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 $\geqslant 4$ and p^θ be the highest power of the prime p which divides k.

Let

$$\gamma = \begin{cases} \theta + 2 \text{ for } p = 2,\ 2 \mid k, \\ \theta + 1 \text{ otherwise} \end{cases}$$

and

$$K = \prod_{(p-1) \mid k} p^\gamma$$

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* $s \geqslant s_0$, *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 kth powers of *primes*.

Then Hua's result means that

$$G_1(k) \leqslant K + s_0.$$

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

$$\overline{\lim_{k \to \infty}} \frac{G_1(k)}{k \log k} \leqslant 6.$$

Further Notations

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

Further let $d_r = p_r^{\gamma_r}$, $r = 1, \cdots, n$.

P is the smallest prime which does not divide K.

* *Mathematische Zeitschrift*, 1938, **44 Band**, 3 Heft, 334–46.

$t = t(k)$ is the least value of s such that $N \equiv x_1 + \cdots + x_s \pmod{K}$ is solvable for ever N in terms of x, where

$$x = 0, P^k \text{ or } p^k, \text{ where } p \mid K$$
$$T = 2(d_1 + \cdots + d_n) + 2^\gamma - 2n + 1$$
$$T_0 = 3(d_1 + \cdots + d_n) + 2^\gamma - 2n.$$

$A_1, A_2, \cdots, A_u$ denote the different positive reduced residue classes mod. K, in $x_1 p_1^k + x_2 p_2^k + \cdots + x_n p_n^k$ where $1 \leqslant x_r \leqslant d_r$, $r = 1, \cdots, n$, arranged in ascending order of magnitudes.

$$J = [(d_1 + d_2 + \cdots + d_n - n + 1)/2^\gamma].$$

Lemmas

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

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

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

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

So the lemma follows :

Lemma (2) : *Let* $(h_s, d_s) = 1$, $s = 1, \cdots, n$ *and* C *be any integer. Then we can find* X_s *such that* $1 \leqslant X_s \leqslant d_s$, $s = 1, \cdots, n$, *and* $X_1 h_1 d_2 \cdots d_n + X_2 h_2 d_1 d_3 \cdots d_n + \cdots + X_n h_n d_1 \cdots d_{n-1} \equiv C \pmod{d_1 \cdots d_n}$.

Since $d_1, \cdots, d_n$ are prime to one another, $(d_1, h_1 d_2 \cdots d_n) = 1$. So by lemma (1), we can find X_1, Y_1 such that

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

Again by lemma (1), we have

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

Hence from lemma (2), we get

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

By repeating this we get,

$h_{n-1} d_n X_{n-1} + d_{n-1} Y_{n-1} \equiv Y_{n-2} \pmod{d_{n-1} d_n}$, with $1 \leqslant X_{n-1} \leqslant d_{n-1}$, $1 \leqslant Y_{n-1}, \leqslant d_n$.

Finally, we have

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

with $1 \leqslant X_n \leqslant d_n$.

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

$$
\begin{array}{llll}
h_1\, d_2 \cdots d_n\, X_1 & + d_1 Y_1 & \equiv C & (\text{mod. } d_1 \cdots d_n) \\
h_2\, d_1\, d_3 \cdots d_n\, X_2 & + d_1 d_2 Y_2 & \equiv d_1 Y_1 & (\quad ,, \quad) \\
h_3\, d_1\, d_2\, d_4 \cdots d_n\, X_3 & + d_1\, d_2\, d_3\, Y_3 & \equiv d_1\, d_2\, Y_2 & (\quad ,, \quad)
\end{array}
$$

....

....

....

$$
\begin{array}{ll}
h_{n-1}\, d_1 \cdots d_{n-2}\, d_n\, X_{n-1} + d_1 \cdots d_{n-1}\, Y_{n-1} \equiv d_1 \cdots d_{n-2}\, Y_{n-2} & (\quad ,, \quad) \\
h_n\, d_1 \cdots d_{n-1}\, X_n \equiv d_1 \cdots d_{n-1}\, Y_{n-1} & (\quad ,, \quad)
\end{array}
$$

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

Lemma (3): *When* $r = 1, 2, \cdots, n$, $p_r^k \equiv h_r . \dfrac{K}{d_r} + 1$ (mod. K), *where* $(h_r, d_r) = 1$.

