Annales Univ. Sci. Budapest., Sect. Comp. 48 (2018) 151–167

SEMIGROUP STRUCTURE OF SETS OF SOLUTIONS TO EQUATION $X^m = X^s$

Štefan Porubský (Prague and Ostrava, Czech Republic)

Communicated by Imre Kátai
(Received February 8, 2018; accepted April 30, 2018)

Abstract. We describe the semigroup and group structure of the set of solutions to equation $X^m = X^s$ over the multiplicative semigroups of factor rings of residually finite commutative rings and of residually finite commutative PID's. The analysis is done in terms of the structure of maximal unipotent subsemigroups and subgroups of semigroups of the corresponding rings. In case of residually finite PID's we employ the available idempotents analysis of the Euler–Fermat Theorem in these rings used to determine minimal positive integers ν and μ such that for all elements x of these rings one has $x^{\kappa+\delta} = x^{\kappa}$. In particular, the case when this set of solutions is a union of groups is handled. As a simple application we show a not yet noticed group structure of the set of solutions to $x^n = x \pmod n$ connected with the message space of RSA cryptosystems and Fermat pseudoprimes.

1. Introduction

In the present paper we describe the semigroup structure of the set of solutions to equation

$$X^m = X^s \tag{1.1}$$

Key words and phrases: Set of solutions, idempotent, maximal semigroup corresponding to an idempotent, maximal group corresponding to an idempotent, Fermat–Euler theorem, commutative ring with identity element, residually finite commutative principal ideal domains.
2010 Mathematics Subject Classification: 11T99, 11D41, 11T06, 13F10, 20M14.
The author was supported by the Grant Agency of the Czech Republic, Grant # 17-02804S and the strategic development financing RVO 67985807. All computations are made using *Mathematica* 10 program package.
https://doi.org/10.71352/ac.48.151

over some classes of commutative rings, where $m > s \geq 1$ are given positive integers. The prototype case of equation (1.1), the set of solutions to congruence

$$x^m \equiv x \pmod{n} \tag{1.2}$$

over the ring $\mathbb{Z}_n$ of residue classes modulo n, where $m > 1$ is a given positive integer, is a subject of an investigation in connection with various types of problems, e.g. with the Fermat Little Theorem and its various generalizations. In [6] the author initiated the study of the semigroup structure of the set of solutions to the polynomial congruence (1.2) over the ring $\mathbb{Z}_n$ of residue classes modulo n, where $m > 1$ is a given positive integer. In his main result (Theorem 4) the author claims that the the semigroup of solutions to (1.2) can be written as the union of the maximal unipotent subgroups corresponding to the idempotents of the multiplicative semigroup of $\mathbb{Z}_m$. Nevertheless, this claim is not correct in the full generality as it is shown by Example 4.2 below. The approach used in [6] uses tools from the theory of polynomials combined partially with some results taken from the theory of semigroups.[1] Our approach to handle the more general equation (1.1) is based on a purely semigroup technique developed by Š. Schwarz [19] in his analysis of the classical Euler–Fermat in the form in which it was extended to more general commutative rings in [13].

2. Idempotents, maximal unipotent semigroups and groups

Let $T(\neq \emptyset)$ be a multiplicatively semigroup. Let $\langle x\rangle = \{x, x^2, x^3, \dots\}$ be the *cyclic* (also monogenic) semigroup generated by the singleton set $\{x\}$, $x \in T$. If $x \in T$ is of *finite order*, i.e. $\operatorname{card}(\langle x\rangle) < \aleph_0$, let $\kappa = \kappa(x)$ and $\delta = \delta(x)$ stand for the smallest positive integers such that $x^\kappa = x^{\kappa+\delta}$. The numbers κ, δ will be referred to as the *index* and the *period* of x, respectively. The *order of the cyclic semigroup* $\langle x\rangle$, or the *order* of x is defined as $\kappa + \delta - 1$.

If $x \in T$ is of finite order then the periodically repeating subset

$$K_x^T = \{x^\kappa, x^{\kappa+1}, \dots, x^{\kappa+\delta-1}\}$$

of $\langle x\rangle$ forms a cyclic group with respect to the multiplication in T. K_x^T is the maximal subgroup contained in $\langle x\rangle$ ([4, Exercise 1.7.4]). Its order is $\delta(x)$. The

[1] In addition he gives and comments splitting of polynomial $X^3 - X$ into linear factors over $\mathbb{Z}_{24}$ and gives 12 its decompositions into linear factors [6, p. 129]. The decomposition $(X-9)(X-16)(X-23)$ is missing in his list of factorizations of $X^3 - X$ over $\mathbb{Z}_{24}$. Notice that there is no factorization into irreducible factors involving quadratic irreducible factors in this case. This is not true in general, however, as one may conjecture using the examples given in [6].

identity element of this cyclic group, say e, is the unique idempotent of T which belongs to $\langle x\rangle$ and we say that *the element x corresponds to the idempotent e*. Let E_T denote the set of idempotents of T. A necessary and sufficient condition for a semigroup to contain a subgroup is that the set E_T of its idempotents is non-empty. The elements of a semigroup which belong to one of its subgroups are called *group elements* and they are characterized by the following simple results

Lemma 2.1. *An element of a semigroup T is a group element in T if and only if its index equals* 1.

A semigroup which each element is a group element is called a *Clifford semigroup*.[2] If a semigroup T is a union of groups, it is a union of (disjoint) groups [4, Exercise 1.7.5 & 6] and this in a unique way.

