Canad. Math. Bull. Vol. **23** (3), 1980

LEAST POSITIVE RESIDUES AND THE QUADRATIC CHARACTER OF TWO

BY
KENNETH H. ROSEN

Let $r_j^{(t)}$ be the least positive residue modulo $2^t k$ of $(2j-1)h$. Define u_t to be the number of $r_j^{(t)}$ with $1 \le j \le 2^{t-2}k$ such that $2^{t-1}k < r_j^{(t)} < 2^t k$. At the Special Session in Combinatorial Number Theory at the 1977 Summer AMS Meeting Szekeres [2] asked for a simple proof that if $(h, 2k) = 1$, then

$$u_4 \equiv \begin{cases} 0 \pmod 4 & \text{if } h \equiv \pm 1 \pmod 8 \\ 2 \pmod 4 & \text{if } h \equiv \pm 3 \pmod 8. \end{cases}$$

Here a simple proof will be given for the following equivalent result.

THEOREM 1. *If* $(h, 2k) = 1$, *then if* $t \ge 4$

$$u_t \equiv \begin{cases} 0 \pmod 4 & \text{if } h \equiv \pm 1 \pmod 8 \\ 2 \pmod 4 & \text{if } h \equiv \pm 3 \pmod 8. \end{cases}$$

To prove Theorem 1, one first expresses u_t as a sum.

LEMMA 2. *If* $(h, 2k) = 1$, *then* $u_t = S_1 - 2S_2$, *where*

$$S_1 = \sum_{j=1}^{2^{t-2}k} \left[\frac{(2j-1)h}{2^{t-1}k}\right] \quad \text{and} \quad S_2 = \sum_{j=1}^{2^{t-2}k} \left[\frac{(2j-1)h}{2^t k}\right].$$

Proof. Lemma 2 follows from the fact that the difference

$$\left[\frac{(2j-1)h}{2^{t-1}k}\right] - 2\left[\frac{(2j-1)h}{2^t k}\right]$$

is zero when $0 < r_j^{(t)} < 2^{t-1}k$ and is one when $2^{t-1}k < r_j^{(t)} < 2^t k$.

The following easily verified identities are useful.

$$S_1 = \sum_{j=1}^{2^{t-1}k} \left[\frac{jh}{2^{t-1}k}\right] - \sum_{j=1}^{2^{t-2}k} \left[\frac{jh}{2^{t-2}k}\right] \quad \text{and} \tag{1}$$

$$S_2 = \sum_{j=1}^{2^{t-1}k} \left[\frac{jh}{2^t k}\right] - \sum_{j=1}^{2^{t-2}k} \left[\frac{jh}{2^{t-1}k}\right]. \tag{2}$$

Received by the editors March 29, 1978 and in revised form, November 23, 1978 and February 1, 1979.

To evaluate S_1 one uses

LEMMA 3. *If* $(m, h)=1$, *then*

$$\sum_{j=1}^{m}\left[\frac{jh}{m}\right]=h+\frac{(h-1)(m-1)}{2}.$$

Proof. Let $\{x\}=x-[x]$. Then

$$\sum_{j=1}^{m-1}\left[\frac{jh}{m}\right]=\sum_{j=1}^{m-1}\left(\frac{jh}{m}-\left\{\frac{jh}{m}\right\}\right)=\frac{h}{m}\frac{m(m-1)}{2}-\sum_{\ell=1}^{m-1}\frac{\ell}{m}=\frac{(h-1)(m-1)}{2}.$$

The second equality is true because as j runs through a full set of residues mod m, so does jh. Lemma 3 follows by addition of h to the first and last members of this string of equalities.

Applying Lemma 3 to (1), one concludes that

$$S_1=\tfrac{1}{2}(h-1)2^{t-2}k \tag{3}$$

To deal with S_2, it is first necessary to prove

LEMMA 4. *If* $(h, 2k)=1$ *and if* c *is a nonnegative integer, then*

$$\sum_{j=1}^{2^ck}\left[\frac{jh}{2^{c+1}k}\right]=-\sum_{j=1}^{(h-1)/2}\left[\frac{2^{c+1}kj}{h}\right]+2^ck\left(\frac{h-1}{2}\right). \tag{4}$$