By Fermat's theorem

$$p_r^k \equiv 1 \ (\text{mod. } p_s),\ s = 1, \cdots, r-1, r+1, \cdots, n.$$

Further

$$p_r^k \equiv 1 \ (\text{mod. } 2^\gamma).$$

Hence $p_r^k \equiv 1$ (mod. K/d_r).

Hence $p_r^k \equiv h_r \cdot \dfrac{K}{d_r} + 1$ (mod. K).

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

Lemma (4): $A_r - A_{r-1} \leqslant T$, $r = 2, 3, \cdots, u$

and $K + A_1 - A_u \leqslant T$.

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

$$X_1\, h_1\, K/d_1 + \cdots + X_n\, h_n\, K/d_n \equiv C \cdot 2^\gamma \ (\text{mod. K}).$$

Let $A_r \equiv a_1\, p_1^k + \cdots + a_n\, p_n^k$ (mod. K) with $1 \leqslant a_s \leqslant d_s$ $s = 1, \cdots, n$.

Then

$$
\begin{aligned}
A_r - C\, 2^\gamma &\equiv \sum_{s=1}^{n} a_s\, p_s^k - C \cdot 2^\gamma && (\text{mod. K}) \\
&\equiv \sum_{s=1}^{n} a_s \left(h_s \frac{K}{d_s} + 1 \right) - \sum_{s=1}^{n} X_s\, h_s \frac{K}{d_s} && (\text{mod. K}) \\
&= \sum_{s=1}^{n} (a_s - X_s)\, h_s\, K/d_s + a_1 + \cdots + a_n.
\end{aligned}
$$

Let $a_s - X_s \equiv b_s$ (mod. d_s),

where $1 \leqslant b_s \leqslant d_s$.

Then $(a_s - X_s)\, h_s\, K/d_s \equiv b_s h_s\, K/d_s \pmod{K}$.

Hence

$$A_r - C\, 2^\gamma \equiv \sum_{s=1}^{n} \{(b_s\, h_s\, K/d_s) + a_s\} \pmod{K}$$

$$= \sum_{s=1}^{n} \left\{b_s \left(h_s \frac{K}{d_s} + 1\right) + a_s - b_s\right\}$$

$$\equiv \sum_{s=1}^{n} b_s\, p_s^k + \sum_{s=1}^{n} (a_s - b_s) \pmod{K}$$

Let $\sum_{s=1}^{n} b_s\, p_s^k \equiv A_i \pmod{K}$.

Then

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

Now

$$C\, 2^\gamma + \sum_{s=1}^{n} (a_s - b_s) \leqslant (J + 1)\, 2^\gamma + \sum_{s=1}^{n} (d_s - 1)$$

$$\leqslant d_1 + \cdots + d_n - n + 1 + 2^\gamma + d_1 + \cdot + d_n - n$$

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

Again

$$C\, 2^\gamma + \sum_{s=1}^{n} (a_s - b_s) \geqslant (J + 1)\, 2^\gamma + \sum_{s=2}^{n} (1 - d_s)$$

$$\geqslant d_1 + \cdot + d_n - n + 1 + n - (d_1 + \cdot + d_n)$$

$$= 1.$$

So

$$A_r - A_i \equiv D \pmod{K}$$

where $1 \leqslant D \leqslant T$.

This means that $r \neq i$, and

$$1 \leqslant A_r - A_i \leqslant T \text{ when } i < r$$

and

$$1 \leqslant K + A_r - A_i \leqslant T \text{ when } i > r.$$

From this the lemma follows :

Lemma (5) : $t = t\,(k) \leqslant T_0$.

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

if $A_r < S \leqslant A_{r+1}$, $1 \leqslant S - A_r \leqslant A_{r+1} - A_r - 1 \leqslant T - 1$,

and if $A_u < S \leqslant K$, $1 \leqslant S - A_u \leqslant K - A_u - 1 \leqslant T - 1$.

Hence if $1 \leqslant S \leqslant K$, there is one r such that

$1 \leqslant S - A_r \leqslant T - 1$, where $r = 0, \cdots, u$, and $A_0 = 0$.

