Partial Sums of Powers of Prime Factors

Jean-Marie De Koninck
Département de Mathématiques et de Statistique
Université Laval
Québec G1K 7P4
Canada
jmdk@mat.ulaval.ca

Florian Luca
Mathematical Institute, UNAM
Ap. Postal 61-3 (Xangari)
CP 58 089
Morelia, Michoacán
Mexico
fluca@matmor.unam.mx

Abstract
Given integers \(k \geq 2\) and \(\ell \geq 3\), let \(S_{k,\ell}^*\) stand for the set of those positive integers \(n\) which can be written as \(n = p_1^k + p_2^k + \cdots + p_\ell^k\), where \(p_1, p_2, \ldots, p_\ell\) are distinct prime factors of \(n\). We study the properties of the sets \(S_{k,\ell}^*\) and we show in particular that, given any odd \(\ell \geq 3\), \(\# \bigcup_{k=2}^{\infty} S_{k,\ell}^* = +\infty\).

1 Introduction
In [1], we studied those numbers with at least two distinct prime factors which can be expressed as the sum of a fixed power \(k \geq 2\) of their prime factors. For instance, given an integer \(k \geq 2\), and letting

\[ S_k := \{ n : \omega(n) \geq 2 \text{ and } n = \sum_{p|n} p^k \}, \]
where $\omega(n)$ stands for the number of distinct prime factors of $n$, one can check that the following 8 numbers belong to $S_3$:

$$
\begin{align*}
378 &= 2 \cdot 3^3 \cdot 7 = 2^3 + 3^3 + 7^3, \\
2548 &= 2^2 \cdot 7^2 \cdot 13 = 2^3 + 7^3 + 13^3, \\
2836295 &= 5 \cdot 7 \cdot 11 \cdot 53 \cdot 139 = 5^3 + 7^3 + 11^3 + 53^3 + 139^3, \\
4473671462 &= 2 \cdot 13 \cdot 179 \cdot 593 \cdot 1621 = 2^3 + 13^3 + 179^3 + 593^3 + 1621^3, \\
23040925705 &= 5 \cdot 7 \cdot 167 \cdot 1453 \cdot 2713 = 5^3 + 7^3 + 167^3 + 1453^3 + 2713^3, \\
13579716377989 &= 19 \cdot 157 \cdot 173 \cdot 1103 \cdot 23857 = 19^3 + 157^3 + 173^3 + 1103^3 + 23857^3, \\
21467102506955 &= 2 \cdot 7^3 \cdot 313 \cdot 1439 \cdot 27791 = 2^3 + 7^3 + 313^3 + 1439^3 + 27791^3, \\
119429556097859 &= 7 \cdot 53 \cdot 937 \cdot 6983 \cdot 49199 = 7^3 + 53^3 + 937^3 + 6983^3 + 49199^3.
\end{align*}
$$

In particular, we showed that 378 and 2548 are the only numbers in $S_3$ with exactly three distinct prime factors.

We did not find any number belonging to $S_k$ for $k = 2$ or $k \geq 4$, although each of these sets may very well be infinite.

In this paper, we examine the sets $S^*_k := \{ n : \omega(n) \geq 2 \text{ and } n = \sum_{p \mid n}^* p^k \}$ ($k = 2, 3, \ldots$),

where the star next to the sum indicates that it runs over some subset of primes dividing $n$.

For instance, $870 \in S^*_2$, because

$$
870 = 2 \cdot 3 \cdot 5 \cdot 29 = 2^2 + 5^2 + 29^2.
$$

Clearly, for each $k \geq 2$, we have $S^*_k \supseteq S_k$. Moreover, given integers $k \geq 2$ and $\ell \geq 3$, let $S^*_{k,\ell}$ stand for the set of those positive integers $n$ which can be written as $n = p_1^k + p_2^k + \cdots + p_\ell^k$, where $p_1, p_2, \ldots, p_\ell$ are distinct prime factors of $n$, so that for each integer $k \geq 2$,

$$
S^*_k = \bigcup_{\ell=3}^\infty S^*_{k,\ell}.
$$

We study the properties of the sets $S^*_{k,\ell}$ and we show in particular that, given any odd $\ell \geq 3$, the set $\bigcup_{\ell=2}^\infty S^*_{k,\ell}$ is infinite. We treat separately the cases $\ell = 3$ and $\ell \geq 5$, the latter case being our main result.

In what follows, the letter $p$, with or without subscripts, always denotes a prime number.

