COVERING CLASSES OF RESIDUES

JAMES H. JORDAN

1. Introduction. A set of ordered pairs of integers $\{(a_i, m_i)\}$ is said to cover the integers if each integer x satisfies the congruence $x \equiv a_i \pmod{m_i}$ for some i. We may assume that the m_i are positive. Trivially $\{(0, 1)\}$ covers, as does $\{(0, m), (1, m), (2, m), \ldots, (m-1, m)\}$. In order to arrive at some non-trivial problems concerning covers, the following definition is given: A finite set of ordered pairs of integers $\{(a_i, m_i)\}_{i=1}^{n}$, with $m_i > 1$ and $m_i \neq m_j$ if $i \neq j$, is called a *covering class of residues* if every integer x satisfies the congruence $x \equiv a_i \pmod{m_i}$ for some i.

These covering classes of residues were introduced by P. Erdös **(2)**, who used them to prove that there is an arithmetic progression of odd numbers none of which is expressible as a power of 2 added to a prime. Erdös **(6)** used the fact that $\{(0, 2), (0, 3), (1, 4), (7, 8), (11, 12), (19, 24)\}$ is a covering class of residues. He also noted that $\{(0, 2), (0, 3), (1, 4), (5, 6), (7, 12)\}$ is a covering class of residues.

Extending the problem, Erdös **(3)** proposed the following question: Does there exist a covering class of residues where $m_i > n$ for every n? For $n = 2$, he observed that

$$\{(0, 3), (0, 4), (0, 5), (1, 6), (6, 8), (3, 10), (5, 12), (11, 15), (7, 20), (10, 24), (2, 30), (34, 40), (59, 60), (98, 120)\}$$

is a covering class of residues **(6)**. J. D. Swift **(1)** found a covering class of residues $\{(a_i, m_i)\}$ such that $m_i > 3$ for all i. All of Swift's m_i's were factors of 2880. J. Selfridge **(5)** found a covering class of residues $\{(a_i, m_i)\}$ with all $m_i > 7$. Erdös has posted a \$50.00 reward **(3)** for settling the general question in either way.

Another question posed by Erdös is: Does there exist a covering class of residues with all m_i odd? He has posted a \$25.00 reward **(3)** for the negative answer to the question. J. Selfridge **(5)** posted a \$250.00 reward for the positive answer to the question (an example required).

Covering classes of residues will be called *essentially different* if each possesses a prime modulus not found in the other class and there can be no cover formed with the remaining moduli after omitting this prime modulus.

J. D. Swift **(7)** established that there were infinitely many essentially different covering classes of residues by the following method: If $2|g$ and $4|g$

Received January 17, 1966. The research in this paper is partially supported by N.S.F. Grant No. G-22765/0009 (undergraduate research) and Washington State University Grant in Aid for research, Project No. 728.

where g is a primitive root modulo an odd prime p, then

$$\{(g^{n-1}, 2^n)\}_{n=1}^{p-1} \cup \{(g^{n-1}, 2^{n-1}p)\}_{n=1}^{p-1} \cup \{(0, 2^{p-1}p)\}$$

is a covering class of residues.

In this paper we shall (i) exhibit a covering class of residues, $\{(a_i, m_i)\}$, with all $m_i > 3$ where the m_i are factors of 360; (ii) prove that there are infinitely many covering classes of residues with all $m_i > 2$; (iii) investigate a two-dimensional generalization of this problem.

2. A covering class with all $m_i > 3$.

THEOREM 1. *The following set is a covering class of residues:*

$$\{(0, 4), (0, 5), (3, 6), (2, 8), (1, 9), (1, 10), (5, 12), (8, 15), (13, 18), (7, 20), (6, 24), (14, 30), (25, 36), (6, 40), (43, 45), (59, 60), (22, 72), (79, 90), (62, 120), (142, 180), (214, 360)\}.$$

The proof amounts to merely checking the numbers $1, 2, \ldots, 360$ to see that they each satisfy at least one of the congruences. The details are left for the reader.

Since $360 \times 8 = 2880$, the method used to generate this example may be more effective than the method Swift used to get his example.

