STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1955-016 r

On theorems of Wolstenholme and Leudesdorf

H.J.A. Duparc and W. Peremans

1955

KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN - AMSTERDAM
Reprinted from Proceedings. Series A, 58, No. 4 and Indag. Math., 17, No. 4, 1955

MATHEMATICS

ON THEOREMS OF WOLSTENHOLME AND LEUDESDORF

BY

H. J. A. DUPARC AND W. PEREMANS

(Communicated by Prof. J. F. KOKSMA at the meeting of April 23, 1955)

Definitions. We say that a rational number u is divisible by a positive integer m if and only if there exist integers r and s such that $r/s = u$, $(s, m) = 1$ and $m|r$.

We say further that the rational numbers u and v are congruent mod m if $u - v$ is divisible by m. If u is a rational number, m a non-negative integer, and p a prime we shall write $p^m || u$ if and only if $p^m | u$ and $p^{m+1} \nmid u$.

By $\sum\limits_{a=1}^{M}{}'$ we shall mean a summation extended over all integers a with $1 \leqq a \leqq M$ and $(a, M) = 1$.

We consider the divisibility of $T_s(M) = \sum\limits_{a=1}^{M}{}' a^{-s}$ (for integral s and positive integral M) by powers of the prime factors of M. This problem has been treated by several authors (cf. WOLSTENHOLME [1], LEUDESDORF [2], CHOWLA [3 and 5], HARDY and WRIGHT [4], RAMA RAO [6]). The theorems we shall prove (theorem 1 and theorem 2) cover and extend the results of the above-mentioned papers. Theorem 1 treats the case that M is a power of a prime number, theorem 2 reduces the case that M is arbitrary to that of powers of primes. Contrary to the proofs given by some of the above-mentioned authors, our proofs will be completely elementary.

We begin with a simple and probably well-known lemma.

Lemma 1. If a, b and r are integers, if m is a positive integer, if $a \neq 0$ and if $(a, b) = 1$, we have

$$(a + b)^r \equiv \sum_{k=0}^{m-1} \binom{r}{k} a^{r-k} b^k \pmod{b^m}.$$

Proof: If $r \geqq 0$, the result is trivial. We therefore may suppose $r < 0$; put $r = -s$. We consider the polynomial

$$P(x) = (1 + x)^s \left\{ (1 + x)^{-s} - \sum_{k=0}^{m-1} \binom{-s}{k} x^k \right\},$$

in which, if expanded into a power series in x, the terms up to the term with exponent $m - 1$ vanish. So we have

$$P(ba^{-1}) \equiv 0 \pmod{b^m},$$

hence

$$1 \equiv (a+b)^s \sum_{k=0}^{m-1} \binom{-s}{k} a^{-s-k} b^k \pmod{b^m}.$$

Multiplying by $(a+b)^{-s}$ we get the required result.

Theorem 1. If p is a prime, if s is an integer and if n is a positive integer, then $T_s(p^n) = \sum_{a=1}^{p^n}{}' a^{-s}$ is divisible by p^k, where the integer $k=k(n)$ is determined in the following way:

i) if $2 \nmid s$, $p \neq 2$, $p-1 | s+1$, $p \nmid s$, then $k = 2n-1$;
ii) if $2 \nmid s$, $p-1 \nmid s+1$ or $p | s$, then $k = 2n$;
iii) if $2 \nmid s$, $p = 2$, then $k = 2n-2$;
iv) if $2 \mid s$, $p-1 | s$, then $k = n-1$;
v) if $2 \mid s$, $p-1 \nmid s$, then $k = n$.

In the cases i), iii) and iv) one has moreover $p^k || T_s(p^n)$. Further in the cases ii) and v), if $p^{k(m)} || T_s(p^m)$ for some positive integer m, one has $p^{k(n)} || T_s(p^n)$ for all $n \geqq 1$.

Proof: We shall first derive some auxiliary congruence relations. By lemma 1 one has

$$\begin{aligned} T_s(p^n) &= \sum_{a=1}^{p^n}{}' (p^n - a)^{-s} \equiv \\ &\equiv (-)^s \sum_{a=1}^{p^n}{}' (a^{-s} + s\, p^n a^{-(s+1)} + \tfrac{1}{2} s(s+1) p^{2n} a^{-(s+2)} + \\ &\qquad + \tfrac{1}{6} s(s+1)(s+2) p^{3n} a^{-(s+3)}) \pmod{p^{4n}}, \end{aligned}$$

hence

$$(1) \quad \begin{cases} (1-(-)^s) T_s(p^n) \equiv (-)^s (s p^n T_{s+1}(p^n) + \tfrac{1}{2} s(s+1) p^{2n} T_{s+2}(p^n) + \\ + \tfrac{1}{6} s(s+1)(s+2) p^{3n} T_{s+3}(p^n)) \pmod{p^{4n}}. \end{cases}$$

