Lemma 8.1. If $s \geq 2k$ (k odd), or $s \geq 4k$ (k even), then $\chi(p) > 0$ for all $p \in P$ and $N \in \mathbb{N}$.

Pf It is enough to show that $x_1^k + \dots + x_s^k \equiv N \pmod{p^\gamma}$ (8.1)

(where $\gamma = \tau + 1$ or $\gamma = \tau + 2$ with $p^\tau \| k$, resp. for $p > 2$ or $p = 2$).

has solution with $x_1, \dots, x_s$ not all divisible by p.

If $N \not\equiv 0$ then for any solution to (8.1), $\exists i$ s.t. $x_i \not\equiv 0\ (p)$.

If $N \equiv 0$ we'll find a sol. to $x_1^k + \dots + x_{s-1}^k + 1 \equiv N\ (p^\gamma)$

$\Longleftrightarrow x_1^k + \dots + x_{s-1}^k \equiv N' = N - 1\ (p^\gamma)$ with $N' \not\equiv 0\ (p^\gamma)$

Thus WLOG if s replaced by $s-1$ then enough to find a solution to (8.1) for $N \not\equiv 0\ (p) \Leftrightarrow N \in \mathbb{Z}_{p^\gamma}^*$

Write $N' \sim N$ if $\exists\ z \in \mathbb{Z}_{p^\gamma}^*$ st. $N' \equiv z^k N\ (p^\gamma)$.

Then solving (8.1) for N or N' is equivalent by a change of variables $x_i' = z x_i \Rightarrow \sum (x_i')^k \equiv z^k \sum x_i^k \equiv N'$ (p^γ).

Let $S(N) = \min \{ s \in \mathbb{N},\ \text{s.t.}\ \exists x_1, \dots, x_s : x_1^k + \dots + x_s^k \equiv N\ (p^\gamma) \}$

Want to prove $S(N) \leq 2k - 1\ \forall N \in \mathbb{Z}_{p^\gamma}^*$ if k odd

and $S(N) \leq 4k - 1\ \forall N \in \mathbb{Z}_{p^\gamma}^*$ (k even)

By the above symmetry observation; $S(N)=S(N')$ if $N \sim N'$ i.e. if $N' = z^k N$ with $z \in \mathbb{Z}_{p^\gamma}^*$.

Let $G_k = \{z^k, z \in \mathbb{Z}_{p^\gamma}^*\} \leq \mathbb{Z}_{p^\gamma}^*$ subgroup.

<u>Claim:</u> $G_k = \frac{p-1}{d}$; $d=(k,p-1)$; <u>assuming $p>2$</u>

<u>Pf</u> Let $m \in \mathbb{Z}_{p^\gamma}$, $m \not\equiv 0\ (p)$ say $m = g^b$; g is the primitive root

If $z \equiv g^a\ (p^\gamma)$ then $z^k \equiv m\ (p^\gamma)$

$$\Leftrightarrow g^{ak} \equiv g^b\ (p^\gamma) \Leftrightarrow ak \equiv b\ (p^{\gamma-1}(p-1))$$

$\exists$, such a if and only if $p^{\gamma-1} | b$ and $(k,p-1)|b$

$$\Rightarrow |G_k| = \#\{b\ (\text{mod } p^{\gamma-1}(p-1));\ p^{\gamma-1}(k,p-1)|b\} =$$

$$= \frac{p^{\gamma-1}(p-1)}{p^{\gamma-1}(k,p-1)} = \frac{p-1}{d};\ d=(k,p-1).$$

Now, for given $s \geq 1$ let $\mathcal{N}_s = \#\{N \in \mathbb{Z}_{p^\gamma}^*;\ S(N)=s\}$

$= \#\{N \in \mathbb{Z}_{p^\gamma};\ \exists x_1,..,x_s:\ x_1^k+..+x_s^k \equiv N\ (p^\gamma)$ but $y_1^k+..+y_{s-1}^k \not\equiv N\ (p^\gamma)$ $\forall y_1,..,y_{s-1}\}$

E.g. $\mathcal{N}_1 = |G_k|$ so

$0 < \mathcal{N}_1 < \mathbb{Z}_{p^\gamma}^*$

For some s one may have $\mathcal{N}_s = 0$, but if $\mathcal{N}_s > 0$ then either $\mathcal{N}_{s+1} > 0$ or $\mathcal{N}_{s+2} > 0$

Indeed, if $x_1^k+..+x_s^k \equiv N\ (p^\gamma)$ then $x_1^k+\ +x_s^k+1 \equiv N+1\ (p^\gamma)$

$x_1^k+\ +x_s^k+1^k+1^k \equiv N+2\ (p^\gamma)$

and $p \nmid N+1$ or $p \nmid N+2$.

Also if $N_s > 0$ then $N_s \geq \frac{p-1}{d}$; let say we have

$\boxed{N_1, \dots,} N_m \neq 0$ so $s(N) \leq m$ for all $N \in \mathbb{Z}_{p^r}^{\times}$. $m = \max_s \{N_s \neq \emptyset\}$

Then $p^{r-1}(p-1) = N_1 + \dots + N_m \geq \frac{m+1}{2} \frac{p-1}{d}$

\# of non-empty N_s'

$$\Rightarrow \quad m+1 \leq \frac{2p^{r-1}\cancel{(p-1)}d}{\cancel{(p-1)}} = 2p^{r-1}(k, p-1) = 2p^{r-1}(k_0, p-1)$$

$$\leq 2p^{r-1}k_0 = 2p^{\tau}k_0 = 2k$$

as $k = p^{\tau}k_0 = p^{r-1}k_0$ and $(k, p-1) = (k_0, p-1)$.

$\Rightarrow m \leq 2k-1$.

Suppose $p = 2$

$g^{ka} \equiv g^b \; (2^{r-1}) \quad ka \equiv b \; (2^{r-1})$

- If k odd $\Leftrightarrow \tau = 0$, then $x^k \equiv N \pmod{2^r}$ solvable for $N \not\equiv 0 \, (2)$

$$\Rightarrow x^k + 1 \equiv N \pmod{2^r} \text{ solvable for } N \equiv 0 \, (2)$$

$\Rightarrow s \leq 3 < 4k$.

- If $\tau \geq 1$ so $k = 2^{\tau}k_0$, then for N odd,

we simply taking $x_j = 0,1$ for all $1 \leq j \leq s := 2^r - 1$

we have that (5.12) has a solution for all $0 < N < 2^r$.

Thus $s = 2^r - 1 = 2^{\tau+2} - 1 = 4k - 1$ works $\square$

Note This argument for $p=2$; and k-even looks very crude, but sharp for many k's.

Let $\Gamma(k) = \min\{ s;$ s.t. (5.12) has a solution with some $x_i \not\equiv 0 \pmod p$ for all p and $N\}$.

Then by Hardy-Littlewood; one has

k	3	4^*	5	6	7	8^*	...	16^*
$\Gamma(k)$	4	16	5	9	4	32		64

Summarizing, we have proved

Thm 8.1. If $s \geq 2^k + 1$ then $\mathfrak{S}(N) \geq C(k,s) > 0$ for all N.

Note We have that $\chi(p) > 0$ $\forall p$, if $s \geq 2k$ or $s \geq 4k$ and need the much stronger condition $s \geq 2^k+1$, for the conv. of $\prod_p \chi(p)$ i.e. for the estimate $|\chi(p) - 1| \lessapprox p^{-1-\delta}$.

This can be improved vastly!