(ACTA F. R. N. UNIV. COMEN. – MATHEMATICA XXVII, 1972)

ACTA FACULTATIS RERUM NATURALIUM UNIVERSITATIS COMENIANAE

MATHEMATICA XXVII – 1972

ON COVERING OF RINGS BY THEIR RESIDUE CLASSES

ŠTEFAN PORUBSKÝ, ŠTEFAN ZNÁM, Bratislava

The disjoint covering of the set of all integers by residue classes is studied in many articles (see for example [1]). In [6] an above estimation for the number of residue classes in a disjoint covering system is shown. In [3] is this result generalized for the disjoint covering of some Abelian groups by their cosets.

Our article contains a generalization of mentioned problem in another direction. We shall study the disjoint covering of principal ideal domains by residue classes and show the mentioned estimation for the number of ideals. Further, we prove our result to be the best possible in some sense.

I.

A commutative integrity domain R with unit is called a principal ideal domain if every ideal of R is principal. That means if I is an ideal of R then there exists an element $a \in R$ such that $I = aR = \{ah : h \in R\}$. Such an ideal I is said to be generated by the element a.

Let R be a ring. Define the function f on R (the image of which is some set of cardinal numbers) in following way

$$a \in R : \quad f(a) = \operatorname{card} R/aR$$

where R/aR is the factor-ring related with ideal aR.

A residue class of R is a set of the form

$$a + nR = \{a + nh : h \in R\}$$

where $a, n \in R$.

A system of residues related with the element a is a set R_a (of elements of the ring R) with

(i) $0 \in R_a$ (0 is the zero of R),

(ii) if $x,y \in R_a$ and $x \neq y$ then $(x + aR) \cap (y + aR) = \emptyset$,

(iii) $\bigcup_{x \in R_a} (x + aR) = R$.

Later on we shall need the following properties:

1. Any principal ideal domain is a unique factorization domain, i.e. every element of R which does not divide the unit of R is expressible as a product of irreducible elements, and, except for the order of the factors and for unit factors, this representation is unique ([5], chapter IV, § 15, theorem 32).

2. If R is principal ideal domain and $a, b \in R$ then there exists a g.c.d. (a,b) of elements a,b in R.

3. Let p be an irreducible element in the principal ideal domain R and $a, b \in R$ so that $ab \neq 0$ and $p \mid ab$. Then either $p \mid a$ or $p \mid b$.

These two properties follows from the property 1.

4. Let R be a principal ideal domain and let $a, b, c \in R$. Then the diophantine equation $ax + by = c$ is solvable for $x,y \in R$ if and only if $(a,b) \mid c$.

It is easy to show the necessity of this condition. The sufficiency follows from the fact that the set $\{ax + by : x, y \in R\}$ is an ideal in R generated by g.c.d. (a,b) of elements a,b.

5. Let R_p be a system of residues related with irreducible element p. If $x \in R_p$ and $x \neq 0$ then $p \nmid X$.

In opposite case it holds

$$(0 + pR) \cap (x + pR) \neq \emptyset$$

And this is a contradiction.

We shall investigate such principal ideal domains for which f(a) is a finite cardinal number for every element $a \in R$, $a \neq 0$.

II

A system of residue classes

$$a_i + n_iR, \quad a_i, n_i \in R, \quad i \in T, \quad |T| > 1 \tag{1}$$

is said to be disjoint covering if

(j) $(a_i+n_iR) \cap (a_j+n_jR) = \emptyset$ for $i \neq j$

(jj) $\bigcup_{i \in T} (a_i+n_iR) = R$

For this system some properties of disjoint covering systems of the set of rational integers can be generalized (see [1], [3] and [6]).

1. $(n_i,n_j) \neq 1$ for any $i \neq 1$.

Suppose $(n_i,n_j) \mid 1$ for some i,j. Then the diophantine equation $a_i-a_j = xn_j-yn_i$ is solvable and hence the classes a_i+n_iR and a_j+n_jR are not disjoint.