If $e \in E_T$ then $eTe = \{eae : a \in T\}$ is a subsemigroup of T with identity element e and the group of units of eTe contains every subgroup H of T that meets it ([4, Theorem 1.11]). We shall denote this group $G^T(e)$ and call it *the maximal* (*one-idempotent* or *unipotent*) *subgroups of T corresponding to the idempotent e*.

Our basic prototype semigroup used for demonstration will be the multiplicative semigroup of the ring $\mathbb{Z}_n$ of residue classes of the ring $\mathbb{Z}$ of integers modulo n. We shall identify the residue class $[x]_n = [x]$ modulo n containing x with x itself when no ambiguity are consequences of such shorthand notation.

Example 2.1. If $n = 48 = 2^4 \cdot 3$ the set of idempotents of $\mathbb{Z}_{48}$ is $E_{\mathbb{Z}_{48}} = = \{0, 1, 16, 33\}$, and $\mathbb{Z}_{48}$ has 4 maximal subgroups:

$$\begin{aligned} G^{\mathbb{Z}_{48}}(0) &= \{0\}, \\ G^{\mathbb{Z}_{48}}(1) &= \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\}, \\ G^{\mathbb{Z}_{48}}(16) &= \{16, 32\}, \\ G^{\mathbb{Z}_{48}}(33) &= \{3, 9, 15, 21, 27, 33, 39, 45\}. \end{aligned}$$

Here $\mathbb{Z}_{48}$ cannot be representable as a union of groups, e.g. 2 is not a group element as follows from Lemma 2.1. From similar reasons also $\mathbb{Z}_{24}$ or $\mathbb{Z}_{12}$ cannot be representable as a union of groups. On the other hand, $\mathbb{Z}_6$ is representable in such a way, $\mathbb{Z}_6 = \{0\} \cup \{1, 5\} \cup \{2, 4\} \cup \{3\}$.

If $e \in E_T$ and

$$P^T(e) = \{x \in T : x^n = e \text{ for some } n\}$$

[2]Thus we take into account the original definition of the Clifford semigroups as studied for the first time in [3], as the semigroups admitting relative inverses, i.e. as completely regular semigroups. The second and today more accepted variant of the Clifford's semigroups, as regular semigroups whose all idempotents are central [11] were also studied in this Clifford's paper. Nevertheless, both notions coincide in the commutative case.

then group $G^T(e)$ is the unique maximal group contained in $P^T(e)$. If T is commutative then P_e^T is a semigroup. If T is moreover a periodic semigroup then the semigroups $P^T(e)$, $e \in E_T$, form a partition of T. The set $P^T(e)$ is called the *the maximal* (*one-idempotent* or *unipotent*) *subsemigroups of* T *corresponding to the idempotent* e. For instance,

Example 2.2. The maximal one-idempotent subsemigroups of $\mathbb{Z}_{48}$ are

$$\begin{aligned} P^{\mathbb{Z}_{48}}(0) &= \{0, 6, 12, 18, 24, 30, 36, 42\}, \\ P^{\mathbb{Z}_{48}}(1) &= \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\}, \\ P^{\mathbb{Z}_{48}}(16) &= \{2, 4, 8, 10, 14, 16, 20, 22, 26, 28, 32, 34, 38, 40, 44, 46\}, \\ P^{\mathbb{Z}_{48}}(33) &= \{3, 9, 15, 21, 27, 33, 39, 45\}. \end{aligned}$$

3. A tower of Fermat–Euler Theorems

Our equations (1.1) and (1.2) are not only visually but principally connected with the classical Euler–Fermat Theorem. A general semigroup analysis of such equation in connection with this theorem was developed in [19] and in a more general form in [13]. It is based on the observation that we have a "tower" of three interlocking semigroups around every element x of a commutative periodic semigroup T:

- the monogenic subsemigroup $\langle x \rangle$ generated by x,
- the maximal subsemigroup $P^T(e)$ where e is the idempotent to which x corresponds, and
- the whole multiplicative semigroup T.

There is a correspondingly related tower of interlocking groups K_x^T, $G^T(e)$, and the group of units of T, respectively. Following Schwarz [19], we can formulate a corresponding Fermat–Euler Theorem on each of these three levels. See [19] or [13] for more details and proofs. The 'first floor' instance, is the Individual Fermat–Euler Theorem:

Lemma 3.1 (Individual Fermat–Euler Theorem)**.** *Let* T *be a commutative periodic semigroup. If* $x \in T$ *then*

$$x^{\kappa(x)+\delta(x)} = x^{\kappa(x)}$$

and the numbers $\kappa(x)$ *and* $\delta(x)$ *are the least positive numbers with this property. Moreover if* $x^{s+h} = x^s$ *then* $s \geq \kappa(x)$ *and* $\delta(x) \mid h$.

Let semigroup T be commutative and periodic. Let T have the property that the orders of the all its cyclic semigroups $\langle x\rangle$, $x \in T$, have a uniform finite bound. Then T will be called the *Fermat–Euler-semigroup* (shortly FE-semigroup). In this case we define the numbers κ_t, and δ_T by the following relations

$$\kappa_T = \max\{\kappa(x) : x \in T\},$$
$$\delta_T = \text{l.c.m.}\{\delta(x) : x \in T\}.$$

The reason for the name FE-semigroup is the following result (cf. also [13]):

Lemma 3.2 (Global Fermat–Euler Theorem)**.** *Let T be a FE-semigroup. Then for every $x \in T$ we have*

$$x^{\kappa_T+\delta_T} = x^{\kappa_T}$$

and the numbers κ_T, δ_T are the least positive integers such that this equality holds for each $x \in T$. Moreover if $x^{s+h} = x^s$ for every $x \in R$, then $s \geq \kappa_T$ and $\delta_T \mid h$.

