AN IMPORTANT CONGRUENCE

BY HANSRAJ GUPTA

(From the Department of Mathematics, Government College, Hoshiarpur)

Received December 5, 1940

(Communicated by Dr. B. L. Bhatia, D.Sc.)

1. In a letter to Professor G. H. Hardy, Bauer gives a proof based on his identical congruences of my generalisation of Leudesdorf's Theorem. The object of this note is to give still another proof of the basic result in my paper.

2. In what follows, \( p \) denotes a prime \( \geq 2 \). All other small letters denote integers \( \geq 1 \), unless stated otherwise. \( S' (m, n) \) denotes the sum of the \( n \)th powers of the integers less than \( m \) and prime to it. \( \text{Pot}_p m \) denotes the index of the highest power of \( p \) which divides \( m \).

**Theorem.** For even values of \( r \),

\[
S' (p^n, r) = 0 \pmod{p^n} \text{ when } (p - 1) \nmid r,
\]

\[
= 0 \pmod{p^{n-1}} \text{ when } (p - 1) \mid r.
\]

First, when \( p \) is an odd prime.

If \( (p - 1) \nmid r \), let \( a \) be a primitive root of \( p^n \);

then

\[
S' (p^n, r) = a^r + a^{r^2} + a^{r^3} + \cdots + a^{r^k} (\pmod{p^n}),
\]

\[
= a^r \{a^r(p^n - 1) - 1\}/(a^r - 1) (\pmod{p^n}),
\]

\[
= 0 (\pmod{p^n});
\]

because \( \text{Pot}_p \{a^r(p^n - 1) - 1\} \geq u \), while \( \text{Pot}_p (a^r - 1) = 0 \).

If \( (p - 1) \mid r \), and \( r = k p^\beta (p - 1) \) where \( (k, p) = 1 \) and \( \beta > 0 \); let \( b \) be a primitive root of \( p^\beta + 1 \).

Then proceeding as before, we have

\[
S' (p^n, r) = b^r \{b^r(p^n - 1) - 1\}/(b^r - 1) (\pmod{p^n}),
\]

\[
= 0 (\pmod{p^{n-1}});\]

because \( \text{Pot}_p \{b^r(p^n - 1) - 1\} = u + \beta \), while \( \text{Pot}_p (b^r - 1) = \beta + 1 \).
Now, when \( p = 2 \), we have
\[
S'(2^r, r) = 1^r + 3^r + 5^r + \cdots + (2^u - 1)^r,
\]
\[
= 2 \{1^r + 3^r + 5^r + \cdots + (2^u - 1)^r\} \pmod{2^u},
\]
because \( r \) is even.

Since \( S'(2, r) = 1 \pmod{2} \), it is easily proved by induction that
\[
S'(2^u, r) = 2^u - 1 \pmod{2^u},
\]
\[
0 \pmod{2^{u-1}}.
\]

REFERENCES