## 2 Preliminary results

We shall first consider the set $S^*_2$. Note that if $n \in S^*_2$, then $P(n)$, the largest prime divisor of $n$, must be part of the partial sum of primes which allows $n$ to belong to $S^*_2$. Indeed, assume the contrary, namely that, for some primes $p_1 < p_2 < \cdots < p_r$,

$$
n = p_1^{a_1} \cdots p_r^{a_r} = p_1^2 + \cdots + p_r^2 \quad \in S^*_2,
$$

where $\omega(n)$ stands for the number of distinct prime factors of $n$, one can check that the following 8 numbers belong to $S_3$:
where $i_1 < i_2 < \cdots < i_\ell \leq r - 1$, with $r \geq 3$. Then

$$p_1 \cdots p_{r-2} p_{r-1} p_r \leq n < \ell p_i^2 \leq r p_{r-1}^2,$$

so that $p_1 \cdots p_{r-2} p_r < r p_{r-1} < r p_r$, which implies that $p_1 \cdots p_{r-2} < r$, which is impossible for $r \geq 3$.

While by a parity argument one can easily see that each element of $S_k$ (for any $k \geq 2$) must have an odd number of prime factors, one can observe that elements of $S_k^*$ can on the contrary be written as a sum of an even number of prime powers, as can be seen with 29895972 $\in S_2^*$ (see below).

We can show that if Schinzel’s Hypothesis is true (see Schinzel [2]), then the set $S_3^*$ is infinite. We shall even prove more.

**Theorem 1.** If Schinzel’s Hypothesis is true, then $\#S_3^* = +\infty$.

**Proof.** Assume that $k$ is an even integer such that $r = k^2 - 9k + 21$ and $p = k^2 - 7k + 13$ are both primes, then $n = 2rp(r + k) \in S_3^*$. Indeed, in this case, one can see that

$$n = 2rp(r + k) = 2^3 + r^3 + p^3, \quad (1)$$

since both sides of (1) are equal to $2k^6 - 48k^5 + 492k^4 - 2752k^3 + 8844k^2 - 15456k + 11466$.

Now Schinzel’s Hypothesis guarantees that there exist infinitely many even $k$’s such that the corresponding numbers $r$ and $p$ are both primes. \qed

Note that the first such values of $k$ are $k = 2, 6, 10, 82$ and 94. These yield the following four elements of $S_3^*$ (observing that $k = 2$ and $k = 6$ provide the same number, namely $n = 378$):

$$
378 = 2 \cdot 3^3 \cdot 7 = 2^3 + 3^3 + 7^3, \\
109306 = 2 \cdot 31 \cdot 41 \cdot 43 = 2^3 + 31^3 + 43^3, \\
45084355098 = 2 \cdot 6007 \cdot 6089 \cdot 6163 = 2^3 + 6007^3 + 6163^3, \\
1063669417210 = 2 \cdot 8011 \cdot 8105 \cdot 8191 = 2^3 + 8011^3 + 8191^3.
$$

Not all elements of $S_3^*$ are generated in this way. For instance, the following numbers also belong to $S_3^*$:

$$
23391460 = 2^2 \cdot 5 \cdot 23 \cdot 211 \cdot 241 = 2^3 + 211^3 + 241^3, \\
173871316 = 2^2 \cdot 223 \cdot 421 \cdot 463 = 2^3 + 421^3 + 463^3, \\
126548475909264420 = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 83 \cdot 101 \cdot 45569 \cdot 501931 \\
= 2^3 + 5^3 + 83^3 + 45569^3 + 501931^3,
$$

as well as all those elements of $S_3$ mentioned in Section 1.

**Theorem 2.** $\bigcup_{k=2}^{\infty} S_{k,3}^* = +\infty$.  

3
Proof. This follows immediately from the fact that for each element \( n \in S_{k,3}^* \), one can find a corresponding element \( n' \in S_{k(2r+1),3}^* \) for \( r = 1, 2, \ldots \). Indeed, if \( n \in S_{k,3}^* \), then it means that 
\[
n = p_1^k + p_2^k + p_3^k
\]
for some distinct primes divisors \( p_1, p_2, p_3 \) of \( n \). In particular, it means that \( p_a | (p_b^k + p_c^k) \) for each permutation \((a, b, c)\) of the integers \(1, 2, 3\). We claim that, given any positive integer \( r \), the number 
\[
n' := p_1^{k(2r+1)} + p_2^{k(2r+1)} + p_3^{k(2r+1)}
\]
belongs to \( S_{k(2r+1),3}^* \). Indeed, we only need to show that \( p_a | (p_b^{k(2r+1)} + p_c^{k(2r+1)}) \) for each permutation \((a, b, c)\) of the integers \(1, 2, 3\). But this follows from the fact that \( (p_b^k + p_c^k) \) divides \( (p_b^{k(2r+1)} + p_c^{k(2r+1)}) \) and therefore that \( n' \in S_{k(2r+1),3}^* \). Since \( 378 \in S_{3,3}^* \), the proof is complete. \( \square \)

Remark. It clearly follows from Theorems 1 and 2 that \( \#S_{3(2r+1),3}^* = +\infty \) for any \( r \geq 1 \).