We can also apply the idea of the Global Fermat–Euler Theorem to the maximal unipotent semigroups $P^T(e)$ in the following way. For $e \in E_T$, define

$$\kappa_T(e) = \max\{\kappa(x) : x \in P^T(e)\},$$
$$\delta_T(e) = \text{l.c.m.}\{\delta(x) : x \in P^T(e)\}.$$

Then for the maximal semigroup $P^T(e)$ we obtain

Lemma 3.3 (Local Fermat–Euler Theorem)**.** *Let T be a FE-semigroup. If $e \in E_T$, then for every $x \in P^T(e)$ we have*

$$x^{\kappa_e+\delta_e} = x^{\kappa_e}.$$

The numbers κ_e, δ_e are the least positive integers such that this equality holds for each $x \in P^T(e)$. Moreover if $x^{s+h} = x^s$ for every $x \in P^T(e)$ then $s \geq \kappa_e$ and $\delta_e \mid h$.

4. Solutions over commutative rings

The impetus to this note was given by a result involving the ring of integers $\mathbb{Z}$. In what follows we shall investigate the above mentioned problem over some classes of commutative rings containing ring $\mathbb{Z}$ as a special case. In what

follows *R will denote a commutative ring with the identity element* $1 = 1_R$, and E_R will denote the set of idempotents of the multiplicative semigroups $(R, \cdot)$ of R. Since $1_R \in E_R$, set E_R is non-empty.

Given positive integers $m > s \geq 1$, let $S^R(m, s)$ denote the set of elements of $x \in R$ satisfying equation (1.1). Since R is commutative and $E_R \subset S^R(m, s)$, $S^R(m, s)$ is a non-empty subsemigroup of the multiplicative semigroup $(R, \cdot)$ of ring R. Moreover

$$P^{S^R(m,s)}(e) = S^R(m, s) \cap P^R(e), \quad e \in E_R.$$

The following result shows a general sufficient condition when $S^R(m, s)$ is a union of groups:

Theorem 4.1. *Let R be a commutative ring with the identity element and $m \geq 2$. Then semigroup $S^R(m, 1)$ is a Clifford one, i.e. $P^{S^R(m,1)}(e)$ is a subgroup of $G^{S^R(m,1)}(e)$ for each $e \in E_R$.*

Proof. Semigroup $S^R(m, 1)$ is a periodic commutative semigroup. If $x \in$ $\in S^R(m, 1)$, then relation $x^m = x$ implies that x is of index 1, that is every element of $S^R(m, 1)$ is a group element (Lemma 2.1). Consequently $S^R(m, 1)$ is a union of groups (cf. also [4, Exercise 1.6.5 & Exercise 1.7.6(a)] or [17]). ■

Even if the previous Theorem shows that the set of solutions to $X^m \equiv X \pmod{n}$ over $\mathbb{Z}_n$, $n \in \mathbb{Z}$ is a union of groups, it is not necessarily the union of the maximal one-idempotent groups $G^R(e)$, as the next Example shows

Example 4.2. The following subgroups of maximal one-idempotent groups in $\mathbb{Z}_{48}$ form a partition of the semigroup $S^{\mathbb{Z}_{48}}(3, 1)$ of solutions to $X^3 \equiv X \pmod{48}$

$$\begin{aligned}
P^{S^{\mathbb{Z}_{48}}(3,1)}(0) &= \{0\} = G^{\mathbb{Z}_{48}}(0),\\
P^{S^{\mathbb{Z}_{48}}(3,1)}(1) &= \{1, 7, 17, 23, 25, 31, 41, 47\} \subsetneq G^{\mathbb{Z}_{48}}(1),\\
P^{S^{\mathbb{Z}_{48}}(3,1)}(16) &= \{16, 32\} = G^{\mathbb{Z}_{48}}(16),\\
P^{S^{\mathbb{Z}_{48}}(3,1)}(33) &= \{9, 15, 33, 39\} \subsetneq G^{\mathbb{Z}_{48}}(33).
\end{aligned}$$

Despite this, there is a class of situation when the set of solutions $S^{\mathbb{Z}_n}(m, 1)$ is the union of the maximal one-idempotent groups $G^{\mathbb{Z}_n}(e)$, $e \in E_{\mathbb{Z}_n}$. For instance, if $n = 24$ then for the same polynomial congruence $X^3 \equiv X$ we have $P^{S^{\mathbb{Z}_{24}}(3,1)}(e) = G^{\mathbb{Z}_{24}}(e)$ for every idempotent e of $\mathbb{Z}_{24}$. This case was used as a demonstration supporting the mentioned result claimed in [6]. In this section we show a correction to this result in more general settings. Namely for commutative rings and some so-called residually finite commutative rings.

Our approach will be based on an idempotent technique developed in [13]. In this setting we shall also address some related questions, e.g. for which n and $e \in E_{\mathbb{Z}_n}$ we have $G^{S^{\mathbb{Z}_n}(m,1)}(e) = G^{\mathbb{Z}_n}(e)$, etc.