Proof. Count the number of terms of the sum on the left hand side of (4) that equal a fixed number n. If $1\leqq n\leqq(h-3)/2$ then n occurs exactly

$$\left[\frac{2^{c+1}k(n+1)}{h}\right]-\left[\frac{2^{c+1}kn}{h}\right]$$

times. The number $(h-1)/2$ occurs exactly

$$2^ck-\left[\frac{2^{c+1}k(h-1)}{2h}\right]$$

times. Hence

$$\begin{aligned}\sum_{j=1}^{2^ck}\left[\frac{jh}{2^{c+1}k}\right]&=\sum_{n=1}^{(h-3)/2}n\left(\left[\frac{2^{c+1}(n+1)k}{h}\right]-\left[\frac{2^{c+1}nk}{h}\right]\right)\\&\quad+\frac{h-1}{2}\left(2^ck-\left[\frac{2^{c+1}k(h-1)}{2h}\right]\right)\\&=-\sum_{j=1}^{(h-1)/2}\left[\frac{2^{c+1}kj}{h}\right]+2^ck\left(\frac{h-1}{2}\right).\end{aligned}$$

https://doi.org/10.4153/CMB-1980-050-8 Published online by Cambridge University Press

From (2) and Lemma 4, one obtains

$$S_2 = \left(\frac{h-1}{2}\right)2^{t-2}k + \sum_{j=1}^{(h-1)/2}\left[\frac{2^{t-1}kj}{h}\right] - \sum_{j=1}^{(h-1)/2}\left[\frac{2^t kj}{h}\right]. \tag{5}$$

The following classical result which is proved in Bachmann [1] relates the sums on the right hand side of (5) to the Jacobi symbol.

LEMMA 5. $(h, 2q) = 1$, *then*

$$\sum_{j=1}^{(h-1)/2}\left[\frac{2qj}{h}\right] \equiv \frac{1}{2}\left(\left(\frac{q}{h}\right)-1\right) \pmod 2$$

where (q/h) *is the Jacobi symbol.*

Consequently, from (3), (5) and Lemma 5, one obtains

$$u_t = S_1 - 2S_2 = -\tfrac{1}{2}(h-1)2^{t-2}k + \left[1-\left(\frac{2}{h}\right)\right] \pmod 4. \tag{6}$$

Theorem 1 now follows from (6), by noting that

$$\left(\frac{2}{h}\right) = \begin{cases} 1 & \text{if } h \equiv \pm 1 \pmod 8 \\ -1 & \text{if } h \equiv \pm 3 \pmod 8. \end{cases}$$

When $t-2$ or $t=3$ note that from (6) one can prove

THEOREM 6. *If* $(h, 2k) = 1$, *then*

$$u_2 \equiv \begin{cases} 0 \pmod 4 & \text{if } h \equiv 1 \pmod 8, \text{ or } h \equiv 3 \pmod 8 \text{ and } k \text{ is odd,} \\ & \text{or } h \equiv 7 \pmod 8 \text{ and } k \text{ is even} \\ 2 \pmod 4 & \text{if } h \equiv 5 \pmod 8, \text{ or } h \equiv 3 \pmod 8 \text{ and } k \text{ is even,} \\ & \text{or } h \equiv 7 \pmod 8 \text{ and } k \text{ is odd} \end{cases}$$

and

$$u_2 \equiv \begin{cases} 0 \pmod 4 & \text{if } h \equiv 1 \pmod 8 \\ 3k+2 \pmod 4 & \text{if } h \equiv 3 \pmod 8 \\ 2k+2 \pmod 4 & \text{if } h \equiv 5 \pmod 8 \\ k \pmod 4 & \text{if } h \equiv 7 \pmod 8. \end{cases}$$

NOTE ADDED ON SEPTEMBER 20, 1978. A different proof of Theorem 1 has been given by G. Szekeres and B. Richmond in their interesting paper, The Taylor Coefficients of Certain Infinite Products, Acta Sci. Math. Szeged 40 (1978) 347–369 as a commemorative article for Professor Turán. Szekeres has remarked, and the author agrees, that it would be desirable to prove Theorem 1 as a consequence of Gauss' Lemma.

ACKNOWLEDGEMENT. The author would like to thank the referee and Prof. Ronald Evans for their helpful comments.

REFERENCES

1. P. Bachmann, *Die Elemente der Zahlentheorie*, Teubner, Leipzig, 1892, (reprint: Chelsea, New York, 1968), p. 144–148.

2. C. Long, Problem List, *Combinatorial Number Theory*, Notices of the American Mathematical Society, **25** (1978), p. 145.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF COLORADO
BOULDER, COLORADO 80309 USA

AUTHOR'S CURRENT ADDRESS:
DEPARTMENT OF MATHEMATICS
THE UNIVERSITY OF MAINE
OROND, MAINE, 04469 USA