A. Zulauf

On the number of representations of an integer as a sum of primes belonging to given arithmetical progressions


<http://www.numdam.org/item?id=CM_1962-1964__15__64_0>
On the Number of Representations of an Integer as a Sum of Primes belonging to given Arithmetical Progressions

by

A. Zulauf

1. Introduction: Let \( K_1, \ldots, K_s \) be \( s \) given positive integers, and \( K \) their least common multiple. Let further \( a_1, \ldots, a_s \) be given integers, \( (a_\sigma, K_\sigma) = 1 \) \( (\sigma = 1, \ldots, s) \), and denote by \( \kappa(n) \) the number of sets of residues \( x_1, \ldots, x_s \) \( (\text{mod} \ K) \) which (i) are relatively prime to \( K \), and (ii) satisfy the following system of congruences.

\[
\begin{align*}
  x_\sigma &\equiv a_\sigma \pmod{K_\sigma} \quad (\sigma = 1, \ldots, s), \\
  \sum_{\sigma=1}^s x_\sigma &\equiv n \pmod{K}.
\end{align*}
\]

Finally let \( N(n) \) denote the number of representations of the positive integer \( n \) in the form

\[
(1) \quad n = p_1 + p_2 + \ldots + p_s, \quad p_\sigma \equiv a_\sigma \pmod{K_\sigma} \quad (\sigma = 1, \ldots, s)
\]

where the \( p_\sigma \) are odd prime numbers.

I have proved \(^1\) that if \( n \equiv s \pmod{2} \), and \( s > 2 \), then

\[
(2) \quad N(n) = \kappa(n) \frac{1}{\varphi^s(K)(s-1)!} \frac{n^{s-1}}{\log^s n} \mathcal{G}^*(n) + O \left( \frac{n^{s-1} \log \log n}{\log^{s+1} n} \right),
\]

where \( \varphi \) denotes Euler's function,

\[
\mathcal{G}^*(n) = \Omega K \prod_{p \nmid nK} \left( 1 - \left[ \frac{-1}{p-1} \right]^s \right) \times \prod_{p \nmid n} \left( 1 - \left[ \frac{-1}{p-1} \right]^{s-1} \right),
\]

where \( p \) runs through the odd prime numbers, and where \( \Omega = 1 \), or \( = 2 \), according as \( K \) is even, or odd.

In this paper we shall prove an explicit formula for \( \kappa(n) \).

2. Lemma: Let \( p \) be a prime number \( \geq 2 \), let \( s \geq 1 \), \( 1 \leq l \leq L \), and let \( \mathcal{N}_p(s, l, L; n) \) denote the number of sets of residues \( x_1, \ldots, x_s \) \( (\text{mod} \ p^L) \) which satisfy simultaneously

\(^1\) see [1], p. 228.

\(^*\) If \( s = 2 \) this results holds for “almost all” \( n \). See [3] and [4].
Then
\[ \kappa_p(s, l, L; n) = \begin{cases} p^{t(t-1)}(p-1) \{ (p-1)^t - (-1)^t \} & \text{if } p | n \\ p^{t(t-1)} \{ (p-1)^t - (-1)^t \} & \text{if } p \nmid n. \end{cases} \]

**Proof.** The lemma is evidently true for \( s = 1 \), since the system
\[ \{(x_1, p) = 1; \ x_1 \equiv n \pmod{p^t}\} \]
has \( p^{t-1} \), or no, solutions \( x_1 \pmod{p^t} \) according as \( p | n \) or \( p \nmid n \). Next, assuming the lemma true for \( s = t \), we shall prove that it is also true for \( s = t+1 \).

The system
\[ \{(x_{t+1}, p) = 1; \ x_{t+1} \equiv n - \sum_{\sigma=1}^{t} x_\sigma \pmod{p^t}\} \]
has \( p^{t-1} \), or no, solutions \( x_{t+1} \pmod{p^t} \) according as
\[ \sum_{\sigma=1}^{t} x_\sigma \not\equiv n \pmod{p}, \]
or not. Thus
\[ (3) \quad \kappa_p(t+1, l, L; n) = p^{t-1} \sum_{m=1 \atop m \equiv n \pmod{p}}^{p} \kappa_p(t, 1, L; m). \]

If \( p | n \) then \( p \nmid m \) for every \( m \not\equiv n \pmod{p} \), and we obtain, by assumption, from (3)
\[ \kappa_p(t+1, l, L; n) = p^{t-1}(p-1)p^{t(t-1)-1} \{ (p-1)^t - (-1)^t \} \]
\[ = p^{(t+1)(t-1)-1}(p-1) \{ (p-1)^t - (-1)^t \}. \]

If \( p \nmid n \) then \( p \nmid m \) for \( (p-2) \) residues \( m \not\equiv n \pmod{p} \), and \( p | m \) for one residue \( m \not\equiv n \pmod{p} \). In this case we obtain, therefore, from (3)
\[ \kappa_p(t+1, l, L; n) = p^{t-1+t(t-1)-1}((p-2) \{ (p-1)^t - (-1)^t \} \]
\[ + (p-1) \{ (p-1)^{t-1} - (-1)^{t-1} \}) \]
\[ = p^{(t+1)(t-1)-1}(p-1) \{ (p-1)^{t+1} - (-1)^{t+1} \}. \]

It follows, by induction, that our lemma is true for all \( s \geq 1 \).