Notice that if $s > 1$, the semigroup $P^{S^R(m,s)}(e)$ need not be a group in general as the following Example shows:

Example 4.3. Consider the ring $\mathbb{Z}_{48}$ and $m = 4$, $s = 2$. Then the partition of the set $S^{\mathbb{Z}_{48}}(4,2)$ of solutions to $X^4 \equiv X^2 \pmod{48}$ in $\mathbb{Z}_{48}$ into subsemigroups of the maximal one-idempotent semigroups of $\mathbb{Z}_{48}$ is:

$$\begin{aligned} P^{S^{\mathbb{Z}_{48}}(4,2)}(0) &= \{0, 12, 24, 36\}, \\ P^{S^{\mathbb{Z}_{48}}(4,2)}(1) &= \{1, 7, 17, 23, 25, 31, 41, 47\}, \\ P^{S^{\mathbb{Z}_{48}}(4,2)}(16) &= \{4, 8, 16, 20, 28, 32, 40, 44\}, \\ P^{S^{\mathbb{Z}_{48}}(4,2)}(33) &= \{9, 15, 33, 39\}. \end{aligned}$$

The corresponding maximal one-idempotent subgroups of $S^{\mathbb{Z}_{48}}(4,2)$ are identical to those appearing in case $S^{\mathbb{Z}_{48}}(3,1)$ from a reason which will be explained later in Corollary 4.7.

In this example $P^{S^{\mathbb{Z}_{48}}(2,4)}(16)$ is not a group. Exercise 4 of [4, § 1.9] implies that $P^{S^R(m,s)}(e)$ is not even a regular semigroup for $s > 1$ in general. In $P^{S^{\mathbb{Z}_{48}}(4,2)}(16)$ the elements $4, 8, 20, 28, 40, 44$ are not regular, but 16 and 32 as group elements are regular.

It is even possible that maximal unipotent subsemigroups of $S^R(m,s)$ reduce to trivial subgroups, namely subgroups of the form $\{e\}$ where $e \in E_T$ as the following example shows.

Example 4.4. We have

$$\begin{aligned} P^{S^{\mathbb{Z}_{48}}(5,2)}(0) &= \{0, 12, 24, 36\}, \\ P^{S^{\mathbb{Z}_{48}}(5,2)}(1) &= \{1\}, \\ P^{S^{\mathbb{Z}_{48}}(5,2)}(16) &= \{4, 16, 28, 40\}, \\ P^{S^{\mathbb{Z}_{48}}(5,2)}(33) &= \{33\}. \end{aligned}$$

That $G^{S^{\mathbb{Z}_{48}}(5,2)}(e) = \{e\}$ for all $e \in E_{\mathbb{Z}_{48}}$ follows from the fact that $d(x) = 1$ for all elements of $S^{\mathbb{Z}_{48}}(5,2)$ (by the way, we have $k(x) = 2$ for all non-idempotent elements of $S^{\mathbb{Z}_{48}}(5,2)$).

The semigroups which are union of groups take a significant place in the theory of semigroups. In our situation this is the case, e.g. for multiplicative semigroups of rings $\mathbb{Z}_n$ where n is a square-free integer, as we shall see later.[3]

[3] In this connection see also footnote 7 on p. 161.

Theorem 4.5. *Let R be a commutative ring with the identity element and let its multiplicative semigroup be a Clifford one. Then every semigroup $S^R(m,s)$ for $m > s \geq 1$ is also Clifford, that is $P^{S^R(m,s)}(e)$ is a subgroup of $G^{S^R(m,1)}(e)$ for every idempotent $e \in E_R$.*

Proof. We again show that $S^R(m,s)$ is a Clifford semigroup. Let $a \in \in S^R(m,s)$. Since $(R,\cdot)$ is a union of groups, there exists the inverse a^{-1} of a in R. Clearly $a^{-1} \in S^R(m,s)$, for $(a^{-1})^j = (a^j)^{-1}$ for both $j = m$ and $j = s$, and the conclusion follows. ■

In the case of finite commutative rings, the proof is even formally simpler. It follows from the fact that a finite group has only groups as subsemigroups as it follows, for instance from Theorem 33 of [18].

4.1. Solutions over commutative residually finite domains

If R satisfies the following finiteness condition

(FN) *For every non-zero ideal $I \subset R$ the residue class ring R/I is finite.*

we say that R is *residually finite*. The class of residually finite rings contains besides trivial class of all finite rings also, for instance,

- the ring of integers;
- polynomial rings $F[X]$ over a finite field F;
- the formal power rings $F\{X\}$ over a finite field F,
- if R is residually finite then the ring of $n \times n$ matrices with entries from R is also residually finite (and vice verse) ([1, Proposition 2.5]);
- if $K \subset \mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$, the the ring $A = K \cap \mathbf{A}$ is a residually finite ring, where $\mathbf{A}$ is the ring of all algebraic integers (cf. also [12, Theorem 1]).

Though the infinite cyclic group is the only infinite commutative group in which every non-zero subgroup is of finite index, in the case of commutative rings the situation is different. The following lemma shows some restrictions on rings caused by imposing the requirement of the (FN) property:[4]

[4]There appears also another definition of residually finiteness in algebra. An associative ring (resp. a group) is said to be residually finite if for each non-zero (respectively, non-identity) element x there is a two sided ideal (respectively, normal subgroup) not containing x and such that the residue class ring (respectively, group) is finite. Under these definitions of the residual finiteness the residually finite groups and rings seem to possess analogous properties.

Lemma 4.1 ([1]). *Let R be a commutative ring (not necessarily with the identity element).*

- *If R is residually finite then it is an integral domain* ([12]).
- *R is residually finite if and only if every non-zero prime ideal of R is finitely generated and of finite index in R* ([1, Corollary 2.4]).