3 Proof of the main result

Theorem 3. Given any odd integer \( \ell \geq 5 \),
\[
\# \bigcup_{k=2}^{\infty} S_{k,\ell}^* = +\infty.
\]
This is an immediate consequence of the following two lemmas.

Lemma 3.1. Let \( t = 2s \geq 2 \) be an even integer and \( p_1, \ldots, p_t \) be primes such that

(i) \( p_i \equiv 3 \pmod{4} \) for all \( i = 1, \ldots, t \).

(ii) \( \gcd(p_i, p_j - 1) = 1 \) for all \( i, j \) in \( \{1, \ldots, t\} \).

(iii) \( \gcd(p_i - 1, p_j - 1) = 2 \) for all \( i \neq j \) in \( \{1, \ldots, t\} \).

Assume furthermore that \( a_1, \ldots, a_t \) are integers and \( n_1, \ldots, n_t \) are odd positive integers such that

(iv) \( \gcd(2n_i + 1, p_i - 1) = 1 \) for all \( i = 1, \ldots, t \).

(v) \( p_i | \sum_{j=1}^{t} p_j^{n_i} + a_i^{n_i} \) for all \( i = 1, \ldots, t \).

(vi) \( s = t/2 \) of the \( t \) numbers \( \left( \frac{a_i}{p_i} \right) \) for \( i = 1, \ldots, t \) are equal to 1 and the other \( s \) are equal to \( -1 \).

Then there exist infinitely many primes \( p \) such that \( S_{p^{-1},t+1}^* \) contains at least one element.
Proof. Let \( a \) be such that

\[
a \equiv 2n_i + 1 \pmod{(p_i - 1)/2}, \quad a \equiv 3 \pmod{4}, \quad a \equiv a_i \pmod{p_i}
\]  

for all \( i = 1, \ldots, t \). The fact that the above integer \( a \) exists is a consequence of the Chinese Remainder Theorem and conditions (i)-(iii) above. Since \( n_i \) is odd, \( (p_i - 1)/2 \) is also odd and \( a \equiv 3 \pmod{4} \), we conclude that the congruence \( a \equiv 2n_i + 1 \pmod{(p_i - 1)/2} \) implies \( a \equiv 2n_i + 1 \pmod{2(p_i - 1)} \).

Now let \( M = 4 \prod_{i=1}^{t} \frac{p_i(p_i - 1)}{2} \). Note that the number \( a \) is coprime to \( M \) by conditions (i)-(iv). Thus, by Dirichlet’s Theorem on primes in arithmetic progressions, it follows that there exist infinitely many prime numbers \( p \) such that \( p \equiv a \pmod{M} \). It is clear that these primes satisfy the same congruences (2) as \( a \) does. Let \( p \) be such a prime and set

\[
n = \sum_{i=1}^{t} p_i(p_i - 1)/2 + p(p-1)/2.
\]

Note that since \( p \equiv 2n_i + 1 \pmod{2(p_i - 1)} \), we get that \( (p-1)/2 \equiv n_i \pmod{p_i - 1} \). Therefore by Fermat’s Little Theorem and condition (v) we get

\[
n \equiv \sum_{j=1}^{t} p_i^{n_i} + p^{n_i} \equiv \sum_{j=1}^{t} p_i^{n_i} + a_i^{n_i} \equiv 0 \pmod{p_i}
\]

for all \( i = 1, \ldots, t \). Finally, conditions (i), (v) and the Quadratic Reciprocity Law show that from the \( t = 2s \) numbers

\[
\left( \frac{p_i}{p} \right) = - \left( \frac{p}{p_i} \right) = - \left( \frac{a_i}{p_i} \right),
\]

exactly half of them are 1 and the other half are \(-1\). Thus, half of the numbers \( p_i^{(p_i - 1)/2} \) are congruent to 1 modulo \( p \) and the other half are congruent to \(-1\) modulo \( p \) which shows that \( n \) is a multiple of \( p \). Hence, \( n \) is a multiple of \( p_i \) for \( i = 1, \ldots, t \) and of \( p \) as well, which implies that \( n \in S_{-1}^{s \times 2, t+1} \).

