEM

By
Saburô UCHIYAMA

1. In our previous papers [1] and [2] we have observed several interesting and significant aspects of the generalized Josephus problem. In the present article we shall again concern ourselves with this problem. Thus, given a total number \( n \geq 1 \) and certain \( n \) objects numbered from 1 to \( n \), and another integer \( m \geq 1 \), called the reduction coefficient, we arrange these \( n \) objects in a circle and, starting with the object numbered 1, and counting each object in turn around the circle, we eliminate every \( m \)th object until all of them are removed. By \( a_m(k,n) \) \((1 \leq k \leq n)\) we denote as before the \( k \)th Josephus number, that is, the object number to be removed in the \( k \)th step of elimination. It is evident that we have

\[
1 \leq a_m(k,n) \leq n
\]

and

\[
a_m(1,n) \equiv m \pmod{n},
\]

and that

\[
a_m(k+1,n+1) \equiv a_m(1,n+1) + a_m(k,n) \pmod{n+1},
\]

from which follows at once

\[
a_m(k+1,n+1) \equiv m + a_m(k,n) \pmod{n+1}
\]

in view of (2); (3) is the fundamental relation due to P. G. Tait for the Josephus numbers \( a_m(k,n) \) (cf. [1; §§1–2]). In effect, the Josephus numbers \( a_m(k,n) \) \((1 \leq k \leq n)\) are completely determined by the conditions (1), (2) and (3).

In what follows we devote ourselves to the study of the special case of \( k = n \) and write for simplicity’s sake \( d_m(n) = a_m(n,n) \) as in [1]. We have then \( d_m(1) = 1 \) for any \( m \geq 1 \), and the fundamental relation (3) becomes

\[
d_m(n+1) \equiv m + d_m(n) \pmod{n+1}.
\]

Received March 9, 2006.
Now, in connexion with his study of a Japanese version of the Josephus problem, Seki Takakazu (1642?–1708) called any positive integer \( n \) for which one has
\[
d_m(n + 1) = 1,
\]
if it exists, a limitative number with respect to the reduction coefficient \( m \); compare [1; § 8]. We have formulated there a hypothesis on the infinitude of limitative numbers \( n \) for every fixed \( m \geq 2 \), regarding it as an implicit intention of Seki’s. The validity of this hypothesis is easy to prove for \( m = 2 \) and 3, but for \( m \geq 4 \) it appears to be difficult to settle it. At present we are able only to show that there are infinitely many integers \( n \) satisfying the condition
\[
1 \leq d_m(n + 1) \leq m - 1
\]
for every fixed reduction coefficient \( m \geq 2 \) (cf. [2; § 3]). In this respect it will be of some interest to note that the set of positive integers \( m \) for which exist only a bounded number of integers \( n \) satisfying \( d_m(n + 1) = 1 \) has natural density 0; in other words, there are unboundedly many limitative numbers \( n \) for almost all, so to say, values of the reduction coefficient \( m \) (\( \geq 4 \)) (see § 3 below).

In the present note we wish to provide a proof for this metric result as an approach to the original hypothesis mentioned above.

**Note.** Let \( S \) be a set of positive integers \( m \). The upper asymptotic density \( \tilde{\delta}(S) \) of the set \( S \) is defined by
\[
\tilde{\delta}(S) = \limsup_{X \to \infty} \frac{1}{X} \sum_{m \in S, m \leq X} 1
\]
and the lower asymptotic density \( \hat{\delta}(S) \) of \( S \) is with \( \liminf \) in place of \( \limsup \); we always have \( \tilde{\delta}(S) \geq \hat{\delta}(S) \) and, in case the upper and lower asymptotic densities coincide with each other, say \( \tilde{\delta}(S) = \delta = \hat{\delta}(S) \), the common value \( \delta = \delta(S) \) is the natural density of the set \( S \). If in particular \( \tilde{\delta}(S) = 0 \) then we have naturally \( \delta(S) = 0 \).