Let R be a commutative residually finite ring and I be its non-trivial ideal. If $a \in R$ then

$$[a] = [a]_I = a + I$$

will denote the residue class containing element $a \in R$ in R/I. Since the representation of a residue class $[a]$ does not depend on the choice of its representative a, we shall freely switch between the residue class $[a]$ and its representatives a to avoid cumbersome phrasing and notation when working with R/I, as we have already done when working with $\mathbb{Z}_n$'s. Since the multiplicative semigroup of R/I is commutative and periodic (even finite), we can apply previous ideas to the set of solutions to congruence

$$x^m \equiv x^s \pmod{I} \tag{4.1}$$

over the ring R/I of residue classes modulo I, where $m > s \geq 1$ are given positive integers.

If similarly, as above, $S^{R/I}(m,s)$ with $m > s \geq 1$ will denote the set of elements of $[x] \in R/I$ satisfying the equation $[x]^m = [x]^s$ then we get from Theorem 4.1:

Corollary 4.1. *Let R be a commutative residually finite ring with the identity element and I its non-trivial ideal. If $m \geq 2$, then each $S^{R/I}(m,1)$ is a Clifford semigroup. More precisely, $P^{S^{R/I}(m,1)}(e)$ is a subgroup of $G^{S^{R/I}(m,1)}(e)$ for each idempotent e of $(R/I,\cdot)$.*

Theorem 4.5 implies the following result

Corollary 4.2. *Let R be a commutative residually finite ring with the identity element and I its non-trivial ideal. Let the ideal I have the property that the multiplicative semigroup of R/I is a Clifford semigroup. Then semigroup $S^{R/I}(m,s)$ with $m > s \geq 1$, is also a Clifford one. More precisely, $P^{S^{R/I}(m,s)}(e)$ is a subgroup of $G^{S^{R/I}(m,s)}(e)$ for each idempotent e of $(R/I,\cdot)$.*

4.2. Solutions over residually finite PID's

In what follows we shall solely work with *(commutative) residually finite principal ideal domains R with identity element $1 = 1_R$*. Further, $I = (n)$ will

stand for a non-trivial ideal, i.e. n is a non-invertible element other than zero. Denote $R/(n) = R_n$.

Notice that an independent direct ring-theoretical proof of Corollary 4.1 can be given if R is a commutative residually finite PID with the identity element. Namely, if R is a PID, it is a GCD-domain, i.e. we have uniquely (up to a divisor of 1) defined the GCD of every couple of its elements. Its group elements can be characterized as follows:

Lemma 4.2 ([8, Theorem 11] or [13, Theorem 2.4])**.** *Let R be a PID with the identity element and $n \in R$ be a non-invertible element other than zero. Then the element $x \in R_n$ is a group member in R_n if and only if*

$$\gcd\left(\frac{n}{\gcd(n,x)}, x\right) = 1. \tag{4.2}$$

Now, let $x \in R_n$ satisfy congruence $x^m \equiv x \pmod{n}$ for some $m \geq 2$. Consequently, $\gcd(x,n) = \gcd(x^m, n)$ for they belong to the same residue class mod n. This implies that every irreducible divisor of n divides x in the same power as it divides n, i.e. (4.2) holds, and Corollary 4.1 follows.

Residually finite PID's allow an easy construction of ideals satisfying assumptions of Corollary 4.2. Since such a ring R is a UFD, an element $1_R \neq n \in R$ is called *square-free* if it is not divisible by a square of an irreducible element of R. Theorem 2.6 of [13] implies that the ideals generated by square-free elements $n \in R$ satisfy the assumption of Corollary 4.2, i.e. that every element of R_n is a group element. On the other hand, the mentioned example of $X^3 - X$ over $\mathbb{Z}_{24}$ from [6] shows that the assumptions of Corollary 4.2 are not necessary for the conclusion.

Two simple applications of Corollary 4.2, to our knowledge not noticed up to now, follow immediately:

1) In a standard RSA cryptosystem the modulus is taken to be a square-free number of the form $n = pq$, where p, and q are distinct primes. We can formally extend the idea of this classical version of the RSA cryptosystem in several directions: (i) to take the modulus with more than 2 prime factors, or (ii) to consider this cryptosystem over a residually finite principal ideal domain and redefine verbatim all the basic notions and procedures used in RSA. The first case is even supported by the PKCS#1 standard [16], the so called Multi Prime RSA.[5] The second one aims in finding more factorization resistent domains, though in the number-theoretical UFD's the factorization is often easier, or equivalent to factorization over the integers (cf. e.g. [5, 20] or [9]). In either case we obtain the following application

[5] On the plus size, this may offer some performance improvement. On the negative side, using too small factors may weaken the modulus.

Corollary 4.3. *Let R be a residually finite PID with the identity element and I its ideal generated by a square-free element n. If k is a positive integer then the set of cipher texts of a plain text with iteration exponent*[6] *k and given modulus n is a Clifford semigroup.*

2) If $R = Z$, then Corollary 4.1 shows that more generally[7], the same conclusion is true for the solutions to the congruence

$$x^n \equiv x \pmod{n} \tag{4.3}$$

Typical prototypes of such a congruences appear in connection with (Fermat) pseudoprimes or Carmichael numbers n, where the well-known Korselt's criterion [15] implies that every Carmichael number is square-free,

Corollary 4.4. *The set of solutions to the congruence* (4.3) *is a Clifford semigroup.*

The following Example demonstrates the previous result for the first Carmichael number:

Example 4.6. Let $n = 341$, then all 121 solutions to (4.3) split into four groups $G^{S^{\mathbb{Z}_{341}}(341,1)}(0) = G^{\mathbb{Z}_{341}}(0)$, $G^{S^{\mathbb{Z}_{341}}(341,1)}(1) \subsetneq G^{\mathbb{Z}_{341}}(1)$, $G^{S^{\mathbb{Z}_{341}}(341,1)}(155) = = G^{\mathbb{Z}_{341}}(155)$, and $G^{S^{\mathbb{Z}_{341}}(341,1)}(187) \subsetneq G^{\mathbb{Z}_{341}}(187)$.