Lemma 3.2. If \( s \geq 2 \) then there exist primes \( p_i \) and integers \( a_i, n_i \) for \( i = 1, \ldots, t \) satisfying the conditions of Lemma 3.1.

Proof. Observe that \( t - 1 \geq 3 \). Choose primes \( p_1, \ldots, p_{t-1} \) such that \( p_i \equiv 11 \pmod{12} \) for all \( i = 1, \ldots, t - 1 \), \( \gcd(p_i, p_j - 1) = 1 \) for all \( i, j \) in \( \{1, \ldots, t - 1\} \), \( \gcd(p_i - 1, p_j - 1) = 2 \) for all \( i \neq j \) in \( \{1, \ldots, t - 1\} \) and finally \( p_1 + \cdots + p_{t-1} \) is coprime to \( p_1 \cdots p_{t-1} \). Note that \( N = p_1 + \cdots + p_{t-1} \) is an odd number. Such primes can be easily constructed starting with \( p_1 = 11 \) and recursively defining \( p_2, \ldots, p_{t-1} \) as primes in suitable arithmetic progressions. Take \( n_i = 1 \) for \( i = 1, \ldots, t \). Let \( q_1, \ldots, q_t \) be all the primes dividing \( N \). Pick some integers \( a_1, \ldots, a_{t-1} \) such that \( s \) of the numbers \( \left( \frac{-a_i}{p_i} \right) \) are \(-1\) and the other \( s - 1 \) are 1. Now choose a prime \( p_t \) such that \( p_t \equiv 11 \pmod{12} \), \( p_t \) is coprime to \( p_i - 1 \) for \( i = 1, \ldots, t - 1 \),
\[ p_t \equiv -a_i - N \pmod{p_t} \text{ for } i = 1, \ldots, t - 1, \text{ and } \left( \frac{q_t}{p_t} \right) = 1 \text{ for all } i = 1, \ldots, t. \] For these last congruences to be fulfilled, we note that it is enough to choose \( p_t \equiv 1 \pmod{q_u} \) if \( q_u \equiv 1 \pmod{4} \) and \( p_t \equiv -1 \pmod{q_u} \) if \( q_u \equiv 3 \pmod{4} \), where \( u = 1, \ldots, t \). Notice that this choice is consistent with the fact that \( p_t \equiv 11 \pmod{12} \) if one of the \( q_u \) is 3.

So far, the primes \( p_1, \ldots, p_t \) satisfy conditions (i)–(iii) of Lemma 3.1. Finally, put \( a_t = -N \).

Note that \( \left( \frac{-a_t}{p_t} \right) = \prod_{u=1}^{\ell} \left( \frac{q_u}{p_t} \right)^{a_u} = 1 \). Here, \( a_u \) is the exact power of \( q_u \) in \( -a_t \). Hence, exactly \( s \) of the numbers \( \left( \frac{-a_i}{p_i} \right) \) are 1 and the others are \(-1\) and since all primes \( p_i \) are congruent to 3 modulo 4 the same remains true if one replaces \(-a_i\) by \( a_i \). Thus, condition (vi) of Lemma 3.1 holds. Now one checks immediately that (v) holds with \( n_i = 1 \) for all \( i = 1, \ldots, t \), because for all \( i = 1, \ldots, t - 1 \) we have

\[
\sum_{j=1}^{t} p_j^{n_j} + a_i^{n_i} \equiv N + p_t + a_i \pmod{p_i} \equiv 0 \pmod{p_i},
\]

while

\[
\sum_{j=1}^{t} p_j^{n_j} + a_t = N + p_t - N \equiv 0 \pmod{p_t},
\]

and (iv) is obvious because \( 2n_i + 1 = 3 \) and \( p_i - 1 \equiv 10 \pmod{12} \) is not a multiple of 3 for \( i = 1, \ldots, t \).

**Remark.** The above argument does not work for \( s = 1 \). Indeed, in this case \( t - 1 = 1 \), therefore \( p_1 + \cdots + p_{t-1} = p_1 \) and this is not coprime to \( p_1 \).

