ON WARING’S PROBLEM WITH POWERS OF PRIMES

By S. S. Pillai
Annamalainagar, S. India

Received December 13, 1938
(Communicated by Prof. A. Narasinga Rao)

Let \( k \) be any integer \( \geq 4 \) and \( p^\theta \) be the highest power of the prime \( p \) which divides \( k \).

Let
\[
\gamma = \begin{cases} 
\theta + 2 & \text{for } \theta = 2, 2 \mid k, \\
\theta + 1 & \text{otherwise} 
\end{cases}
\]

and
\[
K = \prod_{p \mid k} p^{\gamma}
\]

Then Loo-keng Hua* proves

Theorem. Every sufficiently large integer \( N \equiv s \mod{K} \) is a sum of \( s \) \( k \)th powers of primes, provided \( s \geq s_0 \), where \( s_0 = s_0(k) = 6k \log k \).

Towards the end of the paper, he remarks “The congruence condition in the theorem is essential and cannot be replaced by a weaker one.”

Let \( G_1(k) \) be the least value of \( s \) such that every large integer is the sum of at most \( s \) \( k \)th powers of primes.

Then Hua’s result means that
\[
G_1(k) \leq K + s_0.
\]

It can be proved that, for an infinite number of values of \( k, K \) is greater than any power of \( k \). So from Hua’s result we cannot derive that \( G_1(k) \) is less than some fixed power of \( k \) for all \( k \). The object of this paper is to derive from Hua’s result, that
\[
\lim_{k \to \infty} \frac{G_1(k)}{k \log k} \leq 6.
\]

Further Notations

Let \( K = 2^\gamma \cdot p_1^\gamma_1 \cdot p_2^\gamma_2 \cdots p_n^\gamma_n \) so that \( \gamma_r = \theta_r + 1 \) and \( p_r \theta_r \parallel k \), and \( (p_r - 1) \mid k \), for \( r = 1, 2, \ldots, n \).

Further let \( d_r = p_r^{\gamma_r}, r = 1, \ldots, n \).

\( P \) is the smallest prime which does not divide \( K \).

* Mathematische Zeitschrift, 1938, 44 Band, 3 Heft, 331-46.
$t = t(k)$ is the least value of $s$ such that $N \equiv x_1 + \cdots + x_s \pmod{K}$ is solvable for every $N$ in terms of $x$, where

$$x = 0, \, 1^k \text{ or } \frac{p^n - 1}{p - 1} \text{, where } p | K$$

$$T = 2(d_1 + \cdots + d_n) + 2\gamma - 2n + 1$$

$$T_0 = 3(d_1 + \cdots + d_n) + 2\gamma - 2n.$$

$A_1, A_2, \ldots, A_n$ denote the different positive reduced residue classes mod. $K$, in $x_1 \cdot 1^k + x_2 \cdot p_2^k + \cdots + x_n \cdot p_n^k$ where $1 \leq x_r \leq d_r$, $r = 1, \ldots, n$, arranged in ascending order of magnitudes.

$$J = \left\lceil \frac{(d_1 + d_2 + \cdots + d_n - n + 1)}{2\gamma} \right\rceil.$$

**Lemmas**

**Lemma (1):** If $(hA, B) = 1$, then we can find $x, y$ such that

$$hAx + By = C \pmod{AB},$$

with $1 \leq x \leq B$ and $1 \leq y \leq A$, where $h, A, B, C$ are given.

Since $(hA, B) = 1$, when $x = 1, 2, \ldots, B$ and $y = 1, 2, \ldots, A$, $hAx + By$ takes incongruent values mod. $AB$. Hence it runs through a complete residue system mod. $AB$.

So the lemma follows:

**Lemma (2):** Let $(h_i, d_i) = 1$, $i = 1, \ldots, n$ and $C$ be any integer. Then we can find $X_i$ such that $1 \leq X_i \leq d_i$, $i = 1, \ldots, n$, and $X_1 \cdot h_1 \cdot d_1 + X_2 \cdot h_2 \cdot d_2 + \cdots + X_n \cdot h_n \cdot d_n = C \pmod{d_1 \cdot \cdots \cdot d_n}$.

Since $d_1, \ldots, d_n$ are prime to one another, $(d_1, d_2 \cdots d_n) = 1$. So by lemma (1), we can find $X_1, Y_1$ such that

(1) $h_1 \cdot d_2 \cdots d_n \cdot X_1 + d_1 \cdot Y_1 = C \pmod{d_1 \cdot d_2 \cdots d_n}$ with $1 \leq X_1 \leq d_1$ and $1 \leq Y_1 \leq d_2 \cdots d_n$.

Again by lemma (1), we have

(2) $h_2 \cdot d_3 \cdots d_n \cdot X_2 + d_2 \cdot Y_2 = Y_1 \pmod{d_2 \cdots d_n}$, with $1 \leq X_2 \leq d_2$, $1 \leq Y_2 \leq d_3 \cdots d_n$.

