ON SMARANDACHE'S FORM OF THE INDIVIDUAL FERMAT–EULER THEOREM

ŠTEFAN PORUBSKÝ

Appeared in: Proceedings of the first international conference on Smarandache type notions in number theory, *(C.Dumitrescu, V.Seleacu eds.) American Research Press 1997, 163–178, and reprinted in* Smarandache Notions Journal **8**, *no. 1–3, 1997, 5–20.*

Dedicated to the memory of the late Professor Štefan Schwarz

Abstract. In the paper it is shown how a form of the classical Fermat–Euler Theorem discovered by F.Smarandache fits into the generalizations found by Š.Schwarz, M.Laššák and the author. Then we show how Smarandache's algorithm can be used to effective computations of the so called group membership.

1. Variations on Fermat–Euler theorem

In [Schw81] a semigroup approach to the Fermat–Euler Theorem was developed

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \qquad (a,n) = 1$$

based on an idempotent technique giving the best possible extensions of this fundamental result to the set $\mathbb{Z}$ of the all integers. In [LaPo96] the idea was generalized to finite commutative rings R and subsequently to the *residually finite* Dedekind domains, that is Dedekind domains R satisfying the finiteness condition:

(FN) *For every non–zero ideal $\mathfrak{M} \subset R$ the residue class ring $R/\mathfrak{M}$ is finite.*

A detailed specialization of these results depends then upon a corresponding detailed knowledge of the structure of the group of units (i.e. invertible elements) of the corresponding residue class ring $R/\mathfrak{M}$. The most known prototypes of rings where this knowledge is available are, besides $\mathbb{Z}_n$ the ring of residue classes modulo n, the algebraic number fields. Thus for instance, for residually finite Dedekind domains we only have Lemma 8 in general. For algebraic number fields see [LaPo96].

1.1. **Semigroup level.** The basic underlying idea of the proofs of generalizations of Fermat–Euler Theorem given in [Schw81] and [LaPo96] is based on the some elementary semigroup ideas. To describe them we shall suppose in this Section that S is a finite commutative semigroup written multiplicatively.

Given an $x \in S$, the sequence

$$x,\ x^2,\ x^3,\ \ldots \qquad x \in S \tag{1}$$

contains some of its elements multiple times. If we denote by $k = k(x) \in \mathbb{N}$ (here $\mathbb{N}$ is the set of positive integers) the least such exponent for which x^k appears at least

Date: September 15, 2015.

1991 *Mathematics Subject Classification.* 11A07, 11R04, 11T99, 11Y16, 13F05 .

Key words and phrases. Fermat–Euler theorem, Dedekind domain, residually finite ring, idempotent, unitary divisor, Carmichael function.

Research supported by the Grant Agency of the Czech Republic, Grant # 201/97/0433.

twice in (1) and $d = d(x)$ the least exponent with $x^k = x^{k+d}$, then the sequence (1) has the form

$$x, x^2, \ldots, x^{k-1}, x^k, \ldots, x^{k+d-1}, x^k, \ldots$$

The next elementary result is instrumental in the investigations which follow:

Lemma 1 (Frobenius 1895)**.** *For every $x \in S$ the set*

$$C(x) = \{x^k, \ldots, x^{k+d-1}\} \tag{2}$$

forms a cyclic group with respect to the multiplication.

The identity element $e = x^r, r = r(x)$ of the group $C(x)$ is the unique idempotent of R which belongs to (1). This connections are described saying *the element x belongs to the idempotent e.*

The above observations imply (see also proof of Theorem 1.9 in [LaPo96]):

Proposition 1 (Individual Fermat – Euler Theorem)**.** *If $\kappa, \delta \in \mathbb{N}$ with $\kappa \geq k(x)$, $d(x) \mid \delta$, then for every $x \in S$ we have*

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

and the numbers $k(x)$ and $d(x)$ are the least positive numbers possessing this property.

The main problem here is to determine the exact values of $k(x)$ and $d(x)$. As mentioned above, more knowledge about S is required for this task. In the process of the determination of values of these numbers further structural results are needed. To make the paper self–contained we shall outline some crucial facts, the reader is referred to [LaPo96] for more details. Of basic importance are properties of the idempotents.