3. Infinitely many covering classes with all $m_i > 2$.

THEOREM 2. *For an odd prime $p > 3$, let*

$$A_1 = \{(2^{n-1} - 2, 2^n)\}_{n=2}^{p-2};$$
$$A_2 = \{(0, 3), (1, 6), (t, 3 \cdot 2^{p-2}), (3 \cdot 2^{n-1} - 1, 3 \cdot 2^n)\}_{n=2}^{p-3},$$

where t is the simultaneous solution of

$$x \equiv 1 \pmod 3 \quad \textit{and} \quad x \equiv 2^{p-2} - 2 \pmod{2^{p-2}};$$

$$A_3 = \{(0, p), (1, 2p), (a_n, 2^n p)\}_{n=2}^{p-2},$$

where a_n for $n = 2, 3, \ldots, p-3$ is the simultaneous solution of

$$x \equiv 2^{n-1} - 1 \pmod{2^n} \quad \textit{and} \quad x \equiv n \pmod p,$$

and a_{p-2} is the simultaneous solution of

$$x \equiv p - 1 \pmod p \quad \textit{and} \quad x \equiv 2^{p-2} - 2 \pmod{2^{p-2}};$$

$$A_4 = \{(b_n, 2^n 3p)\}_{n=0}^{p-2},$$

where b_0 is the simultaneous solution of

$$x \equiv 2 \pmod 3 \quad \textit{and} \quad x \equiv p - 2 \pmod p,$$

b_1 is the simultaneous solution of

$$x \equiv 1 \pmod 2 \quad \textit{and} \quad x \equiv p - 1 \pmod p,$$

https://doi.org/10.4153/CJM-1967-043-0 Published online by Cambridge University Press

and b_n, *for* $n = 2, 3, \ldots, p-2$, *is the simultaneous solution of*

$$x \equiv 2 \pmod 3,$$
$$x \equiv 2^n - 2 \pmod{2^n},$$
$$x \equiv p - 1 - n \pmod p.$$

Then $A_1 \cup A_2 \cup A_3 \cup A_4$ *is a covering class of residues with all* $m_i > 2$.

Proof. It suffices to prove that if x_0 fails to satisfy any of the congruences of A_1, A_2, or A_3, it must satisfy one of the congruences of A_4. If x_0 does not satisfy one of the congruences of A_1, it is either odd or of the form $a \cdot 2^{p-2} - 2$ for some integer a. If x_0 does not satisfy any of the congruences of A_2, it is even and congruent to 1 or 2 (mod 3) or it is odd and of the form $a \cdot 3 \cdot 2^{p-3} - 1$ for some integer a. If x_0 is neither of form A_1 or A_2, then it must be either of the form (i) $a \cdot 2^{p-2} - 2$ and congruent to 2 (mod 3), since the definition of t in A_2 precludes the possibility of its being congruent to 1 (mod 3), or of the form (ii) $a \cdot 3 \cdot 2^{p-3} - 1$. If x_0 satisfies none of the congruences of A_3 or of the congruences of A_1 or A_2, then either (i) $x_0 = a \cdot 2^{p-2} - 2$ is congruent to 2 (mod 3) and not congruent to $p - 1$ or 0 (mod p) or (ii) $x_0 = a \cdot 3 \cdot 2^{p-3} - 1$ is not congruent to j (mod p), $j = 0, 1, 2, \ldots, p-3$. In other words, either

$$x_0 = a \cdot 2^{p-2} - 2 \equiv s \pmod p \qquad \text{for } s = 1, 2, \ldots, p-2,$$

or

$$x_0 = a \cdot 3 \cdot 2^{p-3} - 1 \equiv j \pmod p \qquad \text{for } j = p-2 \text{ or } p-1.$$

Now if the latter were to hold, then $x_0 \equiv b_i \pmod{2^i 3p}$ for $i = 0$ or 1. If the former were to hold, then $x_0 \equiv b_i \pmod{2^i 3p}$ for $i = 2, 3, \ldots, p-2$. Hence x_0 satisfies a congruence from the set A_4.

A similar type theorem could be proved that there are infinitely many essentially different covering classes of residues with all $m_i > 3$. The length of the statement of the theorem is quite cumbersome and the proof is quite long although similar to the proof of Theorem 2.

