Annales Univ. Sci. Budapest., Sect. Comp. 40 (2013) 275–283

GENERALIZED CYCLIC CONGRUENCE

J. Gonda (Budapest, Hungary)

Dedicated to Professors Zoltán Daróczy and Imre Kátai on their 75th anniversary

Communicated by Pavel Varbanets
(Received March 31, 2013; accepted July 11, 2013)

Abstract. This article generalizes the in the theory of finite fields important relation of $r \sim s$ defined on $\mathbf{Z}$ by the congruence $s \equiv rq^t \ (q-1)$, where r and s are arbitrary integers, t is a non-negative integer and q is a power of a prime.

1. Introduction

In the theory of the finite fields it is proved that if $f \in \mathbf{F}_q[x]$, where $\mathbf{F}_q$ denotes the field containing q elements, and u is a root of f in an extension field of $\mathbf{F}_q$ then also u^{q^k} is a root of the polynomial for any $k \in \mathbf{N}$. The multiplicative group of a finite field is cyclic, and a generating element is a primitive element of the field. Let g be a primitive element of $\mathbf{F}_q$, then the order of g in the multiplicative group of $\mathbf{F}_q$ is equal to the cardinality of that group, that is, to $q-1$. If $u \neq 0$ then $u = g^l$ and $q-1 > l \in N$. Now $u^{q^k} = g^{lq^k}$, and $g^{lq^i} = u^{q^i} = u^{q^j} = g^{lq^j}$ if and only if $lq^i \equiv lq^j \ (q-1)$ for any $l \in N$ and non-negative integers i and j. Let us suppose that $i \leq j$. Both sides of the last congruence can be divided by q^i, as q and $q-1$ are coprimes, so we get that $g^{lq^i} = g^{lq^j}$ if and only if $l \equiv lq^{j-i} \ (q-1)$. Let r and s be integers, and let $r \sim s$ if and only if there exists a non-negative integer t with the property of $s \equiv rq^t \ (q-1)$. It is easy to see that this is a congruence on $\mathbf{Z}$. This relation will be generalized in the next section.

Key words and phrases: Cyclic equivalence, cyclic congruence, cyclic coset.
2010 Mathematics Subject Classification: 08A30, 20M99.

2. New results

Definition 2.1. Let $\mathfrak{R} = (R; +, \cdot)$ be a ring, $\mathfrak{I} \lhd \mathfrak{R}$ such an ideal in $\mathfrak{R}$ that $\overline{\mathfrak{R}} = \mathfrak{R}/\mathfrak{I}$, that is the factor ring of $\mathfrak{R}$ by $\mathfrak{I}$ is a ring with identity, and let S be such a subset of R that its image in $\overline{R}$, denoted by $\overline{S}$ is a subgroup in the centre of the multiplicative semigroup of $\overline{\mathfrak{R}}$. Then $a \in R$, $b \in R$ are **cyclically congruent** modulo $(\mathfrak{S}, \mathfrak{I})$, denoted by $a \widehat{\equiv} b \,(\mathrm{mod}\ (S, I))$, or simply by $a \widehat{\equiv} b\ (S, I)$ if and only if there are such elements s_a and s_b in S that $as_a \equiv bs_b\ (I)$, that is, $as_a - bs_b \in I$. Similarly, if $\overline{a} \in \overline{R}$, $\overline{b} \in \overline{R}$, these elements are **cyclically congruent** modulo $\overline{S}$ exactly in the case if $\overline{a}\overline{s}_a = \overline{b}\overline{s}_b$, where $\overline{s}_a$ and $\overline{s}_b$ are in $\overline{S}$. This relation is denoted by $\overline{a} \widetilde{\equiv} \overline{b}$ (mod $\overline{S}$), abbreviated by $\overline{a} \widetilde{\equiv} \overline{b}\ (\overline{S})$ ($\overline{a}$ is the image of $a \in R$ in the factor ring).

Theorem 2.1. *Let a and b be arbitrary elements of R. Then $a \widehat{\equiv} b\ (S, I)$ if and only if $\overline{a} \widetilde{\equiv} \overline{b}\ (\overline{S})$.*

Proof.