Again by lemma 1 one has

$$\begin{aligned} T_s(p^{n+1}) &= \sum_{a=1}^{p^n}{}' \sum_{k=0}^{p-1} (kp^n + a)^{-s} \equiv \\ &\equiv \sum_{a=1}^{p^n}{}' \sum_{k=0}^{p-1} (a^{-s} - skp^n a^{-(s+1)} + \tfrac{1}{2} s(s+1) k^2 p^{2n} a^{-(s+2)} + \\ &\qquad - \tfrac{1}{6} s(s+1)(s+2) k^3 p^{3n} a^{-(s+3)}) \pmod{p^{4n}}; \end{aligned}$$

hence

$$(2) \quad \begin{cases} T_s(p^{n+1}) \equiv p\, T_s(p^n) - \tfrac{1}{2} s(p-1) p^{n+1} T_{s+1}(p^n) + \\ + \tfrac{1}{12} s(s+1)(p-1)(2p-1) p^{2n+1} T_{s+2}(p^n) + \\ - \tfrac{1}{24} s(s+1)(s+2)(p-1)^2 p^{3n+2} T_{s+3}(p^n) \pmod{p^{4n}}. \end{cases}$$

From (1) and (2) we obtain by elimination of $T_{s+1}(p^n)$:

$$(3) \quad \begin{cases} T_s(p^{n+1}) \equiv \{1 + \tfrac{1}{2}(1-(-)^s)(p-1)\}\, p\, T_s(p^n) + \\ + \tfrac{1}{6} s(s+1)(p-1) p^{2n+1} (p+1) T_{s+2}(p^n) + \\ - \tfrac{1}{24} s(s+1)(s+2)(p-2)(p-1) p^{3n+1} (p+1) T_{s+3}(p^n) \pmod{p^{4n}}. \end{cases}$$

For even s we get from (3)

$$(4)\quad T_s(p^{n+1}) \equiv p\,T_s(p^n) + \tfrac{1}{6}s(s+1)(p-1)\,p^{2n+1}(p+1)\,T_{s+2}(p^n) \pmod{p^{3n+1}}.$$

For odd s we obtain replacing s by $s+2$ in formula (1):

$$-2T_{s+2}(p^n) \equiv (s+2)\,p^n\,T_{s+3}(p^n) \pmod{p^{2n}}.$$

Substituting this result in (3) we obtain for odd s:

$$(5)\quad \begin{cases} 2T_s(p^{n+1}) \equiv \\ \equiv 2p^2\,T_s(p^n) - \tfrac{1}{12}s(s+1)(s+2)(p-1)\,p^{3n+2}(p+1)T_{s+3}(p^n) \pmod{p^{4n}}. \end{cases}$$

If $p-1\,|\,s$ we have by FERMAT's theorem $a^{-s} \equiv 1 \pmod{p}$ for $a=1, \ldots, p-1$, so $\sum\limits_{a=1}^{p-1} a^{-s} \equiv -1 \pmod{p}$. If $p-1 \nmid s$ and if g denotes a primitive root mod p we have $g^{-s} \not\equiv 1 \pmod{p}$ and $\sum\limits_{a=1}^{p-1} a^{-s} \equiv \sum\limits_{a=1}^{p-1} (ga)^{-s} \equiv g^{-s} \sum\limits_{a=1}^{p-1} a^{-s}$ $\pmod{p}$, so $\sum\limits_{a=1}^{p-1} a^{-s} \equiv 0 \pmod{p}$. This yields the result

$$(6)\qquad T_s(p) = \sum_{a=1}^{p-1} a^{-s} \begin{cases} \equiv 0 \pmod{p} \text{ if } p-1 \nmid s \\ \equiv -1 \pmod{p} \text{ if } p-1\,|\,s. \end{cases}$$

Using lemma 1 with $m=2$ one finds for odd s

$$T_s(p) = \sum_{a=1}^{p-1} (p-a)^{-s} \equiv -T_s(p) - s\,p\,T_{s+1}(p) \pmod{p^2},$$

hence using (6) with $s+1$ instead of s one obtains for odd s

$$2\,T_s(p) \equiv 0 \pmod{p^2} \text{ if } p-1 \nmid s+1,$$
$$2\,T_s(p) \equiv sp \pmod{p^2} \text{ if } p-1\,|\,s+1.$$

Consequently if $p \neq 2$ we find for odd s

(7) if $p-1 \mid s+1$ and $p \nmid s$, then $p \,||\, T_s(p)$,

(8) if $p-1 \nmid s+1$ or $p \mid s$, then $p^2 \,|\, T_s(p)$.