2. Let T be a finite set. Then we have

$$\sum_{i \in T} \frac{1}{f(n_i)} = 1 \quad \text{for (1).}$$

We can easy prove that

$$R_{ab} = \{ x+a : x \in R_a, \ y \in R_b \}$$

which implies $f(ab) = f(a)f(b)$. According to this result the residue class $x + aR$ can be disjointly covered by $f(b) = \frac{f(ab)}{f(a)}$ classes of the form $x+ya+abR$ for $y \in R_b$.

Let $n = \prod_{i \in T} n_i$ with n_i from (1). Replace every residue class a_i+n_iR $(i \in T)$ by a system a_i+yn_i+nR $(y \in R_{n/n_i})$ of $\frac{f(n)}{f(n_i)}$ disjoint classes. Thus we get the following system [from (1)]

$$y + nR, \quad y \in R_n$$

So we have

$$f(n) = \sum_{i \in T} \frac{f(n)}{f(n_i)}$$

and our statement is proved.

3. Let

$$n_{i_o} = \prod_{t=1}^{r} p_t^{\lambda t}, \quad i_o \in T \tag{2}$$

be a decomposition into the irreducible elements. Then

$$\text{card } T \geqslant 1 + \sum_{t=1}^{r} \lambda_t [f(p_t) - 1]$$

To prove this assertion we shall need the following theorem.

Theorem 1. If (1) is a disjoint covering system and (2) holds then the elements

$$a_{i_o} + c_t q_t p_t^{\alpha t} \tag{3}$$

(where $t = 1,2,\ldots,r$; c_t runs over all elements of R_{p_t} except of 0; $q_t = n_{i_o}/p_t^{\lambda t}$; $\alpha_t = 0,1,\ldots,\lambda_t - 1$) belong to the distinct classes of the system (1).

To the proof we shall use the following

Lemma. If

$$a_{i_o} + c_t q_t p_t^{\alpha t} \in a_j + n_j R \tag{4}$$

then $p_t^{\beta t} \mid n_j$ with $\beta_t > \alpha_t$.

Proof. From (4) it follows

$$(q_t p_t^{\alpha t}, n_j) \mid a_{i_o} - a_j \tag{5}$$

However, the classes $a_{i_o} + n_{i_o} R$ and $a_j + n_j R$ are disjoint, hence the diophantine equation

$$a_{i_o} + n_{i_o} x = a_j + n_j y \tag{6}$$

is not solvable and so we have $(n_{i_o}, n_j) \nmid a_{i_o} - a_j$. From (5) and (6) it follows that n_j is divisible by $p_t^{\beta_t}$ with $\beta_t > \alpha_t$.

Proof of Theorem 1. The elements of (3) are pairwise distinct. We shall prove it indirectly. Suppose that for some t and t' we have

$$c_t q_t p_t^{\alpha_t} = c_{t'} q_{t'} p_{t'}^{\alpha_{t'}}$$

If $p_t \neq p_{t'}$ then the exponent of p_t on the left-hand side is smaller than that on the right-hand side. Let $p_t = p_{t'}$ and $\alpha_t \neq \alpha_{t'}$. Obviously $\alpha_t < \alpha_{t'}$ may be supposed. Hence we get

$$c_t q_t = c_{t'} q_{t'} p_t^{\alpha_{t'} - \alpha_t}.$$

However $p_t \nmid c_t q_t$ which is a contradiction. If $p_t = p_{t'}$ and $\alpha_t = \alpha_{t'}$, then from $(c_t - c_{t'}) q_t p_t^{\alpha_t} = 0$ we get $c_t = c_{t'}$.

The remaining part of proof is the same as in the case of rational integers ([6]).

Proof of property 3. The number of elements in (4) is exactly $\sum_{t=1}^{r} \lambda_t [f(p_t) - 1]$ since $\operatorname{card} \{c_t : c_t \in R_{p_t},\ c_t \neq 0\} = f(p_t) - 1$ and any of them does not belong to the class $a_{i_o} + n_{i_o} R$.

By the similar considerations as in [6] the following assertion can be proved.

Theorem 2. If R is a principal ideal domain and nR is its arbitrary ideal generated by n with

$$n = \prod_{t=1}^{r} p_t^{\lambda_t}$$

then there exists a disjoint covering system of the form (1) containing the class $0 + nR$ and consisting of $1 + \sum_{t=1}^{r} \lambda_t[f(p_t) - 1]$ classes.