1. If $a \widehat{\equiv} b\ (S, I)$, then $as_a \equiv bs_b\ (I)$, where $s_a \in S$ and $s_b \in S$, so s_a and s_b belong to $\overline{S}$ and $\overline{a}\overline{s}_a = \overline{b}\overline{s}_b$, and then $\overline{a} \widetilde{\equiv} \overline{b}\ (\overline{S})$;
2. $\overline{a} \widetilde{\equiv} \overline{b}\ (\overline{S})$ means that $\overline{a}\overline{s}_a = \overline{b}\overline{s}_b$, where $\overline{s}_a$ and $\overline{s}_b$ belong to $\overline{S}$. If s_a and s_b are such elements of S that $\overline{s}_a$ and $\overline{s}_b$ are their images, respectively, in $\overline{S}$, then $as_a \equiv bs_b\ (I)$ follows from $\overline{a}\overline{s}_a = \overline{b}\overline{s}_b$, and then $a \widehat{\equiv} b\ (S, I)$. ■

The equivalence of the two relations implies that we can freely change from one of them to the other one, that is, if we can prove something concerning one of them, then the statement is true for the other one, too.

Theorem 2.2. *The relation $\widehat{\equiv}$, defined on the ring $\mathfrak{R}$ is a congruence relation of $\mathfrak{R}^\times$, and similarly, $\widetilde{\equiv}$ is a congruence relation on $\overline{\mathfrak{R}}^\times$ ($\overline{\mathfrak{R}}^\times$ denotes the multiplicative semigroup of $\overline{\mathfrak{R}}$).*

Proof. $\widehat{\equiv}$ is defined on the pairs of the elements of R, so $\widehat{\equiv}$ is homogeneous binary relation on R as a set, and then on $\mathfrak{R}^\times$, too, as the base set of $\mathfrak{R}^\times$ is R again. First of all we prove that $\widehat{\equiv}$ is an equivalence relation.

1. As $\overline{\mathfrak{S}}$ is a group, so S can't be empty, and then $as - as = 0 \in I$ for an arbitrary element a in R and an arbitrary element in S, that is, $as \equiv as\ (I)$, so $a \widehat{\equiv} a\ (S, I)$, $\widehat{\equiv}$ is reflexive;

2. let a and b be two elements of R cyclically congruent modulo (S, I), that is, $a \widehat{\equiv} b\ (S, I)$. Then $as_a \equiv bs_b\ (I)$ with appropriate elements s_a, s_b of S. A congruence by an ideal is symmetrical, so $bs_b \equiv as_a\ (I)$, that is, by the definition of the cyclic congruence $b \widehat{\equiv} a\ (S, I)$, $\widehat{\equiv}$ is symmetrical;

3. let us suppose that for the three elements of R, for a, b and c, $a \widehat{\equiv} b\ (S, I)$ and $b \widehat{\equiv} c\ (S, I)$ are true. In that case there exist such elements s_a, s_u, s_v and s_c in S that $as_a \equiv bs_u\ (I)$ and $bs_v \equiv cs_c\ (I)$. $\overline{s_u s_v} \in \overline{S}$, as $\overline{s_u} \in \overline{S}$, $\overline{s_v} \in \overline{S}$ and $\overline{\mathfrak{S}}$ is a group. Then there is such an element s_b in S, that $\overline{s}_b = \overline{s_u s_v}$ (and, as $\overline{\mathfrak{S}}$ is a subgroup of the centre of $\overline{\mathfrak{R}}^{\times}$, $\overline{s}_b = \overline{s_v s_u}$). If $\overline{r} = \overline{t}$ then $r \equiv t\ (I)$, so

$$as_a s_v \equiv bs_u s_v \equiv bs_b \equiv bs_v s_u \equiv cs_c s_u\ (I).$$

Similarly, we get that there are such elements s_i and s_j in S, that $s_a s_v \equiv$ $\equiv s_i\ (I)$ and $s_c s_u \equiv s_j\ (I)$. Then

$$as_i \equiv as_a s_v \equiv cs_c s_u \equiv cs_j\ (I),$$

and, consequently, $a \widehat{\equiv} c\ (S, I)$ that proves the transitivity of the relation $\widehat{\equiv}$.