Hence from lemma (2), we get

(3) $h_3 \cdot d_4 \cdots d_n \cdot X_3 + d_3 \cdot Y_3 = Y_2 \pmod{d_3 \cdots d_n}$ with $1 \leq X_3 \leq d_3$, $1 \leq Y_3 \leq d_4 \cdots d_n$.

By repeating this we get,

$$h_{n-1} \cdot d_n \cdot X_{n-1} + d_{n-1} \cdot Y_{n-1} = Y_{n-2} \pmod{d_{n-1} \cdot d_n},$$

with $1 \leq X_{n-1} \leq d_{n-1}$, $1 \leq Y_{n-1} \leq d_n$.

Finally, we have

$$h_n \cdot X_n = Y_{n-1} \pmod{d_n}$$

with $1 \leq X_n \leq d_n$. 

By multiplying the second congruence by \(d_1\), the third by \(d_1 d_2\), \(d_3\), and the last by \(d_1 d_2 \cdots d_{n-1}\), we get

\[
\begin{align*}
  h_1 d_1 \cdots d_n X_1 + d_1 Y_1 &\equiv C \pmod{d_1 \cdots d_n} \\
  h_2 d_1 \cdots d_n X_2 + d_1 d_2 Y_2 &\equiv d_1 Y_1 \\
  h_3 d_1 d_2 d_3 \cdots d_n X_3 + d_1 d_2 d_3 Y_3 &\equiv d_1 d_2 Y_2 \\
  \vdots \\
  h_{n-1} d_1 \cdots d_{n-2} d_n X_{n-1} + d_1 \cdots d_{n-2} Y_{n-1} &\equiv d_1 \cdots d_{n-2} Y_{n-2} \\
  h_n d_1 \cdots d_{n-1} X_n &\equiv d_1 \cdots d_{n-1} Y_{n-1} \\
\end{align*}
\]

By adding all the above and cancelling common terms, we get the lemma.

**Lemma (3):** When \(r = 1, 2, \ldots, n\), \(p_r^k \equiv h_r \frac{K}{d_r} + 1 \pmod{K}\), where \((h_r, d_r) = 1\).

By Fermat’s theorem

\[
p_r^k \equiv 1 \pmod{2r}
\]

Hence

\[
p_r^k \equiv 1 \pmod{K/d_r}
\]

Hence

\[
p_r^k \equiv h_r \frac{K}{d_r} + 1 \pmod{K}
\]

Since \((p_r^k, K) = d_r, (h_r, d_r) = 1\).

**Lemma (4):** \(A_r - A_{r-1} \leq T, r = 2, 3, \ldots, n\)

and

\[
K + A_1 - A_n \leq T.
\]

In lemma (2), put \(C = J + 1\) and \(h_r\) equal to the \(h_s\) defined in lemma (8) and multiply throughout by \(2^\gamma\). Then we get

\[
X_1 h_1 K/d_1 + \cdots + X_n h_n K/d_n \equiv C \cdot 2^\gamma \pmod{K}.
\]

Let \(A_r = a_1 p_1^k + \cdots + a_n p_n^k \pmod{K}\) with \(1 \leq a_s < d_s\). Then

\[
A_r - C \cdot 2^\gamma \equiv \sum_{s=1}^{n} a_s p_s^k - C \cdot 2^\gamma \pmod{K}
\]

\[
\equiv \sum_{s=1}^{n} a_s \left( h_s \frac{K}{d_s} + 1 \right) - \sum_{s=1}^{n} X_s h_s \frac{K}{d_s} \pmod{K}
\]

\[
= \sum_{s=1}^{n} (a_s - X_s) h_s K/d_s + a_1 + \cdots + a_n.
\]

Let \(a_s - X_s \equiv b_s \pmod{d_s}\),

where \(1 \leq b_s < d_s\).
Then \((a_s - X_s) h_s K/d_s \equiv b_s h_s K/d_s \pmod{K}\).

Hence
\[
A_r - C = 2 \gamma + \sum_{s=1}^{n} \{ (b_s h_s K/d_s) + a_s \} \pmod{K}
\]
\[
= \sum_{s=1}^{n} \left\{ b_s \left( h_s K/d_s^s + 1 \right) + a_s - b_s \right\}
\]
\[
= \sum_{s=1}^{n} b_s \varphi_s^k + \sum_{s=1}^{n} (a_s - b_s) \quad \pmod{K}
\]

Let
\[
\sum_{s=1}^{n} b_s \varphi_s^k = A_i \quad \pmod{K}
\]

Then
\[
A_r - A_i = C \cdot 2 \gamma + \sum_{s=1}^{n} (a_s - b_s) \pmod{K}.
\]

Now
\[
C \cdot 2 \gamma + \sum_{s=1}^{n} (a_s - b_s) \leq (J + 1) \cdot 2 \gamma + \sum_{s=1}^{n} (d_s - 1)
\]
\[
< d_1 + \cdots + d_u - n + 1 + 2 \gamma + d_1 + \cdots + d_u - n
\]
\[
= 2 \sum_{r=1}^{n} d_r + 2 \gamma - 2 n + 1
\]

Again
\[
C \cdot 2 \gamma + \sum_{s=1}^{n} (a_s - b_s) \geq (J + 1) \cdot 2 \gamma + \sum_{s=2}^{n} (1 - d_s)
\]
\[
> d_1 + \cdots + d_u - n + 1 + n - (d_1 + \cdots + d_u)
\]
\[
= 1.
\]

So
\[
A_r - A_i = D \pmod{K}
\]
where \(1 < D < T\).