Let E_S denote the set of idempotents of S. Let $e \in E_S$. Then the set

$$P^S(e) = \{x \in S \,;\, x \text{ belongs to } e\}$$

is the largest subsemigroup of S, which except for e contains no other idempotent of S. This uniquely determined maximal subsemigroup $P^S(e)$ will be called the *maximal (multiplicative) semigroup (of semigroup S) belonging to the idempotent $e \in E_S$*. Note that

$$S = \bigcup_{e \in E_S} P^S(e).$$

Moreover, if $e \in E_S$ is an idempotent in S, then there always exists a subgroup of S containing e as its identity, e.g. the group $\{e\}$ or the group $C(x)$ of Lemma 1 provided x belongs to the idempotent e. Since S is finite, there exist maximal subgroup of S amongst the all subgroups of S for which e serves as the identity element. We shall call this group $G^S(e)$ the *maximal (multiplicative) subgroup of S belonging to the idempotent $e \in E_S$*. It is surprising that the existence of these subgroups is almost unknown in the classical number theory.

Given an idempotent $e \in E_S$, define

$$k_e = \max\{k(x) \,;\, x \in P^S(e)\}, \qquad d_e = \text{l.c.m.}\{d(x) \,;\, x \in P^S(e)\}$$

and

$$k_S = \max\{k(x) \,;\, x \in S\}, \qquad d_S = \text{l.c.m.}\{d(x) \,;\, x \in S\}.$$

The algebraic meaning of numbers $k(x), d(x)$ for $x \in S$, k_e, d_e for $e \in E_S$, k_S, and d_S is best explained by the next results [LaPo96, p.268]:

Lemma 2. *For any $x \in S$*
(a) Every of $x^{k(x)}, x^{k_e}, x^{k_S}$ is an element of a subgroup of S. More precisely, $x^{k(x)} \in C(x)$, $x^{k_e} \in G^S(e)$ for $x \in P_S(e)$, and $x^{k_S} \in \bigcup_{f \in E_S} G^S(f)$.
(b) For every $x \in \bigcup_{f \in E_S} G^S(f)$ the element $x^{d(x)} = x^{d_e} = x^{d_S}$ is an idempotent of S.

These numbers enable us to complement the above individual Fermat–Euler Theorem and its classical version to statements over three basic subsemigroup levels of S, namely:

- the least subsemigroup generated by x yielding Fermat–Euler Theorems of individual type,
- the maximal subsemigroup belonging to an idempotent of S yielding local types of this Theorem, and
- the whole multiplicative semigroup of S giving global type Fermat–Euler Theorems.

Namely, it follows from the definitions of numbers k_e, d_e, k_S, d_S and Theorems 1.10, and 1.11 of [LaPo96] that:

Proposition 2 (Local Fermat – Euler theorem)**.** *If $e \in E_S$, and $\kappa, \delta \in \mathbb{N}$ with $\kappa \geq k_e, d_e \mid \delta$, then then for every $x \in P^S(e)$ we have*

$$x^{\kappa+\delta} = x^{\kappa}.$$

Moreover, the numbers k_e, d_e are the least positive integers such that this equality holds under the given conditions for each $x \in P^S(e)$.

Proposition 3 (Global Fermat – Euler theorem)**.** *For every $x \in S$ and $\kappa, \delta \in \mathbb{N}$ with $\kappa \geq k_S, d_S \mid \delta$ we have*

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

and the numbers k_S, d_S are the least positive integers such that this equality holds under the given conditions for each $x \in S$.

1.2. **Finite rings level.** The classical Fermat–Euler Theorem involves both additive and multiplicative structure of the ring of integers, so it seems unavoidable to respect the interference of both, the additive and multiplicative structure of the underlying ring in the process to find the best possible generalization of this Theorem joining its classical form.

Therefore, in this section we shall always suppose that R denotes a *finite* commutative ring with the identity element $1 = 1_R$. The set E_R of idempotents of R is obviously non empty for $0, 1 \in E$ and it is finite. The set E_R can be endowed with a partial ordering

$$x \leq y \quad \Longleftrightarrow \quad xy = x.$$

An idempotent $e \in E_R$ is called *primitive* if it is minimal in the ordered set $(E_R \setminus \{0\}, \leq)$.