2. Let \( n, p \) and \( q \) be given positive integers \( > 1 \). We denote by \( H(n) \) the set of positive integers \( m \) for which one has \( d_m(n) = 1 \) and by \( H(p, q) \) the set of positive integers \( m \) such that \( d_m(p) = d_m(q) = 1 \). If \( p = q \) then \( H(p, q) = H(p, p) = H(p) \).

We set \( M_1 = 1 \) and for \( n > 1 \)
\[
M_n := \text{L.C.M.}(1, 2, \ldots, n).
\]
Lemma 1. For any \(1 \leq \ell \leq n\) the number \(Z(n; \ell)\) of integers \(m\) \((1 \leq m \leq M_n)\) satisfying the condition \(d_m(n) = \ell\) is given by

\[Z(n; \ell) = \frac{M_n}{n},\]

so that, in particular, the natural density \(\delta(H(n))\) exists and equals \(1/n\).

This is the special case \(k = n\) of Proposition 3 in [2].

Lemma 2. Suppose that \(p\) and \(q\) be prime numbers, \(p < q\). Then, for any \(\ell_p\) \((1 \leq \ell_p \leq p)\) and any \(\ell_q\) \((1 \leq \ell_q \leq q)\) the number \(Z(p, q; \ell_p, \ell_q)\) of integers \(m\) \((1 \leq m \leq M_q)\) fulfilling the conditions \(d_m(p) = \ell_p\) and \(d_m(q) = \ell_q\) is given by

\[Z(p, q; \ell_p, \ell_q) = \frac{M_q}{pq},\]

so that, in particular, the natural density \(\delta(H(p, q))\) exists and is equal to \(1/(pq)\).

Proof. Consider the system of \(q\) congruences in \(m\) (cf. (4)):

\[m \equiv h_i - h_{i-1} \pmod{i} \quad (i = 1, 2, \ldots, q),\]

where \(h_0 = 0\) and the \(h_i\) \((1 \leq i \leq q)\) are parameters taking some integer values such that

\[1 \leq h_i \leq i \quad (1 \leq i \leq q);\]

thus, \(h_1 = 1\) and the first congruence in the system (5) is absurd, so that we shall actually deal with (5) only for \(2 \leq i \leq q\).

We fix \(h_1 = 1, h_p = \ell_p\) and \(h_q = \ell_q\). For an arbitrary integer \(j\) \((2 \leq j \leq q)\) we contemplate the subsystem of (5):

\[m \equiv h_i - h_{i-1} \pmod{i} \quad (i = 2, \ldots, j).\]

The system of congruences (6) may admit a solution

\[m \equiv m_j \pmod{M_j}\]

under certain conditions, in general, to be imposed on the integers \(h_i\). Anyway there may be several, mutually incongruent solutions \(m_j \pmod{M_j}\) of (6), where \(m_j = m_j(h_1, h_2, \ldots, h_j)\) depends on the ordered \(j\)-tuple of integers \((h_1, h_2, \ldots, h_j)\),
and it is readily seen that if moreover \((h'_1, h'_2, \ldots, h'_j)\) is such a \(j\)-tuple different from \((h_1, h_2, \ldots, h_j)\), then we have

\[ m_j(h'_1, h'_2, \ldots, h'_j) \neq m_j(h_1, h_2, \ldots, h_j) \pmod{M_j}. \]

For \(j = 2\) we have plainly with \(1 \leq h_2 \leq 2\)

\[ m_2 = m_2(h_1, h_2) \equiv h_2 - h_1 = h_2 - 1 \pmod{M_2}. \]

For \(j \geq 3\) the solvability condition for the system

\[
\begin{align*}
  m &\equiv m_{j-1} \pmod{M_{j-1}} \\
  m &\equiv h_j - h_{j-1} \pmod{j},
\end{align*}
\]

which is equivalent to (6), is provided by

\[
m_{j-1} \equiv h_j - h_{j-1} \pmod{d_j},
\]

where

\[ d_i = \text{G.C.D.}(M_{i-1}, i) \quad (i \geq 2). \]

Having determined \(m_{j-1}\) modulo \(M_{j-1}\) with \((h_1, \ldots, h_{j-1})\), we fix \(h_j\) to the modulus \(d_j\) by \((h_1, \ldots, h_{j-1})\) according to the congruence (8), so that the number of possible choices for the value of \(h_j\) turns out to be equal primarily to \(j/d_j\).