Finally we prove that this relation is compatible to the multiplication. Let a_1, a_2, b_1 and b_2 be four elements of R, $a_1 \widehat{\equiv} b_1\ (S, I)$ and $a_2 \widehat{\equiv} b_2\ (S, I)$, that is, $a_1 s_1 \equiv b_1 s_2\ (I)$ and $a_2 s_3 \equiv b_2 s_4\ (I)$. A congruence by an ideal is compatible to the multiplication, so

$$(a_1 a_2)(s_1 s_3) \equiv (a_1 s_1)(a_2 s_3) \equiv (b_1 s_2)(b_2 s_4) \equiv (b_1 b_2)(s_2 s_4)\ (I).$$

We can find such elements s_a and s_b, that s_a is congruent to $s_1 s_3$ and s_b is congruent to $s_2 s_4$, thus

$$(a_1 a_2)s_a \equiv (a_1 a_2)(s_1 s_3) \equiv (b_1 b_2)(s_2 s_4) \equiv (b_1 b_2)s_b\ (I)\,.$$

$(a_1 a_2)s_a \equiv (b_1 b_2)s_b\ (I)$ is equivalent to $a_1 a_2 \widehat{\equiv} b_1 b_2\ (S, I)$, so the product of cyclically congruent elements is cyclically congruent, too.

The proof of the statement given in the second part of the theorem is a simple transcription of the proof of the first part, as $a \equiv b\ (I)$ if and only if $\overline{a} = \overline{b}$. ■

Theorem 2.3. *If $a \equiv b\ (I)$ where $a \in R$ and $b \in R$, then $a \widehat{\equiv} b\ (S, I)$.*

Proof. S is not empty, as $\overline{\mathfrak{S}}$ is a group, and a congruence by an ideal is closed for the multiplication. Then, with an appropriate $s \in S$, $as \equiv bs\ (I)$ follows from $a \equiv b\ (I)$ and then $a \widehat{\equiv} b\ (S, I)$. ■

Theorem 2.4. *$\overline{a}\widetilde{\equiv}\overline{b}\ \left(\overline{S}\right)$ if and only if there is such an $\overline{s}\in\overline{S}$, that $\overline{b}=\overline{as}$.*

Proof. $\overline{a}\widetilde{\equiv}\overline{b}\ \left(\overline{S}\right)$ if and only if $\exists\left(\overline{s}_a\in\overline{S}\right)\exists\left(\overline{s}_b\in\overline{S}\right):\overline{as}_a=\overline{b}\overline{s}_b$. As $\overline{\mathfrak{S}}$ is a group, there is an inverse $\overline{s}_b^{-1}$ of $\overline{s}_b$ in $\overline{\mathfrak{S}}$. If $\overline{s}=\overline{s}_a\overline{s}_b^{-1}$, then $\overline{b}=\overline{b}\overline{e}=\overline{b}\overline{s}_b\overline{s}_b^{-1}=$ $=\overline{as}_a\overline{s}_b^{-1}=\overline{as}$. Conversely, if $\overline{b}=\overline{as}$, then $\overline{b}\overline{e}=\overline{b}=\overline{as}$, thus $\overline{a}\widetilde{\equiv}\overline{b}\ \left(\overline{S}\right)$. ■

Theorem 2.5. *$t_a=t_{\overline{a}}$, and from $\overline{a}\widetilde{\equiv}\overline{b}\ \left(\overline{S}\right)$ follows $t_a=t_b$, where $t_{\overline{a}}$ is the additive order of $\overline{a}\in\overline{R}$, while t_a is the least positive integer with the property that $ka\in I$.*

Proof. If $t_{\overline{a}}\overline{a}=\overline{0}$ then $t_{\overline{a}}a\in I$, thus $t_{\overline{a}}\geq t_a$, and from $t_aa\in I$ follows $t_a\overline{a}=\overline{0}$, so $t_a\geq t_{\overline{a}}$, that is, $t_{\overline{a}}=t_a$. $\overline{a}\widetilde{\equiv}\overline{b}\ \left(\overline{S}\right)$ means that $\overline{b}=\overline{as}$ with an element $\overline{s}$ belonging to $\overline{S}$, and then

$$t_a\overline{b}=t_a\left(\overline{as}\right)=\left(t_a\overline{a}\right)\overline{s}=\overline{0}\overline{s}=\overline{0},$$

$t_a>t_b$. Similarly, multiplying both sides of the equation $\overline{b}=\overline{as}$ by the inverse of $\overline{s}$ existing in $\overline{\mathfrak{R}}$, we get that $t_a<t_b$, thus $t_a=t_b$. ■

Definition 2.2. Let $U=U^{(R,I)}$ be a representing system of R by the ideal $\mathfrak{I}$ of $\mathfrak{R}$, and let a be an element of U. Then $C_a^{(R;S,I,U)}=\{b\in U\ |a\widehat{\equiv}b\ (S,I)\}$ is the **cyclic coset of** $\mathfrak{R}$ modulo (S,I,U) **represented by** a and $C_{\overline{a}}^{\left(\overline{R};\overline{S}\right)}=$ $=\left\{\overline{b}\in U\ \left|\overline{a}\widetilde{\equiv}\overline{b}\ \left(\overline{S}\right)\right.\right\}$ is the **cyclic coset of** $\overline{\mathfrak{R}}$ modulo $\overline{\mathfrak{S}}$ **represented by** $\overline{a}$.