Lemma 3. *Let $e_1, \ldots, e_n$ be the all primitive idempotents of R. Then*
(i) *If $0 \neq f \in E$, then*

$$fe_i = \begin{cases} e_i & if \quad e_i \leq f, \\ 0 & otherwise. \end{cases}$$

(ii) *If $0 \neq f \in E$, then*

$$f = \sum_{\substack{i=1 \\ fe_i = e_i}}^{n} e_i.$$

To simplify the notation, given $f \in E_R$, denote

$$\begin{aligned} I_f &= \{i \in \{1,\dots,n\} \; ; \; fe_i = e_i\}, \\ I'_f &= \{1,\dots,n\} \setminus I_f. \end{aligned}$$

Note the following facts (the reader is referred for more details to [LaPo96]) for $e \in E_R$:

- $G^R(e) = P^R(e)e$, thus in particular $G^R(1) = P^R(1)$,
- $G^R(e)$ is the group of units of eR with respect to the ring multiplication and $G^R(e) = P^{eR}(e)$.
- $P^R(0) = N(R)$, where $N(R)$ denotes the the *nil–radical* of the ring R

$$N(R) = \{x \in R \; ; \; x^t = 0 \text{ for some } t > 0\}$$

  which is formed by nilpotent elements of R. Thus nil–radical is the maximal semigroup belonging to the idempotent 0.

If $e_1,\dots,e_n$ are all the primitive idempotents of R, then we have the *Peirce decomposition of* R

$$R = e_1R \oplus \cdots \oplus e_nR,$$

and ([LaPo96, p.263–264])

$$\begin{aligned} P^R(f) &= P^{e_1R}(e_1f) \oplus \cdots \oplus P^{e_nR}(e_nf) = \bigoplus_{i\in I_f} G^R(e_i) \oplus \bigoplus_{i\in I'_f} N(e_iR) \\ &= G^R(f) \oplus N((1-f)R) \\ G^R(f) &= \bigoplus_{i\in I_f} G^R(e_i). \end{aligned} \tag{3}$$

Important observation is given in the next result:

Lemma 4 ([LaPo96, Theorem 1.14])**.** *Let $e_1,\dots,e_n \in E$ be the primitive idempotents of R. Then for every $i = 1,\dots,n$ we have*

$$e_iR = G^R(e_i) \cup N(e_iR) \tag{4}$$

and this union is disjoint.

If we define for $y \in e_iR$

$$\nu_i(y) = \begin{cases} 1 & \text{if } y \in G^R(e_i), \\ t & \text{if } y \in N(e_iR), \text{ where } t \text{ is minimal with } y^t = 0. \end{cases}$$

and

$$\nu(x) = \max\{\nu_i(e_ix) \; ; \; i = 1,\dots,n\},$$

then we have:

Lemma 5 ([LaPo96, Corollary 1 of Theorem 1.15])**.** *For every $x \in R$ we have $k(x) = \nu(x)$.*

Finally, if we define

$$\nu^{(i)} = \max\{\nu(x) \; ; \; x \in e_iR\}, \qquad \mu^{(i)} = \text{l.c.m.}\{d(x) \; ; \; x \in G^R(e_i)\}$$

for every $i = 1,\dots,n$ and

$$\nu_f = \max\{\nu^{(i)} \; ; \; i \in I_{f'}\}, \qquad \mu_f = \text{l.c.m.}\{\mu^{(i)} \; ; \; i \in I_f\}$$

then numbers $\mu_f, f \in E_R$, have the following property ([LaPo96, Lemma 1.8, Corollary 1]):

Lemma 6. *If $f \in E_R$, then $\mu_f | \mu_1$ and the number μ_f is the exponent of the group $G^R(f)$.*

If analogically we define

$$\nu_R = \max\{\nu_f \ ; \ f \in E\} = \nu_0, \qquad \mu_R = \text{l.c.m.}\{\mu_f \ ; \ f \in E\} = \mu_1,$$

then these are the least positive integers such that:

Lemma 7. *(a) x^{ν_R} is an element of a multiplicative subgroup of $(R,.)$ for every $x \in R$,*
(b) x^{μ_R} is an idempotent for every $x \in \bigcup_{f\in E} G^R(f)$.