Remark 4.1. We used the assumption of residual finiteness of R to ensure that the multiplicative semigroups of reside class rings R/I are periodical semigroups. We can achieve a similar conclusion reducing the attention instead to all proper ideals I of R, only to some classes of its ideals. For instance, if R stands for an integral domain and I is a non-zero ideal of R such that $I = P_1^{r_1} P_2^{r_2} \dots P_t^{r_t}$, where $P_1, P_2, \dots, P_t$ are distinct invertible maximal ideals of R and r_i, $i = 1, 2, \dots, t$ are positive integers, then R/I is a principal ideal domain which multiplicative semigroup is an epigroup, and, moreover, it is a complete lattice of unipotent epigroups (cf. [2] for more details in this connection).

Firstov's claim immediately induces already mentioned natural questions when $P^{S^{R/I}(m,s)}(e) = P^{R/I}(e)$ or when $P^{S^{R/I}(m,s)}(e) = G^{R/I}(e)$. To answer this questions we need a more detailed knowledge of the structure of the maximal unipotent semigroups and maximal unipotent groups of the residue class rings R/I. This information for residue class rings of residually finite PID's

[6] If necessary, for more details consult e.g. [21].

[7] Notice that in $\mathbb{Z}_n$ we have (cf. [19] or [10]): The congruence $x^L \equiv x \pmod{n}$ with some $L > 1$ holds for all $x \in \mathbb{Z}_n$ if and only if n is square-free. The least L having this property is $L = \lambda(n) + 1$ where λ stands for the Carmichael function.

is given in [13]. To use these results we need some additional notation and terminology.

Every PID is a UFD. Therefore given an ideal $I = (n)$ of R, the elements of the residue class $[x]_n$ modulo I have a uniquely, up to a unit, determined GCD with n. If $t = \gcd(x, n) = \gcd([x]_n, n)$ we say that x *corresponds to the divisor* t (of n). Let

$$n = \varepsilon p_1^{u_1} \dots p_s^{u_s} \tag{4.4}$$

be the decomposition of $n \in R$ into irreducible non-associated elements of R where ε is an invertible element and u_i's are positive integers. The *radical* of an element $x \in R_n$, denoted $\mathrm{rad}(x)$, is the product of the distinct prime factors of x. We have

Lemma 4.3 ([13, Theorem 2.3])**.** *Let R be a residually finite PID with the identity element. Then $[x] \in R_n$ corresponds to the idempotent $e \in R_n$ if and only if* $\mathrm{rad}(x) = \mathrm{rad}(e)$.

Notice that if $e, f \in E_{R_n}$ and $e \neq f$, then $\mathrm{rad}(e) \neq \mathrm{rad}(f)$. The next result gives an expression for $\kappa(x)$.

Lemma 4.4 ([8, Lemma 3], [13, Theorem 2.5])**.** *Let R be a residually finite PID with the identity element. Let $n \in R$ be an non-invertible element other than zero with factorization* (4.4)*. Let $[x] \in R_n$ be an element corresponding to divisor $t = p_1^{v_1} \dots p_s^{v_s}$ of n, where $0 \leq v_j \leq u_j$, $1 \leq j \leq s$. Then*

$$\kappa(x) = \begin{cases} 1 & \text{if } t = 1, \\ \max\left\{ \left\lceil \frac{u_j}{v_j} \right\rceil : 1 \leq j \leq s, v_j \neq 0 \right\} & \text{otherwise.} \end{cases}$$

A divisor $t \in R$ of an element $n \in R$ is called a *unitary divisor* if $\gcd\left(t, \frac{n}{t}\right) = 1$. The idempotents of the residue class ring R_n correspond in a one to one way to those residue classes in R_n which correspond to the unitary divisors of n (cf. [13, Theorem 2.1] or (4.2)).

Lemma 4.4 (or Lemma 4.2) implies

Corollary 4.5. *Let R be a residually finite PID with the identity element. Then $[x] \in R_n$ is a group element in R_n if and only if x corresponds to a unitary divisor of n.*

If $m = \varepsilon q_1^{w_1} \dots q_s^{w_s}$ is the decomposition of $m \in R$, ε a unit, into irreducible non–associated elements in a unique factorization ring R, then define

$$\eta^R(m) = \max\{w_i \ ; \ i \in \{1, \dots, s\}\}.$$

Formula giving the value of κ_e can be now given explicitly:

Lemma 4.5 ([13, Theorem 2.6(i)]). *Let R be a residually finite PID with the identity element. Let $[e]$ be an idempotent in R_n corresponding to the unitary divisor t of n. Then $\kappa_e = \eta^R(t)$ and $\kappa_0(=: \kappa_{R_n}) = \eta^R(n)$.*

To give a formula for δ_e is a more complex problem. Since δ_e is the exponent of the group $G^{R_n}(e)$, to give an explicit formula for δ_e we need a precise structural characterization of this group. Unfortunately this is known only in some special cases. For instance, in the case $R = \mathbb{Z}$ the value of δ_e is given by Carmichael function λ. More precisely, if idempotent e corresponds to the unitary divisor t of n, then the exponent of $G^{\mathbb{Z}_n}(e)$ equals $\lambda(n/t)$ and $\delta_1 = \delta_{R_n} = \lambda(n)$. For related examples of rings of algebraic integers consults for an overview for formulas for analogs of Carmichael function paper [13] or [7].