Theorem 2.6. *Let $U=U^{(R,I)}$ be a representing system of R by the ideal $\mathfrak{I}$ of $\mathfrak{R}$, and let a and b be elements of U. Then either $C_a^{(R;S,I,U)}=C_b^{(R;S,I,U)}$ or $C_a^{(R;S,I,U)}$ and $C_b^{(R;S,I,U)}$ are disjoint, and similarly, if $C_{\overline{a}}^{\left(\overline{R};\overline{S}\right)}$ and $C_{\overline{b}}^{\left(\overline{R};\overline{S}\right)}$ are different sets then $C_{\overline{a}}^{\left(\overline{R};\overline{S}\right)}\cap C_{\overline{b}}^{\left(\overline{R};\overline{S}\right)}=\emptyset$.*

Proof. The statements are direct consequences of Theorem 2.2. ■

Definition 2.3. Let $U=U^{(R,I)}$ be a representing system of R by the ideal $\mathfrak{I}$ of $\mathfrak{R}$. Then $\left\{C_a^{(R;S,I,U)}\,|a\in U\right\}$ is the **cyclic partition of** $\mathfrak{R}$ modulo (S,I,U) and T is a **cyclic representing system of** $\mathfrak{R}$ modulo (S,I,U) if T contains exactly one element of each class of the partition. Similarly, $\left\{C_{\overline{a}}^{\left(\overline{R};\overline{S}\right)}\,\left|\overline{a}\in\overline{R}\right.\right\}$ is the **cyclic partition of** $\overline{\mathfrak{R}}$ modulo $\overline{\mathfrak{S}}$, and $\overline{T}$ is a **cyclic representing system of** $\overline{\mathfrak{R}}$ modulo $\overline{\mathfrak{S}}$ if $\overline{T}\cap C_{\overline{a}}^{\left(\overline{R};\overline{S}\right)}$ contains one and only one element for every $\overline{a}\in\overline{R}$.

Theorem 2.7. *For all of the* $U \mod I$ *representing systems of the ring* $\mathfrak{R}$ *there exists a bijection between the two sets of* $\left\{C_a^{(R;S,I,U)} \,|a \in U\right\}$ *and* $\left\{C_{\overline{a}}^{(\overline{R};\overline{S})} \,\middle|\overline{a} \in \overline{R}\right\}$.

Proof. There is a one to one correspondence between U and $\overline{R}$ that can be transmitted to the partitionings of the two sets. Furthermore, if a partitioning of $\overline{R}$ is a cyclic congruence, then from the fact that $\overline{a} \widetilde{\equiv} \overline{b} \ \left(\overline{S}\right)$ if and only if $a \widehat{\equiv} b \ (S, I)$ follows that the corresponding partitioning of U is the corresponding cyclic partitioning of $R \mod (S, I, U)$. This statement is right backwards, too. ■

Corollary 2.1. *If* T *is a cyclic representing system of the ring* $\mathfrak{R}$ *mod* (S, I, U), *then* $\overline{T} = \{\overline{a} \,|a \in T\}$ *is a cyclic representing system of* $\overline{R}$ *mod* $\overline{S}$. *Reversely, if* $\overline{T}$ *is a mod* $\overline{S}$ *representing system of* $\overline{R}$, *then there is such a representing system* U *of* R *by* I *that* $T = \left\{a \in U \,\middle|\overline{a} \in \overline{R}\right\}$.

Proof. In the previous theorem a one to one correspondence was established between the two sets of $\left\{C_a^{(R;S,I,U)} \,|a \in U\right\}$ and $\left\{C_{\overline{a}}^{(\overline{R};\overline{S})} \,\middle|\overline{a} \in \overline{R}\right\}$. As both T and $\overline{T}$, respectively, contain one and only one element from the two sets of $C_a^{(R;S,I,U)}$ and $C_{\overline{a}}^{(\overline{R};\overline{S})}$ for any $a \in U$ and $\overline{a} \in \overline{R}$, so $a \longmapsto \overline{a} \ (a \in U)$ results in the bijection expected. ■

Definition 2.4. $c_{\overline{a}}^{(\overline{R};\overline{S})} = \left|C_{\overline{a}}^{(\overline{R};\overline{S})}\right|$ is the **cyclic order of** $\overline{a}$ modulo $\overline{S}$, and $c_b^{(R;S,I)} = \left|C_a^{(R;S,I,U)}\right|$ is the **cyclic order** modulo (S, I) of any element satisfying the condition of $b \equiv a \in U \ (I)$.