The previous considerations together give the following generalized Fermat–Euler Theorems (global and local) which are "computationally easier" to handle in comparison with the Proposition 2 and 3, because it reduces the determination of the values of $\nu^{(i)}, \mu^{(i)}$ for $i = 1, \ldots, n$ to the knowledge of the values ν_f, μ_f for every $f \in E_R$. Thus we have:

Proposition 4 (Local Fermat – Euler theorem)**.** *If $e \in E_R$, and $\kappa, \delta \in \mathbb{N}$ with $\kappa \geq \nu_e, \mu_e \mid \delta$, then then for every $x \in P^R(e)$ we have*

$$x^{\kappa+\delta} = x^{\kappa}.$$

The numbers ν_e, μ_e are the least positive integers such that this equality holds under the given conditions for each $x \in P^R(e)$.

Proposition 5 (Global Fermat – Euler theorem)**.** *For every $x \in R$ and $\kappa, \delta \in \mathbb{N}$ with $\kappa \geq \nu_R, \mu_R \mid \delta$ we have*

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

and the numbers ν_R, μ_R are the least positive integers such that this equality holds under the given conditions for each $x \in R$.

1.3. **Dedekind domains level.** Henceforth we shall suppose that R stands for a residually finite Dedekind domain. If $\mathfrak{M}$ is a non–zero ideal of R then the residue class ring $R/\mathfrak{M}$ will be denoted by $R_{\mathfrak{M}}$ and its elements by $[x] = [x]_{\mathfrak{M}} = x + \mathfrak{M}$ for $x \in R$. The norm $\mathcal{N}(\mathfrak{M})$ of an ideal $\mathfrak{M}$ is defined as the cardinality of the residue class ring $R_{\mathfrak{M}}$.

Since every proper ideal $\mathfrak{M}$ of a Dedekind domain R is uniquely (up to the order of the factors) expressible in the form of a product of powers of prime ideals, suppose that

$$\mathfrak{M} = \mathfrak{P}_1^{u_1} \cdots \mathfrak{P}_r^{u_r}, \tag{5}$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are distinct prime ideals of R and $u_i > 0$, $i = 1, \ldots, r$.

For these rings the Fermat–Euler Theorem is usually stated in the form:

Lemma 8 ([Nark74, Theorem 1.8])**.** *Let $G^{R_{\mathfrak{M}}}([1]_{\mathfrak{M}})$ denote the group of units of the residue class ring $R_{\mathfrak{M}}$ with $\mathfrak{M} \neq (0)$ of a residually finite Dedekind domain R. If $\varphi_R(\mathfrak{M}) = \text{card}\left(G^{R_{\mathfrak{M}}}([1]_{\mathfrak{M}})\right)$, then*

$$\varphi_R(\mathfrak{M}) = \mathcal{N}(\mathfrak{M}) \prod_{\mathfrak{P}} \left(1 - \mathcal{N}(\mathfrak{P})^{-1}\right),$$

where the product is extended over all prime ideals appearing in (5), and, moreover, if $x \in R$ and $((x), \mathfrak{M}) = (1)$, then

$$x^{\varphi_R(\mathfrak{M})} \equiv 1 \pmod{\mathfrak{M}}.$$

As usual, we say that an ideal $\mathfrak{A}$ divides an ideal $\mathfrak{B}$, in symbols $\mathfrak{A}|\mathfrak{B}$, if there exists an ideal $\mathfrak{C}$ with $\mathfrak{B} = \mathfrak{A}\mathfrak{C}$. It can be easily shown that in a Dedekind domain $\mathfrak{A}|\mathfrak{B}$ if and only if $\mathfrak{A} \supset \mathfrak{B}$.

Let an ideal $\mathfrak{T}$ divide the ideal $\mathfrak{M}$. Then the ideal $\mathfrak{T}$ is called the *unitary divisor* of $\mathfrak{M}$, if $(\mathfrak{T}, \frac{\mathfrak{M}}{\mathfrak{T}}) = (1)$. Here the *greatest common divisor* $(\mathfrak{A}, \mathfrak{B})$ of two ideals $\mathfrak{A}$

and $\mathfrak{B}$ is defined as the ideal $\mathfrak{A}+\mathfrak{B}=\{a+b\ ;\ a\in\mathfrak{A}, b\in\mathfrak{B}\}$, i.e. the least (with respect to the set inclusion) ideal containing both ideals $\mathfrak{A}$ and $\mathfrak{B}$. Moreover, an ideal $\mathfrak{D}$ is called *unitary divisor generated by the divisor* $\mathfrak{T}$ of $\mathfrak{M}$ provided $\mathfrak{D}$ is a unitary divisor of the ideal $\mathfrak{M}$ and $\mathfrak{D}$ is divisible by exactly the same prime ideals of the ring R as the ideal $\mathfrak{T}$. We shall denote it by $\mathfrak{D}=\langle\mathfrak{T}\rangle$.

