ON COMPLETE RESIDUE SETS

By T. VIJAYARAGHAVAN (*Waltair*) and S. CHOWLA (*Ludhiana*)

[Received 8 February 1944; in revised form 12 December 1947]

1. THE following result is known:†

If q be an odd prime, $r_1, r_2,..., r_q$ and $s_1, s_2,..., s_q$ be two complete sets of residues (mod q), *then $r_1 s_1, r_2 s_2,..., r_q s_q$ cannot be a complete set of residues* (mod q).

To prove the result we follow Pólya in supposing the contrary. We can take $r_q \equiv 0 \pmod q$ and then it is easy to deduce that $s_q \equiv 0 \pmod q$. We have then (to modulus q)

$$1.2.3...(q-1) \equiv r_1 r_2 ... r_{q-1} \equiv s_1 s_2 ... s_{q-1}$$
$$\equiv r_1 s_1 . r_2 s_2 ... r_{q-1} s_{q-1} \equiv \{1.2.3...(q-1)\}^2$$

which is impossible since (by Wilson's theorem)

$$1.2.3...(q-1) \equiv -1 \pmod q.$$

We prove in this section that the above result is true not only for odd prime values of q but for all values of $q > 2$.

Suppose now that the result is not true for a composite value of q. It is shown below that there arises a contradiction. Let p be a prime divisor of q, and $q/p = N$. We see that $r_t s_t$ is a multiple of p for precisely N values of t and that $r_t s_t$ is prime to p for the remaining $q-N$ values of t. Since in each of the two sets $r_1, r_2,..., r_q$ and $s_1, s_2,..., s_q$ there are precisely $q-N$ numbers that are prime to p, we deduce at once that, whenever $r_t s_t$ is a multiple of a prime number p that divides q, then r_t and s_t are both multiples of p. If we now make the further assumption that q is a multiple of p^2 as well, then we see that either $r_t s_t$ is prime to p or is a multiple of p^2 and that therefore there is no value of t for which $r_t s_t \equiv p \pmod q$.

This contradiction proves the result when q is divisible by the square of a prime. It remains to prove the result when q is a product of two or more distinct primes. In this case we take an odd prime divisor p of q and consider the values of t for which $r_t s_t$ is a multiple of N $(= p/q)$. There are precisely p such values of t; let these values

† A. Hurwitz, *Nouv. Ann.* Serie 3, 1 (1882), 389. See also G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, vol. ii, chap. 8, problem 245, p. 158 and p. 379.

of t be $t_1, t_2, \ldots, t_p$. Now in each of the two sets $r_1, r_2, \ldots, r_q$ and $s_1, s_2, \ldots, s_q$ there are precisely p numbers that are multiples of N and precisely $q-p$ numbers that are not multiples of N. It follows that each of the numbers $r_{t_1}, r_{t_2}, \ldots, r_{t_p}$ is a multiple of N. Moreover, these p numbers in some order or other are congruent to $N, 2N, \ldots, pN$ $(\text{mod}\, q)$ and are therefore incongruent $(\text{mod}\, p)$. The same remarks apply to $s_{t_1}, s_{t_2}, \ldots, s_{t_p}$ and to $r_{t_1}s_{t_1}, r_{t_2}s_{t_2}, \ldots, r_{t_p}s_{t_p}$. But according to the result of A. Hurwitz this is not possible. This completes the proof when q is a product of two or more distinct primes. Hence we have the result:

If $r_1, r_2, \ldots, r_q$ and $s_1, s_2, \ldots, s_q$ are two complete residue sets $(\text{mod}\, q)$, *where $q > 2$, then $r_1 s_1, r_2 s_2, \ldots, r_q s_q$ is not a complete residue set* $(\text{mod}\, q)$.