We now proceed to prove the assertions of the theorem. By mathematical induction we find for odd s and p using (5) and (7):

(i) if $p-1 \mid s+1$ and $p \nmid s$, then $p^{2n-1} \,||\, T_s(p^n)$.

Similarly we find for odd s and odd p using (5) and (8):

(ii) if $p-1 \nmid s+1$ or $p \mid s$, then $p^{2n} \mid T_s(p^n)$.

For odd s and $p=2$ we deduce from (5) and (6):

(iii) $2^{2n-2} \,||\, T_s(2^n)$.

For even s one finds using (4) and (6):

(iv) if $p-1 \mid s$, then $p^{n-1} \,||\, T_s(p^n)$,

(v) if $p-1 \nmid s$, then $p^n \,|\, T_s(p^n)$.

If in case v) for some m we have $p^m \,||\, T_s(p^m)$, it follows from (4) that

$p^{m+1}||T_s(p^{m+1})$ and if $m \geqq 2$ also $p^{m-1}||T_s(p^{m-1})$ hence $p^n||T_s(p^n)$ for all $n \geqq 1$ (in this case $p=3$ is excluded, so the factor 3 in the denominator in (4) is harmless).

To deduce a similar result in case ii) a further discussion is necessary. If we apply lemma 1 with $m=5$ instead of $m=4$, we see that the congruence relations (1) and (2), hence also (5) (with an additional term of the form $cp^{4n}T_{s+4}(p^n)$ where c is an integer) hold mod p^{5n}. Since in case ii) the integers p and $s+4$ are odd, we have $p^{2n-1}|T_{s+4}(p^n)$, consequently $p^{6n-1}|cp^{4n}T_{s+4}(p^n)$. Further in case ii) either $p>3$ or $p=3$ and $3|s$. So in this case, as $3n+2 \geqq 2n+3$, $6n-1 \geqq 2n+3$ and $5n \geqq 2n+3$, we have by (5)

$$(9) \qquad 2T_s(p^{n+1}) \equiv 2p^2\, T_s(p^n) \pmod{p^{2n+3}}.$$

If in case ii) for some m we have $p^{2m}||T_s(p^m)$, it follows from (9) that $p^{2m+2}||T_s(p^{m+1})$ and if $m \geqq 2$ also $p^{2m-2}||T_s(p^{m-1})$, so $p^{2n}||T_s(p^n)$ for all $n \geqq 1$. This completes the proof of theorem 1.

Theorem 2. a) If M is a positive integer, if p is a prime and n a positive integer such that $p^n||M$, if s is an integer and if k is the exponent introduced in theorem 1, then $p^k|T_s(M) = \sum_{a=1}^{M}{}' a^{-s}$.

b) Moreover if in cases i), iii) or iv) of theorem 1 one has $p \nmid \varphi(Mp^{-n})$ (i.e. if for every prime $q|Mp^{-n}$ one has $p \nmid q-1$), then $p^k||T_s(M)$.

c) If on the contrary in cases i), iii) or iv) of theorem 1 one has $p|\varphi(Mp^{-n})$, then $p^{k+1}|T_s(M)$.

Proof: Put $M=p^n m$. Every positive integer a relatively prime to M and $<M$ can be written uniquely in the form $a=u\,p^n+vm$, where u and v are integers and $0<v<p^n$. We then have $(u,m)=1$ and $p\nmid v$. Furthermore for every integer v satisfying $p\nmid v$ and $0<v<p^n$ the set of those integers u for which up^n+vm is relatively prime to M and $<M$ constitutes a reduced residue set mod m.

First suppose s even. Then by lemma 1 one has

$$T_s(M) = \sum_{u,v} (u\,p^n + v\,m)^{-s} \equiv \sum_{u,v} m^{-s}\, v^{-s} = \varphi(m)\, m^{-s} \sum_{v=1}^{p^n}{}' v^{-s} (\text{mod } p^n).$$

By theorem 1 we have $p^k|T_s(p^n)$ and $k \leqq n$, so $p^k|T_s(M)$.