3. **Theorem.** Let \( \kappa(n) \) be defined as in the introduction. Let \( k = (K_1, \ldots, K_s) \), let \( q \) run through all prime factors of \( K \), and put
\[ m_q = n - \sum_{q | K_\sigma}^{s} a_\sigma, \quad s_q = \sum_{q \nmid K_\sigma}^{s} 1. \]
Then
\[ \kappa(n) = K^{z-1} k \times \prod_{\sigma=1}^{s} K_{\sigma}^{-1} \times \prod_{q \mid k \mathcal{m}_{q}} q^{-s_{q}}((q-1)^{s_{q}}-(1)^{s_{q}}) \]
\[ \times \prod_{q \mid \mathcal{m}_{q}} q^{-s_{q}}(q-1)((q-1)^{s_{q}-1}-(1)^{s_{q}-1}), \]
\[ or \ \kappa(n) = 0, \text{ according as} \]
\[ (4) \quad n \equiv \sum_{\sigma=1}^{s} a_{\sigma} \quad (\text{mod } k), \]
or not.

**Proof.** Since the congruences
\[ \{x_{\sigma} \equiv a_{\sigma} \quad (\text{mod } K_{\sigma}) \quad (\sigma = 1, \ldots, s), \sum_{\sigma=1}^{s} x_{\sigma} \equiv n \quad (\text{mod } K)\} \]

imply
\[ n \equiv \sum_{\sigma=1}^{s} x_{\sigma} \equiv \sum_{\sigma=1}^{s} a_{\sigma} \quad (\text{mod } k), \]
it is trivial that \( \kappa(n) = 0 \) if \( n \) does not satisfy the congruence (4).

Suppose now that \( n \) does satisfy the congruence (4). Let
\[ K = \prod_{q} q^{l_{q}}, \quad k = \prod_{q} q^{l_{q}}, \quad k_{\sigma} = \prod_{q} q^{l_{q\sigma}}, \prod_{\sigma=1}^{s} K_{\sigma} = \prod_{q} q^{\Sigma_{q}}, \]
so that
\[ 0 \leq l_{q} \leq \lambda_{q\sigma} \leq L_{q} \quad (\sigma = 1, \ldots, s), \quad L_{q} \geq 1, \sum_{\sigma=1}^{s} \lambda_{q\sigma} = \Sigma_{q}. \]

If \( \kappa_{q}(n) \) denotes the number of sets of residues \( x_{1}, \ldots, x_{s} \)
\( (\text{mod } q^{l_{q}}) \) which satisfy
\[ \begin{cases} x_{\sigma} \equiv a_{\sigma} \quad (\text{mod } q^{l_{q\sigma}}), \quad (x_{\sigma}, q) = 1 \quad (\sigma = 1, \ldots, s), \\ \sum_{\sigma=1}^{s} x_{\sigma} \equiv n \quad (\text{mod } q^{l_{q}}), \end{cases} \]
then, obviously,
\[ (5) \quad \kappa(n) = \prod_{q} \kappa_{q}(n). \]

For finding the value of \( \kappa_{q}(n) \), there is no less of generality in assuming that
\[ l_{q} = \lambda_{q1} \leq \lambda_{q2} \leq \cdots \leq \lambda_{qs} = L_{q}. \]
Consider first the case \( q \mid k \). If \( q \mid k \) we have \( s_q = 0 \) and

\[
1 \leq l_q = \lambda_{q1} \leq \lambda_{q\sigma} \leq L_q \quad (\sigma = 1, \ldots, s).
\]

Since \( \lambda_{q1} = l_q \), and hence

\[
\sum_{\sigma=2}^{s} (L_q - \lambda_{q\sigma}) = (s-1)L_q + l_q - \Sigma_q,
\]

the number of different sets of residues \( x_2, \ldots, x_s \) (mod \( q^{L_q} \)) satisfying

\[
x_\sigma \equiv a_\sigma \pmod{q^{L_q}} \quad (\sigma = 2, \ldots, s)
\]
is evidently given by

\[
q^{(s-1)L_q + l_q - \Sigma_q}.
\]

Now the congruence

\[
x_1 \equiv n - \sum_{\sigma=2}^{s} x_\sigma \equiv n - \sum_{\sigma=2}^{s} a_\sigma \equiv a_1 \pmod{q^{L_q}}
\]

uniquely determines a residue \( x_1 \) (mod \( q^{L_q} \)), and if \( x_1 \) is so determined, then, by (6), (7) and (4), also

\[
x_1 \equiv n - \sum_{\sigma=2}^{s} x_\sigma \equiv n - \sum_{\sigma=2}^{s} a_\sigma \equiv a_1 \pmod{q^{L_q}}
\]

(8)

Since \( (a_\sigma, K_\sigma) = 1 \) and \( \lambda_{q\sigma} \geq 1 \), the congruences (7) and (8) imply \( (x_\sigma, q) = 1 \) \( (\sigma = 1, \ldots, s) \), and hence we conclude that

\[
\kappa_q(n) = q^{(s-1)L_q + l_q - \Sigma_q}
\]

if \( q \mid k \), and \( n \) satisfies (4).