2. The main result of this note is given in this section.

We consider the following problem. Suppose that n is a positive integer, $\phi(n) = h$, and $r_1, r_2, \ldots, r_h$ are all prime to n and incongruent $(\text{mod}\, n)$. Such a set may be called a complete *primitive* residue set $(\text{mod}\, n)$. Suppose now that $r_1, r_2, \ldots, r_h$ and $s_1, s_2, \ldots, s_h$ are two such sets. Can it happen that the product set $r_1 s_1, r_2 s_2, \ldots, r_h s_h$ is also a complete primitive residue set? It is easy to see from the proof of the result of A. Hurwitz that the product set cannot be a complete primitive residue set if n is a prime number > 2; it is easy to verify that the same is the case if $n = 4, 6, 9$, etc. But we see from the following table that for some other values of n the product set can be a complete primitive residue set provided that the first two sets are suitably ordered.

	$n = 2$	$n = 8$	$n = 12$	$n = 15$
r_t	1	1, 3, 5, 7	1, 5, 7, 11	1, 2, 4, 7, 8, 11, 13, 14
s_t	1	1, 5, 7, 3	1, 7, 11, 5	1, 4, 14, 2, 11, 7, 13, 8
$r_t s_t$ reduced $(\text{mod}\, n)$	1	1, 7, 3, 5	1, 11, 5, 7	1, 8, 11, 14, 13, 2, 4, 7

It turns out that there is a neat answer to the query: 'Which numbers have the property considered above?' The answer is given by the following

THEOREM. *If $n = 2$ or has no primitive root, then there exist suitable complete primitive residue sets $r_1, r_2, \ldots, r_h$ and $s_1, s_2, \ldots, s_h$ such that $r_1 s_1, r_2 s_2, \ldots, r_h s_h$ too is a complete primitive residue set.*

Remark. If $n > 2$ and has a primitive root g, then it is easy to show that n has not the property under consideration. For otherwise we should have to modulus n

$$g.g^2...g^h \equiv r_1 r_2...r_h \equiv s_1 s_2...s_h \equiv r_1 s_1 r_2 s_2...r_h s_h \equiv (g.g^2...g^h)^2,$$

which is a contradiction since $n > 2$ and

$$g.g^2...g^h \equiv g^{wh+\frac{1}{2}h} \equiv g^{\frac{1}{2}h} \equiv -1 \pmod{n},$$

where $w = \frac{1}{2}h$ is an integer.

LEMMA. *If m and n are prime to each other and the conclusion of the theorem is true for m and n, then it is true for mn.*

Let $\phi(m) = h$, $\phi(n) = k$, and $r_1, r_2,..., r_h$, $s_1, s_2,..., s_h$ and $r_1 s_1$, $r_2 s_2,..., r_h s_h$ be three complete primitive residue sets $(\operatorname{mod} m)$, and let $\rho_1, \rho_2,..., \rho_k$, $\sigma_1, \sigma_2,..., \sigma_k$, and $\rho_1 \sigma_1, \rho_2 \sigma_2,..., \rho_k \sigma_k$ be three such sets $(\operatorname{mod} n)$. Let $\{\alpha, \beta\}$ denote the residue class $x \pmod{mn}$, where x is such that $x \equiv \alpha \pmod{m}$, $x \equiv \beta \pmod{n}$, and let $R_1, R_2,..., R_{hk}$ be a complete primitive residue set $(\operatorname{mod} mn)$. If $R_a = \{r_b, \rho_c\}$, then we take $S_a = \{s_b, \sigma_c\}$ $(a = 1, 2, 3,..., hk)$. It is easy to verify that $S_1, S_2,..., S_{hk}$ and $R_1 S_1, R_2 S_2,..., R_{hk} S_{hk}$ are two complete primitive residue sets $(\operatorname{mod} mn)$, and this proves the lemma.

The theorem is first proved for values of n that belong to a set S, where S consists precisely of the five following forms:

(1) $n = 2^\lambda$, where $\lambda \neq 2$;

(2) $n = 2^\lambda m$, where $\lambda \geqslant 2$ and m is a power of any odd prime;

(3) $n = p^\lambda q^\mu$, where p and q are any pair of distinct odd primes;

(4) $n = 4M$, where M is any member of the form (3) mentioned just above;

(5) $n = p^\lambda q^\mu r^\nu$, where p, q, r are any three distinct odd primes.