Theorem 2.8.

1. $c_a^{(R;S,I)} = c_{\overline{a}}^{(\overline{R};\overline{S})}$;
2. $\overline{a} \widetilde{\equiv} \overline{b} \ \left(\overline{S}\right) \Longrightarrow c_{\overline{a}}^{(\overline{R};\overline{S})} = c_{\overline{b}}^{(\overline{R};\overline{S})}$;
3. $a \equiv b \ (I) \Longrightarrow c_{\overline{a}}^{(\overline{R};\overline{S})} = c_{\overline{b}}^{(\overline{R};\overline{S})}$.

Proof.

1. If two elements of $C_a^{(R;S,I,U)}$ are incongruent mod I then the corresponding elements in $C_{\overline{a}}^{(\overline{R};\overline{S})}$ are different, and this is true in the other direction, too;
2. $\overline{a}\widetilde{\equiv}\overline{b}\ \left(\overline{S}\right)$ is true if and only if $\overline{a}$ and $\overline{b}$ belong to the same cyclic coset;
3. $a \equiv b\ (I) \Longrightarrow \overline{a} = \overline{b} \Longrightarrow c_{\overline{a}}^{(\overline{R};\overline{S})} = c_{\overline{b}}^{(\overline{R};\overline{S})}$. ■

Theorem 2.9. *Let* $N_{\overline{a}} = \left\{\overline{s} \in \overline{S} \,\middle|\, \overline{a}\,(\overline{s} - \overline{e}) = \overline{0}\right\}$, *then* $\mathfrak{N}_{\overline{a}} \leq \overline{\mathfrak{S}}$ *and* $c_{\overline{a}}^{(\overline{R};\overline{S})} = \left|\overline{\mathfrak{S}} : \mathfrak{N}_{\overline{a}}\right|$. *If* $\overline{T}_a$ *is a representing system of* $\overline{S}$ *by* $N_{\overline{a}}$, *then*

$$C_{\overline{a}}^{(\overline{R};\overline{S})} = \left\{\overline{a}\overline{t} \,\middle|\, \overline{t} \in \overline{T}_a\right\},\ \left|C_{\overline{a}}^{(\overline{R};\overline{S})}\right| = \left|\overline{T}_a\right|,$$

and $\overline{a}\overline{s}_1 = \overline{a}\overline{s}_2 \Longleftrightarrow \overline{s}_2 \in \overline{s}_1 N_{\overline{a}}$.

Proof. $N_{\overline{a}}$ is not empty, as $\overline{e}$ belongs to it: $\overline{\mathfrak{S}}$ is a group, so $\overline{e} \in \overline{S}$, and $\overline{a}\,(\overline{e} - \overline{e}) = \overline{0}$. If $\overline{s}$ and $\overline{t}$ is two elements of $N_{\overline{a}}$, then $\overline{a}\left(\overline{s}\overline{t}^{-1} - \overline{e}\right) = \left(\overline{a}\,(\overline{s} - \overline{e}) - \overline{a}\left(\overline{t} - \overline{e}\right)\right)\overline{t}^{-1} = \overline{0}$, $\overline{s}\overline{t}^{-1} \in N_{\overline{a}}$, therefore $N_{\overline{a}}$ is a group with the multiplication of the similar operation of $\overline{S}$, so $\mathfrak{N}_{\overline{a}} \leq \overline{\mathfrak{S}}$. Now

$$\overline{a}\overline{s} = \overline{a}\overline{t} \Longleftrightarrow \overline{a}\left(\overline{s}\overline{t}^{-1} - \overline{e}\right)\overline{t} = \overline{0} \Longleftrightarrow \overline{a}\left(\overline{s}\overline{t}^{-1} - \overline{e}\right) = \overline{0}$$
$$\Longleftrightarrow \overline{s}\overline{t}^{-1} \in N_{\overline{a}} \Longleftrightarrow \overline{s} \in N_{\overline{a}}\overline{t},$$

that is, two elements of $C_{\overline{a}}^{(\overline{R};\overline{S})} = \left\{\overline{b} \,\middle|\, \overline{a}\widetilde{\equiv}\overline{b}\ \left(\overline{S}\right)\right\} = \left\{\overline{a}\overline{s} \,\middle|\, \overline{s} \in \overline{S}\right\}$ differ from one another if and only if they are generated by such elements that belong to different cosets by $N_{\overline{a}}$, hence $c_{\overline{a}}^{(\overline{R};\overline{S})} = \left|\overline{\mathfrak{S}} : \mathfrak{N}_{\overline{a}}\right|$, and the other statements of the theorem hold, too. ■