Remark 1. Using the axiom of choice we can show that the property II.3 also holds for principal ideal domains in which $f(a)$ is any cardinal number.

Remark 2. If R is equal to Z (rational integers), then $f(p_t) = p_t$ and hence property II.3 is a generalization of Mycielski's conjecture from [4].

Remark 3. If R is a ring in which the unique factorization theorem is false then the property II.3 does not hold for arbitrary decomposition into irreducible elements. For example: Let $R = \{a + b\sqrt{-5}: a, b \in Z\}$. The ring R is not unique factorization domain and we have $6 = 2.3 = (1 + \sqrt{-5}).(1 - \sqrt{-5})$, where $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible in R (see [2], p. 211).

The system

$$k + (1 + \sqrt{-5})R \quad \text{for} \quad k = 0,1,\ldots,5$$

disjointly covers the ring R. Similarly the system

$$k(1 + \sqrt{-5}) + 6R \quad \text{for} \quad k = 0,1,\ldots,5$$

is disjoint and covers the residue class $0 + (1+\sqrt{-5})R$. Hence the system

$$\begin{aligned} &0 + 6R \\ &k + (1 + \sqrt{-5})R \\ &k(1 + \sqrt{-5}) + 6R \end{aligned} \qquad k = 1,2,\ldots, 5$$

is disjoint covering on R. (The number of classes is 11.)

On the other hand we can easy show that $f(2) = 4$, $f(3) = 9$, (because $R_2 = \{0,1,\sqrt{-5},1+\sqrt{-5}\}$ and $R_3 = \{0,1,2\ \sqrt{-5},2\ \sqrt{-5},1 +$

$\sqrt{-5}$, $1+2\sqrt{-5}$.$2+\sqrt{-5}$,$2+2\sqrt{-5}\}$) and from the factorization $6=2.3$ we should get

$$\text{card } T \geqslant 1 + (4-1) + (9-1) = 12.$$

However, this question is open for unique factorization domains which are not principal ideal domains (or more precisely for rings in with the property I.4 is false).

Remark 4. Our estimation for covering of rings by residue classes is different from like one for covering of groups by their cosets. For example: consider the ring $G = \{a + bi: a, b \in Z\}$ of all gaussian integers. The set $H = 3G = \{3(a + bi): a, b \in Z\}$ form an ideal of ring G and a subgroup of additive group of G.

Now, it is easy to check that the cosets

$$\{1 + 3a + bi: a,b \in Z\} = 1 + \{3a + bi: a, b \in Z\}$$

$$\{2 + 3a + bi: a,b \in Z\} = 2 + \{3a + bi: a, b \in Z\}$$

$$\{a + (1+3b)i: a, b \in Z\} = i + \{a+ 3bi: a, b \in Z\}$$

$$\{a + (2+3b)i: a, b \in Z\} = 2i + \{a + 3bi: a, b \in Z\}$$

together with F form a disjoint covering of G as a group (hence 5 cosets).

From Theorem 1 it follows that the minimal number of residue classes of any disjoint covering of G (as a ring) containing H is 9. Namely, the element 3 is irreducible in G and $R_3 = \{0,1,2,i,2i,1 + i,1+2i,2+i,2+2i\}$, hence $f(3) = 9$, thus card $T \geqslant 1 + [f(3)-1] = 9$.

REFERENCES

[1] ERDÖS P., Egy kongruenciarendszerekről szóló problémáról, Matematikai Lapok III (1952), 122-128
[2] HARDY G. H., WRIGHT E. M., An introduction to the theory of numbers, Oxford, 1954
[3] HEJNÝ M., ZNÁM Š., Coset decomposition of the Abelain groups, Acta F.R.N. Univ. Comen., XXV (1971) 15 - 19
[4] MYCIELSKI J., SIERPINSKI W., Sur une propriété des ensembles lineaires, Fund. Math. 58 (1966), 143-147
[5] ZARISKI O., SAMUEL P., Commutative algebra, vol. 1
[6] ZNÁM Š., On Mycielski's problem on systems of arithmetical progressions, Coll. Math. 15 (1966), 202 - 205

Author's address: Katedra algebry a teórie čísel PFUK, Bratislava, Matematický pavilón, Mlynská dolina

Received: February 16, 1971