It may be remarked here that, if a number n has no primitive root, then either it is a member of S or can be represented as a product of two or more mutually prime members of S. In view of the lemma already proved it follows immediately that the theorem of this note is completely proved when it has been proved for all values of n that belong to S.

(I) $n = p^\lambda q^\mu$. Let g be a primitive root of p^λ, $\phi(p^\lambda) = 2M$, g' a primitive root of q^μ and $\phi(q^\mu) = 2N$. We denote by $\{\alpha, \beta\}$ the residue class x which is such that

$$x \equiv g^\alpha \pmod{p^\lambda}, \qquad x \equiv g'^\beta \pmod{q^\mu}.$$

It should be noticed that by giving to α the values 0, 1, 2,..., $2M-1$ and to β the values 0, 1, 2,..., $2N-1$ we get all the $4MN$ primitive residue classes (mod $p^\lambda q^\mu$). Also

$$\{\alpha, \beta\} = \{\alpha+2M, \beta\} = \{\alpha, \beta+2N\}$$

for every pair of values α, β; the converse is also true, i.e. if

$$\{\alpha, \beta\} = \{\alpha', \beta'\},$$

then $\alpha \equiv \alpha'$ (mod $2M$) and $\beta \equiv \beta'$ (mod $2N$). Finally, if $x = \{\alpha, \beta\}$ and $y = \{\alpha', \beta'\}$, then $xy = \{\alpha+\alpha', \beta+\beta'\}$ for all $\alpha, \beta, \alpha', \beta'$. These properties enable us to solve the problem under consideration. Let $r_1, r_2,..., r_h$ (where $h = 4MN$) be a complete set of primitive residues (mod n). We show below how a complete set of primitive residue classes $s_1, s_2,..., s_h$ can be chosen in such a way that $r_1 s_1, r_2 s_2,..., r_h s_h$ is also a complete primitive residue set.

If $r_t = \{\alpha, \beta\}$ $(1 \leqslant \alpha \leqslant M; 1 \leqslant \beta \leqslant N)$,
then s_t is to be taken equal to $\{\alpha, \beta\}$;

if $r_t = \{\alpha, \beta\}$ $(M < \alpha \leqslant 2M; 1 \leqslant \beta \leqslant N)$,
then s_t is to be taken equal to $\{\alpha, \beta-1\}$;

if $r_t = \{\alpha, \beta\}$ $(M \leqslant \alpha < 2M; N < \beta \leqslant 2N)$,
then s_t is to be taken equal to $\{\alpha+1, \beta-1\}$;

if $r_t = \{\alpha, \beta\}$ $(0 \leqslant \alpha < M; N < \beta \leqslant 2N)$,
then s_t is to be taken equal to $\{\alpha+1, \beta\}$.

It is easy to verify that, if $r_1, r_2,..., r_h$ be a complete primitive residue set, the same is true of $s_1, s_2,..., s_h$ and also of $r_1 s_1, r_2 s_2,..., r_h s_h$.

The proofs are as follows:

(i) *for the numbers* r_t. From the first two lines of the above scheme we see that α takes $2M$ incongruent values (mod $2M$) when

$$1 \leqslant \beta \leqslant N;$$

from the third and fourth lines we see that α takes $2M$ incongruent values (mod $2M$) when $N < \beta \leqslant 2N$;

(ii) *for the numbers* s_t. From the first and fourth lines of the scheme we see that $s_t = \{\alpha, \beta\}$, where $1 \leqslant \alpha \leqslant M$ and β takes $2N$ incongruent values (mod $2N$); from the second and third lines of the scheme we see that $s_t = \{\alpha, \beta\}$, where $M < \alpha \leqslant 2M$ and β takes $2N$ incongruent values (mod $2N$);

(iii) *for the numbers* $r_t s_t$. Here we have $r_t s_t = \{\alpha, \beta\}$, where

in the first line, α takes all even values (mod $2M$),
β takes all even values (mod $2N$);

in the second line, α takes all even values (mod $2M$),
β takes all odd values (mod $2N$);

in the third line, α takes all odd values (mod $2M$),
β takes all odd values (mod $2N$);

in the fourth line, α takes all odd values (mod $2M$),
β takes all even values (mod $2N$).