Now suppose s odd. Again by lemma 1 one has

$$\begin{aligned} 2T_s(M) &= \sum_{a=1}^{M}{}' a^{-s} + \sum_{a=1}^{M} (M-a)^{-s} = \\ &= \sum_{u,v} (u\,p^n + vm)^{-s} + \sum_{u,v} ((p^n - v)\, m - u\, p^n)^{-s} \equiv \\ &\equiv \sum_{u,v} (m^{-s}\, v^{-s} + m^{-s}\,(p^n - v)^{-s} - sm^{-(s+1)}\, p^n\, uv^{-(s+1)} + \\ &+ sm^{-(s+1)}\, p^n\, u\,(p^n - v)^{-(s+1)}) = 2\,\varphi(m)\, m^{-s}\, T_s(p^n) + \\ &+ sm^{-(s+1)}\, p^n \sum_{u,v} u\,((p^n - v)^{-(s+1)} - v^{-(s+1)})\ (\text{mod } p^{2n}). \end{aligned}$$

Since $s+1$ is even one has

$$p^n = (p^n - v) + v \mid (p^n - v)^{-(s+1)} - v^{-(s+1)}.$$

In either of the cases $p \neq 2$ and $p=2$ one deduces from $p^k | T_s(p^n)$ that $p^k | T_s(M)$.

It is easily verified that in cases i), iii) and iv) of theorem 1 if $p \nmid \varphi(m)$ we have $p^k || T_s(M)$ and if $p | \varphi(m)$ we have $p^{k+1} | T_s(M)$. This completes the proof of theorem 2.

Remark. If $p=2$ the condition $2 | \varphi(m)$ always holds, except if $m=1$ (i.e. except if M is a power of 2); moreover we then have cases iii) or iv) of theorem 1.

In two corollaries we formulate the conditions under which $M^2 | T_s(M)$ and $M | T_s(M)$ have been found to hold.

Corollary 1. If M is an odd positive integer, if s is an odd integer and if for every prime p satisfying $p^n || M$ with $n \geqq 1$, $p-1 | s+1$ and $p \nmid s$, also $p | \varphi(Mp^{-n})$, then $M^2 | T_s(M)$.

Corollary 2. If M is a positive integer $\neq 2$, if s is an integer and if in the case that s is even for every prime satisfying $p^n || M$ with $n \geqq 1$ and $p-1 | s$ also $p | \varphi(Mp^{-n})$, then $M | T_s(M)$.

We now discuss the results of the six above-mentioned papers and show briefly how their results are contained in ours.

Wolstenholme [1; 1862] proved for $p > 3$ the result $p^2 | T_1(p)$, which obviously is a special case of our theorem 1, ii.

Leudesdorf [2; 1889] proved the following two results:

Suppose s odd, $M = p^n m$ and $p \nmid m$.

If $p > 2$, and $p | s$ or $p-1 \nmid s+1$, then $p^{2n} | T_s(M)$.
If $p=2$ and $m \neq 1$, then $p^{2n-1} | T_s(M)$.

His first result is equivalent to our assertions 1, ii and 2a, wnereas his second result is equivalent to our assertions 1, iii; 2a and 2c.

Chowla [3; 1930] proved the following two results:

If $p > 3$, then $p^{2n} | T_1(p^n)$,
If $p=3$, then $p^{2n-1} | T_1(p^n)$.

These results follow from our assertions 1, ii and 1, i respectively.

Hardy and Wright [4; 1933] proved the following five results:

If $2 \nmid M$, $3 \nmid M$, then $M^2 | T_1(M)$ (a consequence of 1, ii and 2a).
If $2 \nmid M$, $3 | M$, then $\frac{1}{3} M^2 | T_1(M)$ (a consequence of 1, i; 1, ii and 2a).
If $2 | M$, $3 \nmid M$, and M is not a power of 2, then $\frac{1}{2} M^2 | T_1(M)$ (a consequence of 1, i; 1, iii; 2a and 2c).
If $2 | M$, $3 | M$, then $\frac{1}{6} M^2 | T_1(M)$ (a consequence of 1, i; 1, ii; 1, iii; 2a and 2c).
If M is a power of 2, then $\frac{1}{4} M^2 | T_1(M)$ (a consequence of 1, iii and 2a).

Chowla [5; 1934] proved

If $2 \nmid$M, $3 \nmid M$, then $M^2 | T_1(M)$.

This result is contained in the results of Hardy and Wright [4].

Rama Rao [6; 1937] proved the following two results:
Let s be odd, suppose that every prime p with $p-1|s+1$ satisfies $p \nmid \frac{M}{(M,s)}$. Then $M^2|T_s(M)$.
Suppose that every prime p with $p-1|s$ satisfies $p \nmid M$. Then $M|T_s(M)$.