This means that \(r \neq i\), and

1 < \(A_r - A_i < T\) when \(i < r\)

and

1 < \(K + A_r - A_i < T\) when \(i > r\).

From this the lemma follows:

Lemma (5) : \(t = t(k) < T_0\).

Let 1 < \(S < K\). Then, by lemma (4),

if \(A_r < S < A_{r+1}\), 1 < \(S - A_r < A_{r+1} - A_r - 1 < T - 1\),

and if \(A_r < S < K\), 1 < \(S - A_r < K - A_r - 1 < T - 1\).

Hence if 1 < \(S < K\), there is one \(r\) such that

1 < \(S - A_r < T - 1\), where \(r = 0, \cdots, u\), and \(A_0 = 0\).

So
\[
S = A_r + D \text{ where } D < T - 1.
\]
On Waring's Problem with Powers of Primes

For every $N$ there is one $S$ such that
$$1 \leq S \leq K \text{ and } N \equiv S \pmod{K}.$$  
But $S = A_r + D$.

Hence $N \equiv A_r + D \pmod{K}$.

Further
$$D \equiv D \cdot P^k \pmod{K}$$

and
$$A_r \equiv a_1 p_1^k + \cdots + a_n p_n^k \pmod{K}$$

where $1 \leq a_r \leq d_r$, $s = 1, \cdots, n$.

So
$$N \equiv a_1 p_1^k + \cdots + a_n p_n^k + D \cdot P^k \pmod{K}.$$

Since $a_1 + \cdots + a_n \leq d_1 + \cdots + d_n$

and $D \leq T - 1$, the lemma follows.

**Lemma (6):** $T_0 \leq 4 \cdot 5 \sigma (k) + 4 k$,

where $\sigma (k) = \sum_{d|k} d$.

$$T_0 = 3 \sum_{r=1}^{n} d_r + 2\gamma - 2n$$

$$= 3 \sum \frac{\phi}{p} (p - 1) p^\theta + 2\gamma - 2n,$$

where $p$ is an odd prime such that $(p - 1) p^\theta | k$.

So
$$T_0 \leq 3 \sum \frac{\phi}{p} (p - 1) p^\theta + 2\gamma - 2n$$

$$\leq 3 \sum \frac{\phi}{p} (p - 1) p^\theta + 2\gamma$$

$$\leq 4 \cdot 5 \sum_{d|n} d + 4 k$$

$$= 4 \cdot 5 \sigma (k) + 4 k.$$

**Theorems**

**Theorem I:** $G_1 (k) \leq s_0 + t$.

From the definition of $t$, for every $N$

$$N - s_0 = x_1 + x_2 + \cdots + x_t \pmod{K},$$

where $x = 0, P^k$, or $p^k$, where $p | K$.

Let $M = N - x_1 - \cdots - x_t$.

Then $M$ is large when $N$ is large and $M \equiv s_0 \pmod{K}$.

Therefore from Hua's result, $M$ is the sum of $s_0 \cdot k$th powers of primes.

But $N = M + x_1 + \cdots + x_t$, where $x = 0, P^k$ or $p^k$.

Hence $N$ is the sum of at most $s_0 + t \cdot k$th powers of primes.

**Theorem II:** $G_1 (k) \leq s_0 + T_0$.  

$A3$
This follows from Theorem I and lemma (5).

**Theorem III.** \( G_1(k) \leq s_0 + 4 \cdot 5 \sigma(k) + 4k \).
This follows from Theorem II and lemma (6).

**Theorem IV.** \( \lim_{k \to \infty} \frac{G_1(k)}{k \log k} \leq 6 \).

Since \( T_0 = 0[\sigma(k)] \) and \( s_0 \sim 6k \log k \), the theorem follows from Theorem III.

**Theorem V.** \( G_1(4) \leq 34 \).
By verification \( t = 15 \), when \( k = 4 \) and \( s_0 = 19 \).

**Theorem VI.** \( G_1(6) \leq 56 \).
By verification \( t(6) = 11 \), and \( s_0(6) = 45 \).

**Conclusion**

Conjecture I. \( t(k) \leq \Gamma(k) + 2 \) in all cases, except when \( k = 2 \).
Elsewhere, I have shown that when \( k = 2^r \) or \( \phi(p^r) \)
\( G_1(k) \geq \Gamma(k) + 2 \), and \( G_1(2) > 7 \).

By slightly modifying the method of proof for lemma (2), we can prove

**Theorem :** If \( (a_1, a_2, \ldots, a_n) = 1 \)
we can find \( x_1, \ldots, x_n \) integers such that
\[
| x_r | < (a_1, a_2, \ldots, a_{r-1}, a_{r+1}, \ldots, a_n), r = 1, \ldots, n
\]
and \( a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 1 \).