Theorem 2.10. *If* $\overline{a}$ *is at least one sided regular in* $\overline{\mathfrak{R}}$, *then* $c_{\overline{a}}^{(\overline{R};\overline{S})} = \left|\overline{S}\right|$, *and if* $\overline{S}$ *is finite then* $c_{\overline{a}}^{(\overline{R};\overline{S})} \mid c$.

Proof. In the first case $N_{\overline{a}}$ contains only $\overline{e}$ (it is obvious if $\overline{a}$ is a left sided regular element, and in the case of the right sided regularity it comes from the fact that $\overline{s}$ and $\overline{e}$, and then $\overline{s} - \overline{e}$, too, are in the center of $\overline{\mathfrak{R}}$), then $\overline{\mathfrak{S}}\widetilde{=}\overline{\mathfrak{S}}/\mathfrak{N}_{\overline{a}}$, so $c_{\overline{a}}^{(\overline{R};\overline{S})} = \left|\overline{\mathfrak{S}} : \mathfrak{N}_{\overline{a}}\right| = \left|\overline{\mathfrak{S}}/\mathfrak{N}_{\overline{a}}\right| = \left|\overline{S}\right|$. The second statement is true, too, as the index of a subgroup divides the order of the group, if this group is finite.■

Theorem 2.11. *If $\overline{a}$ is not a left sided zero divisor or $\overline{b}$ is not a right sided zero divisor, then $c_{\overline{a}\overline{b}}^{(\overline{R};\overline{S})} = c_{\overline{b}}^{(\overline{R};\overline{S})}$ and $c_{\overline{a}\overline{b}}^{(\overline{R};\overline{S})} = c_{\overline{a}}^{(\overline{R};\overline{S})}$, respectively, otherwise if both $c_{\overline{a}}^{(\overline{R};\overline{S})}$ and $c_{\overline{b}}^{(\overline{R};\overline{S})}$ are finite, then $c_{\overline{a}\overline{b}}^{(\overline{R};\overline{S})} \left| \left(c_{\overline{a}}^{(\overline{R};\overline{S})}, c_{\overline{b}}^{(\overline{R};\overline{S})} \right) \right.$.*

Proof. An element of $\overline{S}$, say $\overline{s}$ belongs to $N_{\overline{a}\overline{b}}$, if $\left(\overline{a}\overline{b}\right)(\overline{s}-\overline{e}) = \overline{0}$. Then

$\overline{a}\left(\overline{b}\,(\overline{s}-\overline{e})\right) = \overline{0}$, and it can be seen that if $\overline{a}$ is not a left sided zero divisor then $\overline{a}\left(\overline{b}\,(\overline{s}-\overline{e})\right) = \overline{0}$ if and only if $\overline{b}\,(\overline{s}-\overline{e}) = \overline{0}$, that is, if $\overline{s} \in N_{\overline{b}}$. In the other case we can refer to the fact again that $\overline{s}-\overline{e}$ is in the centre, so

$$\overline{0} = \left(\overline{a}\overline{b}\right)(\overline{s}-\overline{e}) = \overline{a}\left(\overline{b}\,(\overline{s}-\overline{e})\right) = \overline{a}\left((\overline{s}-\overline{e})\,\overline{b}\right) = (\overline{a}\,(\overline{s}-\overline{e}))\,\overline{b},$$

and if $\overline{b}$ is not a right sided zero divisor, then $(\overline{a}\,(\overline{s}-\overline{e}))\,\overline{b} = \overline{0}$ coincides to $\overline{a}\,(\overline{s}-\overline{e}) = \overline{0}$, and that means that $\overline{s} \in N_{\overline{a}}$. In general, if $\overline{s} \in N_{\overline{a}}$ or $\overline{s} \in N_{\overline{b}}$, then $\overline{s} \in N_{\overline{a}\overline{b}}$, and then $\mathfrak{N}_{\overline{a}} \leq \mathfrak{N}_{\overline{a}\overline{b}}$ and $\mathfrak{N}_{\overline{b}} \leq \mathfrak{N}_{\overline{a}\overline{b}}$, furthermore the order of a subgroup of a finite group is finite and divides the order of the group, and these facts imply that $c_{\overline{a}\overline{b}}^{(\overline{R};\overline{S})} \left| \left(c_{\overline{a}}^{(\overline{R};\overline{S})}, c_{\overline{b}}^{(\overline{R};\overline{S})} \right) \right.$. ■