Now consider the case \( q \nmid k \). If \( q \nmid k \) we have \( 1 \leq s_q \leq s - 1 \), and

\[
0 = l_q = \lambda_{q1} = \cdots = \lambda_{qs_q} < \lambda_{q(s_q+1)} \leq \cdots \leq \lambda_{qs} = L_q.
\]

Since \( 0 = l_q = \lambda_{q1} = \cdots = \lambda_{qs} \), and hence

\[
\sum_{\sigma=s_q+1}^{s} (L_q - \lambda_{q\sigma}) = (s-s_q)L_q + l_q - \Sigma_q,
\]

the number of different sets of residues \( x_{s_q+1}, \ldots, x_s \) (mod \( q^{L_q} \)) which satisfy

\[
x_\sigma \equiv a_\sigma \pmod{q^{L_q}} \quad (s_q < \sigma \leq s)
\]
is evidently given by

\[
q^{(s-s_q)L_q + l_q - \Sigma_q}.
\]
It follows that there are

\[ q^{(r_s - r_q) L_s + 1_q - \Sigma_q - \Sigma} \kappa_q(s_q, L_q, L_q^q; n - \sum_{q=1}^s x_q) \]

different sets of residues \(x_1, \ldots, x_s \pmod{q^{L_q^q}}\) which satisfy the congruences (11) and

\[
\begin{aligned}
(x_\sigma, q) &= 1 \quad (\sigma = 1, \ldots, s_q), \\
\sum_{\sigma=1}^s x_\sigma &\equiv n \pmod{q^{L_q^q}}.
\end{aligned}
\]

But \(\lambda_q = 0\) and, consequently,

\[ x_\sigma = a_\sigma \pmod{q^{\lambda_q}} \quad \text{for} \quad \sigma = 1, \ldots, s_q. \]

Further, the congruences (11) and the conditions \((a_\sigma, K_\sigma) = 1\) imply

\[ (x_\sigma, q) = 1 \quad \text{for} \quad s_q < \sigma \leq s, \]

since then \(\lambda_q \geq 1\). Hence, if \(q \nmid k\), then \(\kappa_q(n)\) is given by the expression (12). By (10) and (11), the condition

\[ q \mid \left\{ n - \sum_{\sigma=1}^s x_\sigma \right\} \]

is equivalent to \(q \mid m_q\). We deduce, therefore, from (12) and the lemma that, in the case \(q \nmid k\),

\[ \kappa_q(n) = \begin{cases} 
q^{(s-1)L_q + 1_q - \Sigma_q - \Sigma} (q-1)((q-1)^{s-1} - (-1)^{s-1}) & \text{if} \quad q \mid m_q \\
q^{(s-1)L_q + 1_q - \Sigma_q - \Sigma} ((q-1)^{s-1} - (-1)^{s-1}) & \text{if} \quad q \nmid m_q.
\end{cases} \]

The truth of our theorem, when \(n\) satisfies (4), is thus established by (5), (9) and (13).

4. Conclusion. We have \(\kappa(n) > 0\) if simultaneously

\[(14a) \quad n \equiv s \pmod{2}, \]

\[(14b) \quad n \equiv \sum_{\sigma=1}^s a_\sigma \pmod{k}, \]

\[(14c) \quad n \not\equiv \sum_{\sigma=1}^s a_\sigma \pmod{2} \quad \text{for every odd prime number} \quad q \quad \text{which divides all} \quad K_\sigma \text{except one,} \quad K_{\sigma^*} \text{say.} \]

(Condition (14c) may be stated as \(q \nmid m_q\) for every odd prime number \(q \mid K\) for which \(s_q = 1\).)
It follows that all sufficiently large integers \( n \) satisfying the conditions (14) can be represented as a sum of primes in the form (1), and (2) will be an asymptotic formula for the number of such representations. \(^1\)

To prove the above statement about \( \kappa(n) > 0 \), we observe that, since \( (a_\sigma, K_\sigma) = 1 \),

\[
m_2 = n - \sum_{\sigma=1}^{s} a_\sigma \equiv n - (s - s_2) \equiv s_2 \pmod{2}
\]

provided that \( n \) satisfies (14a). Hence \( s_2 \) is odd if \( 2 \nmid m_2 \), and \( (s_2 - 1) \) is odd if \( 2 | m_2 \). It follows that, if (14a) and (14b) are satisfied, then \( \kappa(n) \) vanishes only if there is an odd prime number \( q \) for which \( s_q = 1 \) and \( q | m_\sigma \).

\(^1\) The above conclusions could also be drawn from general results proved in my paper [2].

REFERENCES

A. Zulauf


J. G. Van der Corput


University College, Ibadan, Nigeria.
March 19th, 1959.

(Oblatum 30-5-1959).