Setting \(Z_1 = M_1 = 1\), we denote by \(Z_j\) for \(2 \leq j \leq q\) the number of different (i.e. incongruent) solutions \(m_j \pmod{M_j}\) of the system (6), or of the system (7). Clearly \(Z_q = Z(p, q; \ell_p, \ell_q)\).

If \(2 \leq j < p\) then we have

\[ Z_j = Z_{j-1} \frac{j}{d_j} = M_j. \]

For \(j = p\), a prime, we have \(d_p = 1\) and may arbitrarily fix the integer \(h_p = \ell_p\) with \(1 \leq \ell_p \leq p\), so that

\[ Z_p = Z_{p-1} \cdot 1 = M_{p-1} = \frac{M_p}{p}; \]

for \(p + 1 \leq j \leq q\) we find, as above, that

\[ Z_j = Z_{j-1} \frac{j}{d_j} = \frac{M_j}{p}, \]

and finally for \(j = q\), a prime different from \(p\), we have again \(d_q = 1\) and, therefore, with \(h_q = \ell_q, 1 \leq \ell_q \leq q\),
\[ Z_q = Z_{q-1} \cdot 1 = \frac{M_q - 1}{p} = \frac{M_q}{pq}, \]

which was to be proved.

Needless to add, our Lemma 2 can naturally be extended to the case in which three or more distinct primes are involved. Given an arbitrary finite set \( P \) of prime numbers \( p \) and a set \( \{\ell_p\} \) of prescribed integers \( \ell_p \) with \( 1 \leq \ell_p \leq p \) \( (p \in P) \), the number \( Z(P; \{\ell_p\}) \) of integers \( m \) \( (1 \leq m \leq M_s) \) such that we have

\[ d_m(p) = \ell_p \quad \text{for all} \quad p \in P \]

is found to be equal to \( M_s / D \), where \( s \) is any integer not less than the maximal prime of the set \( P \) and \( D \) is the product of all primes \( p \in P \).

3. We are now in a position to enunciate and establish our principal result about the hypothesis of Seki, as mentioned in §1 above. We shall prove the following

**Theorem.** For all values of the reduction coefficient \( m \) \( (>1) \), except possibly for a set of integers \( m \) of natural density 0, there exist unboundedly many positive integers \( n \) satisfying the condition \( d_m(n) = 1 \).

**Proof.** Let \( A_0 \) (resp. \( A_0(v) \), \( v \) being a natural number) the set of positive integers \( m \) such that there are only a bounded number (resp. at most \( v \) in number) of integers \( n \) satisfying \( d_m(n) = 1 \). We have to show that \( \delta(A_0) = 0 \); this can be achieved, if we prove that \( \delta(A_0(v)) = 0 \) however large the bound \( v \) \( (<+\infty) \) may be, since we have \( A_0(v) \subseteq A_0(v') \) if \( v < v' \) so that

\[ A_0 = \bigcup_{1 \leq v < +\infty} A_0(v) \quad \text{and} \quad \delta(A_0) = \sup_{1 \leq v < +\infty} \delta(A_0(v)) = 0. \]

We define for a fixed positive integer \( n \)

\[ c_m(n) = \begin{cases} 1 & \text{if} \ d_m(n) = 1, \\ 0 & \text{otherwise}; \end{cases} \]

this is the characteristic function of the set \( H(n) \) of integers \( m \) for which holds \( d_m(n) = 1 \). Denoting by \( p \) and \( q \) generic primes, we have, in virtue of Lemmas 1 and 2,

\[ \delta(H(p)) = \frac{1}{M_s} \sum_{m=1}^{M_s} c_m(p) = \frac{1}{p} \quad \text{if} \quad p \leq s \]
and

\[
\delta(H(p,q)) = \frac{1}{M} \sum_{m=1}^{M} c_m(p)c_m(q) = \begin{cases} 
\frac{1}{pq} & \text{if } p \neq q, \ p, q \leq s, \\
\frac{1}{p} & \text{if } p = q \leq s.
\end{cases}
\]