So $S = A_r + D$ where $D \leqslant T - 1$.

For every N there is one S such that

$$1 \leqslant \mathrm{S} \leqslant \mathrm{K} \text{ and } \mathrm{N} \equiv \mathrm{S} \pmod{\mathrm{K}}.$$

But $\quad \mathrm{S} = \mathrm{A}_r + \mathrm{D}$.

Hence $\quad \mathrm{N} \equiv \mathrm{A}_r + \mathrm{D} \pmod{\mathrm{K}}$.

Further

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

and

$$\mathrm{A}_r \equiv a_1 p_1^k + \cdots + a_n p_n^k \pmod{\mathrm{K}}$$

where $\quad 1 \leqslant a_s \leqslant d_s,\ s = 1, \cdots, n$.

So

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

Since $\quad a_1 + \cdot + a_n \leqslant d_1 + \cdots + d_n$

and $\quad \mathrm{D} \leqslant \mathrm{T} - 1$, the lemma follows.

Lemma (6) : $\mathrm{T}_0 \leqslant 4 \cdot 5\, \sigma(\mathrm{k}) + 4\,\mathrm{k}$,

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

$$\mathrm{T}_0 = 3 \sum_{r=1}^{n} d_r + 2\gamma - 2n$$

$= 3 \Sigma\, p^{\theta+1} + 2\gamma - 2n$, where p is an odd prime such that $(p-1)\, p^\theta \mid k$.

So

$$\begin{aligned} \mathrm{T}_0 &= 3 \Sigma \frac{p}{p-1} (p-1)\, p^\theta + 2\gamma - 2n \\ &\leqslant 3 \Sigma\, \tfrac{3}{2} (p-1)\, p^\theta + 2\gamma \\ &\leqslant 4 \cdot 5 \sum_{d \mid n} d + 4k \\ &= 4 \cdot 5\, \sigma(k) + 4k. \end{aligned}$$

Theorems

THEOREM I : $\mathrm{G}_1(k) \leqslant \mathrm{s}_0 + \mathrm{t}$.

From the definition of t, for every N

$$\mathrm{N} - s_0 \equiv x_1 + x_2 + \cdots + x_t \pmod{\mathrm{K}}.$$

where $\quad x = 0,\ \mathrm{P}^k$, or p^k, where $p \mid \mathrm{K}$.

Let $\quad \mathrm{M} = \mathrm{N} - x_1 - \cdots - x_t$.

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

Therefore from Hua's result, M is the sum of s_0 kth powers of primes.

But $\quad \mathrm{N} = \mathrm{M} + x_1 + \cdot + x_t$, where $x = 0$, P^k or p^k.

Hence N is the sum of at most $s_0 + t$ kth powers of primes.

THEOREM II. $\mathrm{G}_1(\mathrm{k}) \leqslant \mathrm{s}_0 + \mathrm{T}_0$.

This follows from Theorem I and lemma (5).

THEOREM III. $G_1(k) \leqslant s_0 + 4 \cdot 5\, \sigma(k) + 4k.$

This follows from Theorem II and lemma (6).

THEOREM IV. $$\lim_{k \to \infty} \frac{G_1(k)}{k \log k} \leqslant 6.$$

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

THEOREM V. $G_1(4) \leqslant 34.$

By verification $t = 15$, when $k = 4$ and $s_0 = 19$.

THEOREM VI. $G_1(6) \leqslant 56.$

By verification $t(6) = 11$, and $s_0(6) = 45$.

Conclusion

Conjecture I. $t(k) \leqslant \Gamma(k) + 2$ in all cases, except when $k = 2$.

Elsewhere, I have shown that when $k = 2^r$ or $\phi(p^\theta)$

$$G_1(k) \geqslant \Gamma(k) + 2, \text{ and } G_1(2) \geqslant 7.$$

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

THEOREM: *If* $(a_1, a_2, \cdots, a_n) = 1$ *we can find* $x_1, \cdots, x_n$ *integers such that*

$$|x_r| < (a_1, a_2, \cdots, a_{r-1}, a_{r+1}, \cdots, a_n), \; r = 1, \cdots, n$$

and $a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 1.$