If (5) is the factorization of an ideal $\mathfrak{M}$ with distinct prime ideals $\mathfrak{P}_1,\dots,\mathfrak{P}_r$, $u_i>0$, $i=1,\dots,r$, then given a divisor $\mathfrak{T}$ of the ideal $\mathfrak{M}$, define

$$J_{\mathfrak{T}}=\{i\in\{1,\dots,r\}\ ;\ \mathfrak{P}_i|\mathfrak{T}\}.$$

The next result describes the relation between unitary divisors of the ideal $\mathfrak{M}$ and idempotents of the residue class ring $R_{\mathfrak{M}}$.

Lemma 9 ([LaPo96, Theorem 3.2])**.** *There exists a one–to–one correspondence between unitary divisors of the ideal* $\mathfrak{M}$ *and idempotents of the residue class ring* $R_{\mathfrak{M}}$*. More precisely, every idempotent in* $R_{\mathfrak{M}}$ *is a solution of the congruence system*

$$\begin{aligned} x &\equiv 0\ (\mathrm{mod}\,\mathfrak{P}_i^{u_i}) \qquad \textit{for}\quad i\in J_{\mathfrak{D}},\\ x &\equiv 1\ (\mathrm{mod}\,\mathfrak{P}_i^{u_i}) \qquad \textit{for}\quad i\in\{1,\dots,r\}\setminus J_{\mathfrak{D}}, \end{aligned} \tag{6}$$

where $\mathfrak{D}$ *is a unitary divisor of the ideal* $\mathfrak{M}$*.*

If an idempotent $[f]\in R_{\mathfrak{M}}$ is given by the system (6), where the ideal $\mathfrak{D}$ is a unitary divisor of the ideal $\mathfrak{M}$, then we again say that $[f]$ is the *idempotent belonging to the (unitary) divisor* $\mathfrak{D}$.

This implies, for instance, that we have 2^r idempotents in the ring $R_{\mathfrak{M}}$, and that primitive idempotent $[e_i]$, for every $i=1,\dots,r$, is just the idempotent belonging to the unitary divisor

$$\mathfrak{M}_i=\frac{\mathfrak{M}}{\mathfrak{P}_i^{u_i}}=\prod_{\substack{j=1\\ j\neq i}}^{r}\mathfrak{P}_j^{u_j}.$$

This shows that our notation $J_{\mathfrak{T}}$ does not collide with its previous usage. If $[x]\in R_{\mathfrak{M}}$ and $\mathfrak{T}=((x),\mathfrak{M})$, then we say that $[x]$ *belongs to the divisor* $\mathfrak{T}$ of $\mathfrak{M}$.

The next result brings us back to Fermat–Euler Theorem via the explicit determination of $\nu([x])$:

Lemma 10 ([LaPo96, Theorem 4.3])**.** *Let* $[x]\in R_{\mathfrak{M}}$ *belong to a divisor* $\mathfrak{T}=\prod_{j\in J_{\mathfrak{T}}}\mathfrak{P}_j^{v_j}$*, where* $1\le v_j\le u_j$ *for every* $j\in J_{\mathfrak{T}}$*. Then*

$$\nu([x])=\begin{cases} 1 & \textit{if}\ \ \mathfrak{T}=1\quad (J_{\mathfrak{T}}=\emptyset),\\ \max\limits_{j\in J_{\mathfrak{T}}}\left\lceil\dfrac{u_j}{v_j}\right\rceil & \textit{otherwise.}\end{cases} \tag{7}$$

This Theorem in turn implies that

$$\nu^{(i)}=u_i.$$

For later purposes define the function $\mathcal{H}$ on proper non–zero ideals $\mathfrak{M}$ of a Dedekind ring R by

$$\mathcal{H}^R(\mathfrak{M})=\max\{u_i\ ;\ i\in\{1,\dots,r\}\}$$

if (5) is the decomposition of $\mathfrak{M}$ into the product of prime ideals.