We now calculate, with a positive real number \(Q\), the dispersion

\[
V(Q) := \lim_{X \to \infty} \frac{1}{X} \sum_{m \leq X} \left( \sum_{p \leq Q} \left( c_m(p) - \frac{1}{p} \right) \right)^2,
\]

where \(\sum_{p \leq Q}\) indicates the summation over the prime numbers \(p \leq Q\).

Let \(s\) be any integer not less than the largest prime \(\leq Q\). Then it follows from (9) and (10) that

\[
V(Q) = \frac{1}{M} \sum_{m=1}^{M} \left( \sum_{p \leq Q} \left( c_m(p) - \frac{1}{p} \right) \right)^2 = \sum_{p \leq Q} \frac{1}{p} \left( 1 - \frac{1}{p} \right),
\]

which ensures the existence of the limit on the right-hand side of (11).

For any natural number \(v\) let us denote by \(A(v)\) the set of positive integers \(m\) for which we have \(d_m(p) = 1\) for at most \(v\) primes \(p\) in number.

Writing for the sake of brevity

\[
S(Q) := \sum_{p \leq Q} \frac{1}{p},
\]

we have for every \(m \in A(v)\)

\[
\left| \sum_{p \leq Q} \left( c_m(p) - \frac{1}{p} \right) \right| \geq S(Q) - v.
\]

Consequently, however large the bound \(v \ (< +\infty)\) may be, we may choose \(Q\) so large as to satisfy \(S(Q) > 2v\), which is certainly possible, since \(S(Q)\) tends to infinity with \(Q\), as is seen from the well-known inequality

\[
S(Q) > \log \log Q - \frac{1}{2} \quad (Q > 2),
\]

and we find, by (11),
\[ V(Q) \geq \limsup_{X \to \infty} \frac{1}{X} \sum_{m \leq X \atop m \in A(v)} \left( \sum_{p \leq Q} \left( c_m(p) - \frac{1}{p} \right) \right)^2 \geq \left( \frac{1}{2} S(Q) \right)^2 \limsup_{X \to \infty} \frac{1}{X} \sum_{m \leq X \atop m \in A(v)} 1 = \frac{1}{4} (S(Q))^2 \tilde{d}(A(v)). \]

We have \( V(Q) < S(Q) \) in view of (12), so that
\[
\tilde{d}(A(v)) \leq \frac{V(Q)}{\left( S(Q) \right)^2} < \frac{4}{S(Q)},
\]
and we may conclude that \( \tilde{d}(A(v)) = 0 \), on letting \( Q \to +\infty \). We thus have \( \delta(A(v)) = 0 \) for all \( v < +\infty \) and so \( \delta(A_0) = 0 \), as was noticed above.

This completes our proof of the theorem.

Note that we have actually demonstrated that for almost all values of \( m > 1 \) there are indefinitely many primes \( p \) satisfying \( d_m(p) = 1 \); here, that the qualifier ‘almost’ cannot be omitted is clear, as we recall the fact that for \( m = 2 \) the integers \( n \) for which holds \( d_2(n) = 1 \) are exclusively the powers of 2 (cf. [1; §8]).

**Remark.** We note also that if the (upper or lower) asymptotic density were a completely additive probability measure over the subsets of the set of positive integers \( m \), then, in our proof of the theorem, we could have directly appealed to the Borel-Cantelli lemma in probability theory; the density is not a completely additive measure, however.

**References**


Saburô Uchiyama
Prof. Emer.
University of Tsukuba
(Institute of Mathematics) and
Okayama University