### 4 Computational results and further remarks

To conduct a search for elements of \( S^*_{k,\ell} \), one can proceed as follows. If \( n \in S^*_{k,\ell} \), then there exists a positive number \( Q \) and primes \( p_1, p_2, \ldots, p_{\ell} \) such that

\[
n = Q p_1 \cdots p_{\ell-1} p_{\ell} = p_1^k + \cdots + p_{\ell-1}^k + p_{\ell}^k,
\]

so that a necessary condition for \( n \) to be in \( S^*_{k,\ell} \) is that \( p_{\ell} | (p_1^k + \cdots + p_{\ell-1}^k) \). (Note that some of the \( p_i \)'s may also divide \( Q \).)

For instance, in order to find \( n \in S^*_{k,3} \), we examine the prime factors \( p \) of \( r^k + q^k \) as \( 2 \leq r < q \) run through the primes up to a given \( x \), and we then check if \( Q := \frac{r^k + q^k + p^k}{rqp} \) is an integer. If this is so, then the integer \( n = Q rqp \) belongs to \( S^*_{k,3} \).
Proceeding in this manner (with $\ell = 3, 4$), we found the following elements of $S_2^*$:

\[ 870 = 2 \cdot 3 \cdot 5 \cdot 29 = 2^2 + 5^2 + 29^2, \]
\[ 188355 = 3 \cdot 5 \cdot 29 \cdot 433 = 5^2 + 29^2 + 433^2, \]
\[ 298995972 = 2^2 \cdot 3 \cdot 11 \cdot 131 \cdot 17291 = 3^2 + 11^2 + 131^2 + 17291^2, \]
\[ 1152597606 = 2 \cdot 3 \cdot 5741 \cdot 33461 = 2^2 + 5741^2 + 33461^2, \]
\[ 1879906755 = 3 \cdot 5 \cdot 2897 \cdot 43261 = 5^2 + 2897^2 + 43261^2, \]
\[ 520910541772 = 2^2 \cdot 3 \cdot 11 \cdot 17291 \cdot 2282281 = 3^2 + 11^2 + 17291^2 + 2282281^2. \]

Although we could not find any elements of $S_4$, we did find some elements of $S_4^*$, but they are quite large. Here are six of them:

\[ 107827277891825604 = 2^2 \cdot 3 \cdot 7 \cdot 31 \cdot 67 \cdot 18121 \cdot 34105993 = 3^4 + 31^4 + 67^4 + 18121^4, \]
\[ 48698490414981559698 = 2 \cdot 3^4 \cdot 7 \cdot 13 \cdot 17 \cdot 157 \cdot 83537 \cdot 14816023 = 2^4 + 17^4 + 83537^4, \]
\[ 3137163227263018301981160710533087044 \]
\[ = 2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 191 \cdot 283 \cdot 7541 \cdot 1330865843 \cdot 2086223663996743 \]
\[ = 3^4 + 7^4 + 191^4 + 1330865843^4, \]
\[ 12950087100661466823050335477000185618 \]
\[ = 2 \cdot 3^2 \cdot 7 \cdot 13^2 \cdot 31 \cdot 241 \cdot 15331 \cdot 21613 \cdot 524149 \cdot 1389403 \cdot 3373402577 \]
\[ = 2^4 + 241^4 + 3373402577^4, \]
\[ 225611412654969160905328479254197935523312771590 \]
\[ = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13^2 \cdot 37 \cdot 41 \cdot 109 \cdot 113 \cdot 127 \cdot 151 \cdot 541 \cdot 911 \cdot 5443 \]
\[ \cdot 3198662197 \cdot 689192061269 \]
\[ = 5^4 + 7^4 + 113^4 + 127^4 + 911^4 + 689192061269^4, \]
\[ 17492998726637106830622386354099071096746866616980 \]
\[ = 2^2 \cdot 5 \cdot 7 \cdot 23 \cdot 31 \cdot 97 \cdot 103 \cdot 373 \cdot 1193 \cdot 8689 \cdot 2045107145539 \cdot 2218209705651794191 \]
\[ = 2^4 + 103^4 + 373^4 + 1193^4 + 2045107145539^4. \]

Note that these numbers provide elements of $S_{4,3}^*$, $S_{4,4}^*$, $S_{4,5}^*$ and $S_{4,6}^*$.