Theorem 2.12. *If $\overline{c} \in \overline{R}$ and $\overline{a} \tilde{\equiv} \overline{b}$ $\left(\overline{S}\right)$ then $\overline{c}\overline{a} \tilde{\equiv} \overline{c}\overline{b}$ $\left(\overline{S}\right)$ és $\overline{a}\overline{c} \tilde{\equiv} \overline{b}\overline{c}$ $\left(\overline{S}\right)$, and, if $\overline{c} \neq \overline{0}$, then $\overline{a} \tilde{\equiv} \overline{b}$ $\left(\overline{S}\right)$ follows from $\overline{c}\overline{a} \tilde{\equiv} \overline{c}\overline{b}$ $\left(\overline{S}\right)$ or $\overline{a}\overline{c} \tilde{\equiv} \overline{b}\overline{c}$ $\left(\overline{S}\right)$ if and only if $\overline{c}$ is not a left sided or right sided zero divisor, respectively.*

Proof.

$$\overline{a} \tilde{\equiv} \overline{b} \ \left(\overline{S}\right) \Longleftrightarrow \left(\exists\left(\overline{s} \in \overline{S}\right) : \overline{b} = \overline{a}\overline{s}\right)$$
$$\Longrightarrow \left(\exists\left(\overline{s} \in \overline{S}\right) : \overline{c}\overline{b} = \overline{c}\,(\overline{a}\overline{s}) = (\overline{c}\overline{a})\,\overline{s}\right) \Longleftrightarrow \overline{c}\overline{a} \tilde{\equiv} \overline{c}\overline{b} \ \left(\overline{S}\right),$$

and we get the similar result in the other case, too, considering $(\overline{a}\overline{s})\,\overline{c} = (\overline{a}\overline{c})\,\overline{s}$, as $\overline{s}$ is in the center of $\overline{\mathfrak{R}}$.

If $\overline{c}$ is regular from the left side or the right side, respectively, then in the previous chain we can exchange $\Longrightarrow$ by $\Longleftrightarrow$. But if $\overline{c}$ is not a left sided zero divisor, then there exists such $\overline{a} \neq \overline{0}$, that $\overline{c}\overline{a} = \overline{0} = \left(\overline{c}\overline{0}\right)\overline{s}$ and then $\overline{c}\overline{a} \tilde{\equiv} \overline{c}\overline{0}$ $\left(\overline{S}\right)$, while $\overline{0}\overline{s} = \overline{0}$ implies that $C_{\overline{0}}^{(\overline{R};\overline{S})} = \left\{\overline{0}\right\}$, and consequently $\overline{a} \tilde{\equiv} \overline{0}$ $\left(\overline{S}\right)$ is not true. The case if $\overline{c}$ is not a right sided zero divisor is similar. ■

Example 2.13. Let $R = Z$, $k \in N^+$, $r \in N^+$, $(k,r) = 1$, $I = kZ$, $S = \{r\}$ $(r \in R)$. Then

1. $c_i^{(R;S,I)} = ord_{t_i}(r)\,|ord_k(r)|\,\varphi(k)$;

2. $(i,k)=1 \Longrightarrow c_i^{(R;S,I)} = ord_k(r)$;
3. $i \widehat{\equiv} j \ (S,I) \Longrightarrow t_i = t_j$;
4. $t_i = t_j \Longrightarrow c_i^{(R;S,I)} = c_j^{(R;S,I)}$;
5. $ir^u \equiv ir^v \ (k) \Longleftrightarrow u \equiv v \ \left(c_i^{(R;S,I)}\right)$,

where $i \in Z$, $j \in Z$, $u \in N$, $v \in N$, $t_i = o^+\left(\bar{i}\right) = \frac{k}{(i,k)}$, and $ord_s(t) = \min\left\{l \in N^+ \left| t^l \equiv 1 \ (s)\right.\right\}$.