The numbers $\delta(x)$, δ_e are exponents of groups K_x^T, and $G^T(e)$, respectively. For δ_T we have

Lemma 4.6. *Let T be the multiplicative semigroups of a finite commutative ring R with the identity element. Then δ_T is the exponent of $G^T(1)$ and the exponent $\delta(e)$ of $G^T(e)$ divides δ_T for every $e \in E_T$,.*

Proof. We know (cf. [13, Theorem 1.5]) that in a finite commutative ring R we have $G^R(1)e = G^R(e)$, and that [13, Lemma 1.6(ii)] mapping $x \mapsto xe$ is a group homomorphism of group $G^R(1)$ onto $G^R(e)$. Since the order of a homomorphic image of a finite group divides its order, the Lemma follows. ■

Remark 4.2. Notice that for a general commutative semigroup with the identity element we have the one-sided inclusion $G^T(1)e \subset G^T(e)$ only. To see this recall that ([4, Exercise 3, p. 23]) we have $G^T(e) = \{x \in T : xe = x \text{ and } xy = = e \text{ for some } y \in T\}$.

We now turn to the question when $P^{S^{R_n}(m,s)}(e) = P^{R_n}(e)$ for an idempotent e in R_n if $I = (n)$ is an non-trivial ideal of a residually finite PID R. In the cases when $P^{R_n}(e)$ is actually a group this will simultaneously answer the question when $P^{S^{R_n}(m,s)}(e)$ is the maximal unipotent group corresponding to idempotent e.

The Individual Fermat–Euler Theorem implies the following characterization of $P^{S^T(m,s)}(e)$ and $G^{S^T(m,s)}(e)$:

Theorem 4.7. *Let R be a residually finite PID with the identity element and I its ideal generated by an element n. Let $1 \leq s < m$. Then for $e \in E_{R_n}$ we*

have

$$\begin{aligned} P^{S^{R_n}(m,s)}(e) &= \{x \in P^{R_n}(e) : \kappa(x) \le s, \delta(x) \mid (m-s)\} = \\ &= \{x \in R_n : \mathrm{rad}(x) = \mathrm{rad}(e), \kappa(x) \le s, \delta(x) \mid (m-s)\}, \\ G^{S^{R_n}(m,s)}(e) &= \{x \in P^{R_n}(e) : \kappa(x) = 1, \delta(x) \mid (m-s)\} = \\ &= \{x \in G^{R_n}(e) : \delta(x) \mid (m-s)\} = \\ &= \{x \in R_n : \mathrm{rad}(x) = \mathrm{rad}(e), \kappa(x) = 1, \delta(x) \mid (m-s)\}. \end{aligned}$$

Proof. We clearly have $P^{S^{R_n}(m,s)}(e) \subset P^{R_n}(e)$. If an $x \in P^{R_n}(e)$ satisfies the conditions $\kappa(x) \le m$ and $\delta(x) \mid (m-s)$ then the Individual Fermat–Euler Theorem implies that $x^m = x^s$, i.e. $x \in P^{S^{R_n}(m,s)}(e)$.

The statement about $G^{S^{R_n}(m,s)}(e)$ follows from the fact that $G^{S^{R_n}(m,s)}(e) = P^{S^{R_n}(m,s)}(e) \cap G^{R_n}(e)$. ■

Note that the elements with $\kappa(x) = 1$ are just group elements in every R_n which gives a further proof of Theorem 4.1 provided $m = 1$.

Corollary 4.6. *Under the assumption of Theorem* 4.7 *there holds that* $P^{S^{R_n}(m,s)}(e) = P^{R_n}(e)$ *if and only if* $s \ge \max\{\kappa(x) : x \in P^{R_n}(e)\} = \eta^{R_n}(d)$ *and* $\delta_e \mid (m-s)$, *where* d *is the unitary divisor to which* e *corresponds.*

To the proof note that as in the previous proof the conditions $m \ge \kappa(x)$ and $\delta_x \mid (m-s)$ are necessary and sufficient for an $x \in P^{R_n}(e)$ to satisfy $x^m = x^s$.

Theorems 4.7 and 4.6 imply

Corollary 4.7. *Under the assumption of Theorem* 4.7 *there holds that* $P^{S^{R_n}(m,s)}(e) = G^{R_n}(e)$ *if and only if* $\kappa_e = \eta^{R_n}(d) = 1$ *and* $\delta_e \mid (m-s)$, *where* d *is the unitary divisor to which* e *corresponds.*

These results show an interesting dependency not on the values m and s themselves but only on their difference.

Corollary 4.8. *If under the assumption of Theorem* 4.7 *we have that* $\gcd(\delta_e, m-s) = t$ *for an* $e \in E_{R_n}$, *then the exponent of* $G^{S^{R_n}(m,s)}(e)$ *equals* t, *or in other words the order of any element in* $G^{S^{R_n}(m,s)}(e)$ *divides* t.