The smallest elements of $S_2^*$, $S_3^*$, ..., $S_{10}^*$ are the following:

\[ 870 = 2 \cdot 3 \cdot 5 \cdot 29 = 2^2 + 5^2 + 29^2, \]
\[ 378 = 2 \cdot 3^3 \cdot 7 = 2^3 + 3^3 + 7^3. \]

\[ 107827277891825604 = 2^2 \cdot 3 \cdot 7 \cdot 31 \cdot 67 \cdot 18121 \cdot 34105993 = 3^4 + 31^4 + 67^4 + 18121^4 \]
\[ 178101 = 3^2 \cdot 7 \cdot 11 \cdot 257 = 3^5 + 7^5 + 11^5 \]
\[ 594839010 = 2 \cdot 3 \cdot 5 \cdot 17 \cdot 29 \cdot 37 \cdot 1087 = 2^5 + 6^5 + 29^6 \]
\[ 275223438741 = 3 \cdot 23 \cdot 43 \cdot 92761523 = 3^7 + 23^7 + 43^7 \]
\[ 26584448904822018 = 2 \cdot 3 \cdot 7 \cdot 17 \cdot 19 \cdot 113 \cdot 912733109 = 2^8 + 17^8 + 113^8 \]
\[ 40373802 = 2 \cdot 3^4 \cdot 7 \cdot 35603 = 2^9 + 3^9 + 7^9 \]
\[ 420707243066850 = 2 \cdot 3^2 \cdot 5^2 \cdot 29 \cdot 32238102917 = 2^{10} + 5^{10} + 29^{10}. \]
Below is a table of the smallest element $n \in S^*_{k,\ell}$ for $\ell = 3, 4, 5, 6, 7$ (with a convenient $k$):

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$378 = 2 \cdot 3^2 \cdot 7 = 2^3 + 3^2 + 7^3$</td>
</tr>
<tr>
<td>4</td>
<td>$298995972 = 2^2 \cdot 3 \cdot 11 \cdot 131 \cdot 17291 = 3^2 + 11^2 + 131^2 + 17291^2$</td>
</tr>
<tr>
<td>5</td>
<td>$2836295 = 5 \cdot 7 \cdot 11 \cdot 53 \cdot 139 = 5^3 + 7^3 + 11^3 + 53^3 + 139^3$</td>
</tr>
<tr>
<td>6</td>
<td>(a 48 digit number) = $5^4 + 7^4 + 11^3 + 127^4 + 911^4 + 689192061269^4$</td>
</tr>
<tr>
<td>7</td>
<td>(a 145 digit number) = $2^{14} + 3^{14} + 5^{14} + 11^{14} + 131^{14} + 149^{14} + 19809551197^{14}$</td>
</tr>
</tbody>
</table>

Theorem 3 provides a way to construct infinitely many elements of $S^*_{k,\ell}$ given any fixed positive odd integer $\ell$. However, in practice, the elements obtained are very large. Indeed, take the case $k = 5$. With the notation of Lemma 1, we have $t = 4$; one can then choose \( \{p_1, p_2, p_3, p_4\} = \{11, 47, 59, 227\} \). As suggested in Lemma 2, let $n_i = 1$ for $i = 1, 2, 3, 4$. An appropriate set of integers $a_i$'s is given by \( \{a_1, a_2, a_3, a_4\} = \{8, 32, 10, 110\} \), which gives \( \left\{ \left(\frac{a_i}{p_i}\right) : i = 1, 2, 3, 4 \right\} = \{-1, 1, -1, 1\} \). Looking for a solution $a$ of the set of congruences

\[
\begin{align*}
    a &\equiv 3 \pmod{\frac{p_i-1}{2}} \quad (i = 1, 2, 3, 4) \\
    a &\equiv 3 \pmod{4} \\
    a &\equiv a_i \pmod{p_i} \quad (i = 1, 2, 3, 4)
\end{align*}
\]

we obtain $a = 4\,619\,585\,064\,883$. With $M = 4 \prod_{i=1}^{4} p_i(p_i - 1) = 10\,437\,648\,923\,020$, we notice that indeed $\gcd(a, M) = 1$. As the smallest prime number $p \equiv a \pmod{M}$, we find $p = 10M + a = 108\,996\,074\,295\,083$. This means that the smallest integer $n \in S^*_{k,5}$ constructed with our algorithm is given by

\[
n = \sum_{i=1}^{4} p_i^{\frac{p_i-1}{2}} + p^{\frac{p-1}{2}},
\]

which is quite a large integer since

\[
n \approx p^{\frac{p-1}{2}} \approx (10^{14})^{\frac{1}{2}} \approx 10^{7 \cdot 10^{14}}.
\]

References


2000 Mathematics Subject Classification: Primary 11A41; Secondary 11A25.

Keywords: prime factorization.