4. A generalization. Let G be the ring of the Gaussian integers, i.e.,

$$G = \{\alpha | \alpha = a + bi, a, b \in Z\}.$$

In G the unique factorization theorem holds and G is a principal ideal ring. Therefore congruences can easily be defined as $\alpha \equiv \beta \pmod \gamma$ if $\gamma | \alpha - \beta$. We define: A set of ordered pairs of Gaussian integers $\{(\alpha_j, \gamma_j)\}$ *covers* G if every Gaussian integer β satisfies $\beta \equiv \alpha_j \pmod{\gamma_j}$ for some j.

Clearly $\{(0, 1)\}$, $\{(0, i)\}$, $\{(0, 1 + i), (1, 1 + i)\}$, and

$$\{(0, 1 + i), (1, 1 - i)\}$$

all cover G. Also $\{(0, 2), (i, 2i), (1, -2), (1 + i, -2i)\}$ covers G. So in order to adopt ground rules that are comparable to the definition of covering classes of

residues of §1 we eliminate units and associates. This is implemented by the following definition: A finite set of ordered pairs of Gaussian integers $\{(\alpha_j, \gamma_j)\}_{j=1}^{n}$ with $|\gamma_j| > 1$ such that no two γ_j's are associates is called a *covering class of residues in G* if every β in G satisfies the congruence $\beta \equiv \alpha_j \pmod{\gamma_j}$ for some j.

THEOREM 3. *The set*

$$\{(0, 1 + i), (i, 2), (1, 2 + 2i), (1 + 2i, 4), (0, 2 + i), (i, 3 - i), (1 + 2i, 4 + 2i), (1 + 6i, 6 - 2i), (11, 8 + 4i)\}$$

is a covering class of residues in G.

Proof. The only integers that do not satisfy

$$x \equiv 0 \pmod{1 + i}, \qquad x \equiv i \pmod 2,$$
$$x \equiv 1 \pmod{2 + 2i}, \qquad \text{or } x \equiv 1 + 2i \pmod 4$$

are Gaussian integers of the form $3 + 4\delta$ where δ is a Gaussian integer. Now δ is congruent to 0, 1, 2, 3, or 4 $(\text{mod } 2 + i)$. If $\delta \equiv 0 (\text{mod } 2 + i)$, then $3 + 4\delta \equiv i \pmod{3 - i}$ since $3 \equiv i \pmod{3 - i}$ and $(1 - i)(2 + 2i) = 4$ and $\delta = (2 + i)\rho$ so $4\delta = (2 + 2i)(3 - i)\rho$. Hence $3 - i | 3 - i + 4\delta$. If $\delta \equiv 1 \pmod{2 + i}$, then $3 + 4\delta \equiv 11 \pmod{8 + 4i}$; if $\delta \equiv 2 \pmod{2 + i}$, then $3 + 4\delta \equiv 1 + 2i \pmod{4 + 2i}$; if $\delta \equiv 3 \pmod{2 + i}$, then

$$3 + 4\delta \equiv 0 \pmod{2 + i};$$

and if $\delta \equiv 4 \pmod{2 + i}$, then $3 + 4\delta \equiv 1 + 6i \pmod{6 - 2i}$.

Now the questions that Erdös asked have generalizations in this system.

1. Does there exist a covering class of residues in G, $\{(\alpha_j, \gamma_j)\}$, that have all $|\gamma_j| > \sqrt{n}$?

We have an example for $n = 2$ which consists of the divisors or

$$200 = i(1 + i)^6(2 + i)^2(2 - i)^2.$$

We shall of course give a reward of \$50.00 for a positive or negative answer to Question 1.

2. Does there exist a covering class of residues in G, $\{(\alpha_j, \gamma_j)\}$, that have all γ_j odd? (I.e., $\gamma_j \neq (1 + i)\delta_j$.)

We shall of course give a \$25.00 reward for the negative answer to this question and a \$250.00 reward for the positive answer with example.

These problems seem to be somewhat harder than in the real case.