Proof. The proof follows from two basic facts about finite commutative groups:

• a finite commutative group of order g has a subgroup of order h for every divisor h of g,

• in a finite commutative group of exponent f there is an element whose order is f. ■

Thus for instance[8], if R is a residually finite PID with the identity element and if the exponent of $G^{R_n}(1)$ is coprime to $m - s$ then so are the exponents of all groups $G^{R_n}(e)$. Therefore in such a case all the $G^{S^{R_n}(m,s)}(e)$'s are trivial groups as it was the case with $S^{\mathbb{Z}_{48}}(5, 2)$ in Example 4.4.

As mentioned, an effective characterization of the structure of $G^T(e)$ within $P^T(e)$ is known only in some classes of commutative semigroups T. We know (cf. [13, p. 260]) that in a finite commutative ring R we have $G^R(e) = P^R(e)e$ or that $G^R(e) = P^{eR}(e)$ for $e \in E_R$. There follows form the first identity that always $P^R(1) = G^R(1)$, that is $P^R(1)$ is always a group. As there follows from the lines above, if $\eta^R(n) = 1$ (i.e. n is square-free) then every $P^{R_n}(e)$ is a group. More precisely, if idempotent e corresponds to unitary divisor d of $n \in R$ such that $\eta^R(d) = 1$ then $P^{R_n}(e)$ is a group. If $\eta^R(d) \geq 2$ then $P^{R_n}(e)$ is not necessarily a group.

Remark 4.3. The used technique can be applied to more general structures. For instance, a corresponding more general analysis for residually finite Dedekind domains is done in [13]. In this case, as already mentioned above, we have all the necessary information about the structure of the maximal unipotent semigroups and maximal unipotent groups of the multiplicative semigroups for rings of algebraic integers. The reader is referred to [13] for more details.

References

[1] **Chew, K.L. and S. Lawn,** Residually finite rings. *Can. J. Math.* **22** (1970) 92–101.

[2] **Cao, Y.**, Multiplicative semigroup of a residue class ring, *Semigroup Forum* **70** (2005) 361–368.

[3] **Clifford, A. H.**, Semigroups admitting relative inverses, *Ann. Math.* **42** (4) (1941) 1037–1049.

[4] **Clifford, A.H. and G.B. Preston,** *The algebraic theory of semigroups*, Vol. I., Mathematical Surveys. 7. American Mathematical Society, XV, Providence, R.I. 1961.

[5] **El-Kassar, A.-N., R.A. Haraty and Y. Awad,** Modified RSA in the domains of Gaussian integers and polynomials over finite fields, Proceedings of the ISCA 18th International Conference on Computer Applications in Industry and Engineering, November 9-11, 2005, Sheraton Moana Surfrider, Honolulu, Hawaii, USA.

[8] This follows from Lemma 4.6 too.

[6] **Firstov, V.E.,** Periodic semigroups in the ring of residue classes. *Chebyshevskiĭ Sb.*, **13** (2(42)) (2012) 124–130.

[7] **Farahat, H.K.,** The multiplicative groups of a ring, *Math. Z.* **87** (1965), 378–384.

[8] **Farahat, H.K. and L. Mirsky,** Group membership in rings of various types, *Math. Z.* **70** (1958) 231–244.

[9] **Hashiguchi, K., K. Hashimoto and S. Jimbo,** Modified RSA cryptosystems over bicodes, In: Advances in algebra. Proceedings of the ICM satellite conference in algebra and related topics, Hong Kong, China, August 14–17, 2002, River Edge, NJ: World Scientific 2003, pp. 377–389.

[10] **Hewitt, E.,** Certain congruences that hold identically. *Amer. Math. Monthly*, **83** (1976) 270271.

[11] **Howie, J.M.,** *Fundamentals of Semigroup Theory*, Clarendon Press, Oxford 1995.

[12] **Ion, I.D. and C. Niţă,** Residually finite subrings of the ring of algebraic integers, *An. Univ. Bucur., Mat.* **56** (2) (2007) 231–234.

[13] **Laššák, M. and Š. Porubský,** Fermat–Euler theorem in algebraic number fields, *J. Number Theory* **60** (2) (1996) 254–290.

[14] **Munn, W.D.,** Pseudo-inverses in semigroups, *Proc. Camb. Philos. Soc.* **57** (2) (1961) 247–250.

[15] **Korselt, A.R.,** Probleme chinois. *L'Intermédiaire des Mathématiciens.* **6** (1899) 142–143.

[16] PKCS#1v2.2: RSA Cryptography Standard, RSA Laboratories, October 2012, `https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf#page=8`.

[17] **Poole, A.R.,** Finite ova, *Am. J. Math.* **59** (1937) 23–32.

[18] **Rédei, L.,** *Algebra*, International Series of Monographs in Pure and Applied Mathematics. Vol. 91, Pergamon Press, Oxford 1967.

[19] **Schwarz, Š.,** The role of semigroups in the elementary theory of numbers, *Math. Slovaca* **31** (4) (1981) 369–395.

[20] **Vaskouski, M. and N. Kondratyonok,** Analogue of the RSA-cryptosystem in quadratic unique factorization domains, *Dokl. Nats. Akad. Nauk Belarusi* **59** (5) (2015) 18–23.

[21] **de Vries, A.,** The ray attack, an inefficient trial to break RSA cryptosystems, `https://arxiv.org/abs/cs/0307029`

Š. Porubský
Institute of Computer Science
Academy of Sciences of the Czech Republic
Pod Vodárenskou věží 2
1802 07 Prague,
Czech Republic
and
Department of Mathematics
Faculty of Sciences
University of Ostrava
30. dubna 22
701 03 Ostrava 1
Czech Republic
sporubsky@hotmail.com