In all the cases (i), (ii), (iii) we get $4MN$ numbers $\{\alpha, \beta\}$, where α runs through $2M$ incongruent values (mod $2M$) and β runs through $2N$ incongruent values (mod $2N$). Thus we have proved that the three sets r_t, s_t, and $r_t s_t$ $(1 \leqslant t \leqslant h)$ are complete primitive residue sets.

We can present the choices in the above scheme more briefly in a tabular form. [In the table given below the 'type' to which $r_t s_t$ belongs is indicated; if α is even and β is odd we shall say that $r_t s$ belongs to the type $+-$. The three other types $++$, $-+$, $--$ are similarly defined.]

$$n = p^\lambda q^\mu; \qquad r_t = \{\alpha, \beta\}$$

α	β	s_t	$r_t s_t$
$1 \leqslant \alpha \leqslant M$	$1 \leqslant \beta \leqslant N$	$\{\alpha, \beta\}$	$++$
$M < \alpha \leqslant 2M$	$1 \leqslant \beta \leqslant N$	$\{\alpha, \beta-1\}$	$+-$
$M \leqslant \alpha < 2M$	$N+1 \leqslant \beta \leqslant 2N$	$\{\alpha+1, \beta-1\}$	$--$
$0 \leqslant \alpha < M$	$N < \beta \leqslant 2N$	$\{\alpha+1, \beta\}$	$-+$

An even more brief representation of the table would be

r_t	11	21	2′2	1′2
s_t	11	21′	22′	12
$r_t s_t$	$++$	$+-$	$--$	$-+$

(II) $n = 4q^\mu$. This case is disposed of in exactly the same way as $n = p^\lambda q^\mu$ since the number 4 has the primitive root 3. The case $2^\lambda q^\mu$, where $\lambda > 2$, is discussed a little farther down.

(III) $n = 2^\lambda$ $(\lambda > 2)$. This case is disposed of in exactly the same way as $p^\lambda q^\mu$ for the following reason. Any primitive residue class (mod 2^λ) can be represented as $\{\alpha, \beta\}$, where $\{\alpha, \beta\}$ represents the residue class x, if and only if $x \equiv 5^\alpha(-1)^\beta \pmod{n}$.

We get all the residue classes by giving to α the values 0, 1, 2,...,

$2^{\lambda-2}-1$, and to β the values 0 and 1. This representation has all the properties mentioned earlier in connexion with the case $n = p^\lambda q^\mu$. We give below the details of the choice of $s_1, s_2,\ldots, s_h$, where

$$h = 2^{\lambda-1} = 4M.$$

r_t	$-5, -5^2,\ldots, -5^M$	$-5^{M+1},\ldots, -5^{2M}$	$5^M, 5^{M+1},\ldots, 5^{2M-1}$	$1, 5, 5^2,\ldots, 5^{M-1}$
s_t	$-5, -5^2,\ldots, -5^M$	$5^{M+1},\ldots, 5^{2M}$	$-5^{M+1}, -5^{M+2},\ldots, -5^{2M}$	$5, 5^2, 5^3,\ldots, 5^M$
$r_t s_t$	$5^{2\alpha}$ $(1 \leqslant \alpha \leqslant M)$	$-5^{2\alpha}$ $(M < \alpha \leqslant 2M)$	$-5^{2\alpha+1}$ $(M \leqslant \alpha < 2M)$	$5^{2\alpha+1}$ $(0 \leqslant \alpha < M)$

(IV) $n = p^\lambda q^\mu r^\nu$. Let g, g', g'' be respectively primitive roots of p^λ, q^μ, r^ν. We denote by $\{\alpha, \beta, \gamma\}$ the residue class $x \pmod n$, where

$$x \equiv g^\alpha \pmod{p^\lambda}, \quad x \equiv g'^\beta \pmod{q^\mu}, \quad x \equiv g''^\gamma \pmod{r^\nu}.$$