One result without much substance but of some interest is

THEOREM 4. *The set*

$$\{(0, 2 + i), (1, 2 - i), (2, 5), (0, 3), (4, 6 + 3i), (8, 6 - 3i), (13, 15), (5, 9), (29, 18 + 9i), (44, 45)\}$$

covers the real integers and $1 + i$ *is not a factor of* γ_j *for any* j.

https://doi.org/10.4153/CJM-1967-043-0 Published online by Cambridge University Press

The proof is quite simple and we omit it.

Results analogous to Theorem 2 are the following two theorems:

THEOREM 5. *For ρ a non-real odd Gaussian prime and $N(\rho) = p$ a real prime let*

$$A = \{((1+i)^{n-1}, (1+i)^n)\}_{n=1}^{p-1}, \qquad B = \{(n2^{(p-1)/2}, (1+i)^n\rho)\}_{n=0}^{p-1}.$$

Then $A \cup B$ is a covering class of residues in G.

THEOREM 6. *Let p be a real Gaussian prime and*

$$D = \{a + bi \mid 0 \leqslant a \leqslant p-1, 0 \leqslant b \leqslant p-1\}.$$

Let A' be the A of Theorem 5 with n ranging from 1 to $(p^2-3)/2$, and let

$$C = \{(\delta_j 2^{(p^2-1)/2}, (1+i)^j p)\}_{j=0}^{p^2-1}$$

where the δ_j are from D. Then $A' \cup C$ is a covering class of residues in G.

Proof of Theorem 5. If a β in G fails to satisfy one of the congruences of A, then $\beta = \gamma 2^{(p-1)/2}$ for some γ in G. But for γ there is an $n \in Z$ such that $\gamma \equiv n \pmod{\rho}$ with $0 \leqslant n \leqslant p-1$; see representation A of **(4)** for details. So $\beta \equiv n2^{(p-1)/2} \pmod{\rho}$ and further

$$\beta \equiv n2^{(p-1)/2} \pmod{(1+i)^n} \qquad \text{for all } 0 \leqslant n \leqslant p-1.$$

Hence $\beta \equiv n2^{(p-1)/2} \pmod{(1+i)^n\rho}$. Therefore each β that fails to satisfy one of the congruences of A must satisfy one of the congruences of B.

Proof of Theorem 6. The β of G that fail to satisfy one of the congruences of A' must be of the form $\beta = \gamma 2^{(p^2-1)/2}$ for some γ in G. But for each γ in G there is a δ_j in D such that $\gamma \equiv \delta_j \pmod{p}$; see representation B or C of **(4)** for details. So

$$\beta \equiv \delta_j 2^{(p^2-1)/2} \pmod{p}$$

and further

$$\beta \equiv \delta_j 2^{(p^2-1)/2} \pmod{(1+i)^j} \qquad \text{for all } 0 \leqslant j \leqslant p^2-1.$$

Hence

$$\beta \equiv \delta_j 2^{(p^2-1)/2} \pmod{(1+i)^j p}.$$

So each β in G that fails to satisfy a congruence from A' must satisfy one of the congruences of C.

Theorem 5 or Theorem 6 shows that there are infinitely many essentially different covering classes of residues in G. We do not know whether there are infinitely many essentially different covering classes of residues in G with all $|\gamma_j| > \sqrt{2}$.

The author wishes to express his gratitude to Professors J. L. Selfridge and S. K. Stein for their remarks concerning the background of this problem.

References

1. H. Davenport, *The higher arithmetic* (New York, 1960), p. 57.
2. P. Erdös, *On a problem concerning congruence systems*, Mat. Lapok., *3* (1952), 122–128.
3. ——— Proceedings of the 1963 Number Theory Conference, University of Colorado, Proposed Problem No. 28.
4. J. H. Jordan and C. J. Potratz, *Complete residue systems in the Gaussian integers*, Math. Mag., *38* (1965), 1–12.
5. J. L. Selfridge, Proceedings of the 1963 Number Theory Conference, University of Colorado, Proposed Problem No. 28.
6. S. K. Stein, *Brief notes on unions of arithmetic progressions*, Math. Dept., University of California at Davis.
7. J. D. Swift, *Sets of covering congruences*, Bull. Amer. Math. Soc., *60* (1954), 390.

Washington State University,
Pullman, Wash.