Also here the results can be easily derived from our theorems 1 and 2, but they are also straightforward consequences of our corollaries 1 and 2 to theorem 2. We remark that in both cases M is odd. Rama Rao's conditions imply that no primes p exist for which $p^n||M$ with $n \geqq 1$, $p-1|s+1$ and $p \nmid s$, respectively $p^n||M$ with $n \geqq 1$, $p-1|s$, $2|s$. Therefore our corollaries yield immediately his results.

Finally we thank Dr. C. G. Lekkerkerker for valuable remarks and suggestions.

Note added in proof.

After the above paper was communicated the authors learned the existence of the paper of L. Carlitz (A note on Wolstenholme's theorem, Amer. Math. Monthly **61** (1954), 174–176), dealing with another generalization of Leudesdorf's theorem. Although his results are not covered by ours, they can be proved easily by our methods.

In his paper he considered sums of the following type

$$T_s(M, k) = \sum_{a=1}^{M}{}' (kM+a)^{-s},$$

properties of which by our method might be proved as follows.

If s is odd and if $M^e\,|\,2k+1$ for some non-negative integer e we find, applying lemma 1 with $m=e+2$,

$$T_s(M, k) \equiv \sum_{j=1}^{e+1} \binom{-s}{j} M^j k^j T_{s+j}(M) \pmod{M^{e+2}}$$

and similarly

$$T_s(M, k) = \sum_{a=1}^{M}{}' ((k+1)M-a)^{-s} \equiv \sum_{j=0}^{e+1} (-)^{j+s} \binom{-s}{j} M^j (k+1)^j T_{s+j}(M) \pmod{M^{e+2}}.$$

By adding we get

$$2\,T_s(M, k) \equiv \sum_{j=1}^{e+1} \binom{-s}{j} M^j T_{s+j}(M) \,\{k^j + (-)^{j+1}(k+1)^j\} \pmod{M^{e+2}}.$$

Using the fact that $2k+1\,|\,k^j+(-)^{j+1}(k+1)^j$, we get

$$2\,T_s(M, k) \equiv -s(2k+1)MT_{s+1}(M) \pmod{M^{e+2}}.$$

Hence

$$2\,T_s(M, k) \equiv 0 \pmod{M^{e+1}}.$$

Moreover if $M\,|\,s$ or if $M \neq 2$ and for every prime p satisfying $p^n\,||\,M$ with $n \geqq 1$ and $p-1\,|\,s+1$ also $p\,|\,\varphi(Mp^{-n})$, we get using corollary 2

$$2\,T_s(M, k) \equiv 0 \pmod{M^{e+2}}.$$

So we find that if M and s are odd, $T_s(M,k)$ is divisible by an arbitrarily high power of M, if k is suitably chosen. For $s=1$ this is the result of Carlitz.

If s is even, we get in a similar way

$$2T_s(M,k) \equiv 2T_s(M)+sMT_{s+1}(M) \pmod{M^2}.$$

If $M \neq 2$, by corollary 2 we have $M \mid T_{s+1}(M)$, and so $2T_s(M,k) \equiv \equiv 2T_s(M) \pmod{M^2}$.

In this case we only find that if M is odd and $M \mid T_s(M)$, $M^2 \nmid T_s(M)$, also $M \mid T_s(M,k)$ and $M^2 \nmid T_s(M,k)$.

It is obviously possible to get refinements of these results in a way similar to that used in this paper.

Note on two papers of N. ELJOSEPH.

In reading the second proof the authors found that results similar to theirs have been obtained by N. ELJOSEPH (Rev. Lemat. **4**, 9–15 and 59–61 (1950)). In a further note they intend to compare his theorems – proved by different methods – with the above results.

Mathematisch Centrum,
Amsterdam.

REFERENCES

1. WOLSTENHOLME, J., On certain properties of prime numbers, Quart. J. of Math. **5**, 35–39 (1862).
2. LEUDESDORF, C., Some results in the elementary theory of numbers, Proc. London Math. Soc. (1) **20**, 199–212 (1889).
3. CHOWLA, S. D., A generalization of a theorem of WOLSTENHOLME, J. London Math. Soc. **5**, 158–160 (1930).
4. HARDY, G. H. and E. M. WRIGHT, LEUDESDORF's extension of WOLSTENHOLME's theorem, J. London Math. Soc. **9**, 38–41 (1934).
5. CHOWLA, S. D., LEUDESDORF's generalization of WOLSTENHOLME's theorem, J. London Math. Soc. **9**, 246 (1934).
6. RAMA RAO, N., An extension of LEUDESDORF's theorem, J. London Math. Soc. **12**, 247–250 (1937).