Proof.

1. Let $U = \{u \in N | i < k\}$. $c_i^{(R;S,I)} = \left|\left\{j \in U \left| \exists (l \in N) : j \equiv ir^l \ (k)\right.\right\}\right|$, that is, the cyclic order of i is equal to the number of the integers of the form ir^l incongruent by modulo k.

$$ir^u \equiv ir^v \ (k) \Longleftrightarrow r^u \equiv r^v \ \left(\frac{k}{(i,k)}\right) \Longleftrightarrow r^{v-u} \equiv 1 \ \left(\frac{k}{(i,k)}\right),$$

as k and r are coprimes (and we supposed that $u \leq v$). If t is the least positive integer with the property that $r^t \equiv 1 \ \left(\frac{k}{(i,k)}\right)$, and $t > l \in N$, then ir^l is not congruent to $i = ir^0$ mod k, but for every $t \leq l \in N$ there exists such $t > s \in N$ that $r^l \equiv r^s \ \left(\frac{k}{(i,k)}\right)$, and then $c_i^{(R;S,I)} = t = ord_{\frac{k}{(i,k)}}(r)$. If $r^s \equiv 1 \ (k)$ then $r^s \equiv 1 \ \left(\frac{k}{(i,k)}\right)$ holds, too, and then $\frac{k}{(i,k)}$ divides both $r^s - 1$ and $r^t - 1$, consequently their greatest common divisor, $r^{(s,t)} - 1$, too, and this results in the relation of $r^{(s,t)} \equiv 1 \ \left(\frac{k}{(i,k)}\right)$. But t is the least positive integer having this property, so $t \leq (s,t)$, and, on the other hand, $t \geq (s,t)$, as $t \neq 0$, that means, that $t = (s,t)$, and that is only possible if $t \,|s$. The last divisibility follows from the Euler-Fermat theorem, namely, if an integer is relatively prime to k, then its order by modulo k divides $\varphi(k)$, where φ is the Euler's totient function;

2. if i and k are coprimes then $\frac{k}{(i,k)} = k$, and then $ord_{\frac{k}{(i,k)}}(r) = ord_k(r)$;
3. $i \widehat{\equiv} j \ (S,I) \Longrightarrow j \equiv ir^l \ (k) \Longrightarrow t_i j \equiv t_i ir^l \equiv 0 \ (k) \Longrightarrow t_j \,|t_i$. $0 \equiv \equiv t_j j \equiv t_j ir^l \ (k)$, and we can divide by r^l, as $(k,r) = 1$, so $t_j i \equiv 0 \ (k)$, consequently $t_i \,|t_j$, and $t_i = t_j$, as both of them are positive;
4. if $t_i = t_j$ then obviously $ord_{t_i}(r) = ord_{t_j}(r)$;
5. the proof of this statement is a part of the proof of the first point of the theorem. ■

Example 2.14. Let $R = Z$, $m \in N^+$, $n \in N^+$, $I = (m^n - 1)\,Z$, $S = \{m\}$ $(m \in R)$. Then $c_i^{(R;S,I)} \,|n$, and, if $(i, m^n - 1) = 1$ then $c_i^{(R;S,I)} = n$.

Proof. $m^n - 1 \,\Big|\, m^{n'} - 1$ if and only if $n \,|n'$, and the least such integer is equal to n', so, the second assertion is a special case of the second point of the previous example.

$im^l \equiv i \ (m^n - 1)$ if and only if $m^n - 1$ divides $i\left(m^l - 1\right)$. $m^n - 1$ evidently divides $i\,(m^n - 1)$, so $im^l \equiv i \ (m^n - 1)$ if and only if $m^n - 1 \,\big|\, i\left(m^{(l,n)} - 1\right)$, that is, if and only if $im^{(l,n)} \equiv i \ (m^n - 1)$, and this congruence is equivalent to the condition that $c_i^{(R;S,I)} \,|(l, n)|\, n$, so, the first statement holds, too. ■

References

[1] **Gonda, J.,** Finite Fields, `http://www.inf.elte.hu/karunkrol /digitkonyv/Jegyzetek2011/GondaJanos-VegesTestek2011.pdf` (in hungarian)

[2] **Lidl, R. and H. Niederreiter,** *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

[3] **Lidl, R. and G. Pilz,** *Applied Abstract Algebra* Springer-Verlag, New York, 1984.

J. Gonda
Eötvös University
Budapest
Hungary
`andog@inf.elte.hu`