The choice of s_t is made according to the following table:

r_t	111	211	222	122	2′21	1′21	2′12	1′12
s_t	111	21′1	22′2′	122′	22′1′	121′	21′2	112
$r_t s_t$	$+++$	$+-+$	$+--$	$++-$	$---$	$-+-$	$--+$	$-++$

A more explicit version of this table would be

$$n = p^\lambda q^\mu r^\nu, \qquad \phi(p^\lambda) = 2M, \qquad \phi(q^\mu) = 2N,$$
$$\phi(r^\nu) = 2L, \qquad r_t = \{\alpha, \beta, \gamma\}$$

α	β	γ	s_t	$r_t s_t$
$1 \leqslant \alpha \leqslant M$	$1 \leqslant \beta \leqslant N$	$1 \leqslant \gamma \leqslant L$	$\{\alpha, \beta, \gamma\}$	$+++$
$M < \alpha \leqslant 2M$	$1 \leqslant \beta \leqslant N$	$1 \leqslant \gamma \leqslant L$	$\{\alpha, \beta-1, \gamma\}$	$+-+$
$M < \alpha \leqslant 2M$	$N < \beta \leqslant 2N$	$L < \gamma \leqslant 2L$	$\{\alpha, \beta-1, \gamma-1\}$	$+--$
$1 \leqslant \alpha \leqslant M$	$N < \beta \leqslant 2N$	$L < \gamma \leqslant 2L$	$\{\alpha, \beta, \gamma-1\}$	$++-$
$M \leqslant \alpha < 2M$	$N < \beta \leqslant 2N$	$1 \leqslant \gamma \leqslant L$	$\{\alpha+1, \beta-1, \gamma-1\}$	$---$
$0 \leqslant \alpha < M$	$N < \beta \leqslant 2N$	$1 \leqslant \gamma \leqslant L$	$\{\alpha+1, \beta, \gamma-1\}$	$-+-$
$M \leqslant \alpha < 2M$	$1 \leqslant \beta \leqslant N$	$L < \gamma \leqslant 2L$	$\{\alpha+1, \beta-1, \gamma\}$	$--+$
$0 \leqslant \alpha < M$	$1 \leqslant \beta \leqslant N$	$L < \gamma \leqslant 2L$	$\{\alpha+1, \beta, \gamma\}$	$-++$

(V) $n = 4q^\mu r^\nu$. This case is disposed of like the previous case since the number 4 has the primitive root 3.

(VI) $n = 2^\lambda r^\nu$ $(\lambda > 2)$. This case also is covered by the discussion in the case $n = p^\lambda q^\mu r^\nu$, for the residue class $x \pmod{2^\lambda r^\nu}$ can be represented by $\{\alpha, \beta, \gamma\}$, where α, β, γ are such that

$$x \equiv 5^\alpha(-1)^\beta \pmod{2^\lambda}, \qquad x \equiv g^\gamma \pmod{r^\nu},$$

g being a primitive root of r^ν. This completes all the cases included in the set S, and, as pointed out already, the proof of the theorem is now plain.

SUMMARY

It is known that, if $q > 2$ and q is prime, then there do not exist two complete residue sets $r_1, r_2, \ldots, r_q$ and $s_1, s_2, \ldots, s_q$ such that $r_1 s_1, r_2 s_2, \ldots, r_q s_q$ also is a complete residue set (mod q). It is pointed out in this note that the same conclusion holds not only for prime values of q but also for all numbers $q > 2$. The main result of the note is the theorem

THEOREM. *If $n > 2$ and $\phi(n) = h$, then there exist complete primitive residue sets $r_1, r_2, \ldots, r_h$ and $s_1, s_2, \ldots, s_h$ such that $r_1 s_1, r_2 s_2, \ldots, r_h s_h$ too is a complete primitive residue set if and only if n has no primitive root.*