If $[f]$ is the idempotent belonging to the divisor $\mathfrak{D}$ of $\mathfrak{M}$, then

$$\nu_{[f]}=\max_{j\in J_{\mathfrak{D}}}u_j=\mathcal{H}^R(\mathfrak{D});$$

in the case $[f]=[0]$ we get

$$\nu_{[0]}=\max_{j\in\{1,\dots,r\}}u_j=\nu_{R_{\mathfrak{M}}}=\mathcal{H}^R(\mathfrak{M}).$$

We also have:

Lemma 11. *Let $[f]$ be the idempotent of the ring $R_{\mathfrak{M}}$ belonging to the unitary divisor $\mathfrak{D}$ of $\mathfrak{M}$. Then*
(i) *The element $[x]^{\mathcal{H}^R(\mathfrak{D})}$ belongs to $G^{R_{\mathfrak{M}}}([f])$ for every $[x] \in P^{R_{\mathfrak{M}}}([f])$.*
(ii) *The element $[x]^{\mathcal{H}^R(\mathfrak{M})}$ belongs to a group for every $[x] \in R_{\mathfrak{M}}$.*
The numbers $\mathcal{H}^R(\mathfrak{D})$ and $\mathcal{H}^R(\mathfrak{M})$ are the least positive integers possessing these properties.

Of fundamental importance is also the following structural result:

Lemma 12. *Let $[f] \in R_{\mathfrak{M}}$ be the idempotent belonging to the unitary divisor $\mathfrak{D}$ of $\mathfrak{M}$. Then the finite commutative rings $R_{\frac{\mathfrak{M}}{\mathfrak{D}}}$ and $[f]_{\mathfrak{M}}R_{\mathfrak{M}}$ with identities $[1]_{\frac{\mathfrak{M}}{\mathfrak{D}}}$ and $[f]_{\mathfrak{M}}$ are isomorphic.*

Corollary 12.1. *Let $[f] \in R_{\mathfrak{M}}$ be the idempotent belonging to the unitary divisor $\mathfrak{D}$ of $\mathfrak{M}$. Then the unit groups $G^{R_{\frac{\mathfrak{M}}{\mathfrak{D}}}}([1]_{\frac{\mathfrak{M}}{\mathfrak{D}}})$ and $G^{[f]_{\mathfrak{M}}R_{\mathfrak{M}}}([f]_{\mathfrak{M}})$ are isomorphic.*

Corollary 12.2. *If $[e_i]$, $i = 1, \ldots, r$ are primitive idempotents of $R_{\mathfrak{M}}$, then*

$$G^{R_{\mathfrak{M}}}([e_i]_{\mathfrak{M}}) \simeq G^{R_{\mathfrak{P}_i^{u_i}}}([1]_{\mathfrak{P}_i^{u_i}}).$$

This shows that for the determination of the values $\mu^{(i)}$, $\mu_{[f]}$, and $\mu_{R_{\mathfrak{M}}} = \mu_{[1]}$ the information about the structure of the groups $G^{R_{\mathfrak{P}^u}}([1]_{\mathfrak{P}^u})$, where $\mathfrak{P}$ is the prime ideal of the ring R and $u > 0$, is necessary. Thus for instance, a classical structural result says:

Lemma 13. *If p is a prime number in $\mathbb{Z}$ and $u > 0$, then*

$$G^{\mathbb{Z}_{p^u}}([1]_{p^u}) \simeq \begin{cases} \mathbb{Z}_1 & \text{if } p = 2, \quad u = 1, \\ \mathbb{Z}_2 & \text{if } p = 2, \quad u = 2, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{u-2}} & \text{if } p = 2, \quad u > 2, \\ \mathbb{Z}_{p^u - p^{u-1}} & \text{if } p > 2. \end{cases}$$

Therefore the exponent of the unit group $G^{\mathbb{Z}_m}([1]_m)$, where $m \in \mathbb{Z}$, $m \neq 0$, is given by the so–called *Carmichael function* λ defined by:
(8)

$$\lambda(m) = \begin{cases} 1 & \text{if } m = 1, \\ 2^{u-2} & \text{if } m = 2^u, \quad u > 2, \\ \varphi(m) & \text{if } m = 2, 4, \text{ or } p^u \text{ for odd prime } p, \\ \text{l.c.m.}\{\lambda(p_i^{u_i})\,;\, i = 1, \ldots, r\} & \text{if } m = p_1^{u_1} \cdots p_r^{u_r}, \end{cases}$$

where φ is the EULER totient function, i.e.:

Lemma 14. *For every $j = 1, \ldots, r$*

$$\mu^{(j)} = \lambda(p_j^{u_j}) = \begin{cases} 1 & \text{if } p_j = 2, \quad u_j = 1, \\ 2 & \text{if } p_j = 2, \quad u_j = 2, \\ 2^{u_j - 2} & \text{if } p_j = 2, \quad u_j > 2, \\ p_j^{u_j} - p_j^{u_j - 1} & \text{if } p_j > 2. \end{cases}$$

This yields the following (by the way the best possible) extensions of FERMAT–EULER Theorem for $\mathbb{Z}$ which are proved in [Schw81], where

$$H(m) = \mathcal{H}^{\mathbb{Z}}((m)).$$

Proposition 6 (Global Fermat–Euler Theorem)**.** *Let $a, m \in \mathbb{Z}$, $m \neq 0$. If $\kappa, \delta \in \mathbb{N}$ with $\kappa \geq H(m), \lambda(m) \mid \delta$, then*

$$a^{\kappa+\delta} \equiv a^{\kappa} \pmod{m},$$

where $H(n) = \max\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ for n having the standard form $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. The exponents $\lambda(m), H(m)$ are the least positive integers for which the congruence is true for every a.

If again, given a divisor d of m, $\langle d\rangle$ denotes the unitary divisor of m having the same set of prime divisors as d, and, a *unitary divisor of* m is such a divisor t of m for which $(m, m/t) = 1$, then

Proposition 7 (Local Fermat–Euler Theorem)**.** *Let $a, m \in \mathbb{Z}$, $m \neq 0$ and $d = \langle (a, m)\rangle$. If $\kappa, \delta \in \mathbb{N}$ with $\kappa \geq H(d), \lambda(\frac{m}{d}) \mid \delta$, then*

$$a^{\kappa+\delta} \equiv a^{\kappa} \pmod{m},$$

The exponents $\lambda(m/d), H(d)$ are the least possible positive integers over the set $P(d) = \{n \in \mathbb{Z} \,:\, \langle (n, m)\rangle = d\}$.

Various other forms of Fermat–Euler Theorem found in the literature can be derived from the just given one using that the Lagrange's Theorem of group theory which in case of $\mathbb{Z}_m$ says

$$\forall_{m\in\mathbb{N}} \quad \lambda(m) \mid \varphi(m). \tag{9}$$

This follows directly also from (8). For concretization of Propositions 2 and 5 for other rings the values of μ_e and μ_R are needed. In [LaPo96] the corresponding values for Gaussian integers, and other quadratic extensions of $\mathbb{Z}$ and general number fields can be found.

2. Smarandache's algorithm

Given two integers a, m with $m \neq 0$, F.Smarandache [Smar81] proved that the following algorithm terminates

Let	$d_0 = (a, m)$,	$a = a_0 d_0$, $m = m_0 d_0$,	$(a_0, m_0) = 1$.
If $d_0 > 1$ then			
	$d_1 = (d_0, m_0)$,	$d_0 = d_0^1 d_1$, $m_0 = m_1 d_1$,	$(d_0^1, m_1) = 1$.
If $d_1 > 1$ then			
	$d_2 = (d_1, m_1)$,	$d_1 = d_1^1 d_2$, $m_1 = m_2 d_2$,	$(d_1^1, m_2) = 1$.
If $d_2 > 1$ then			
	$d_3 = (d_2, m_2)$,	$d_2 = d_2^1 d_3$, $m_2 = m_3 d_3$,	$(d_2^1, m_3) = 1$.
etc. until $d_{s-1} > 1$ and			
	$d_s = (d_{s-1}, m_{s-1})$,	$d_{s-1} = d_{s-1}^1 d_s$, $m_{s-1} = m_s d_s$,	$(d_{s-1}^1, m_s) = 1$,

where $d_s = 1$.

This algorithm provided him the basis for the following generalization of the Fermat–Euler Theorem:

Proposition 8 (Smarandache, [Smar81, Thorème])**.** *If $a, m \in \mathbb{Z}$, $m \neq 0$, then*

$$a^{\varphi(m_s)+s} \equiv a^{s} \pmod{m}, \tag{10}$$

where m_s and s are defined through the above algorithm and φ is the Euler*'s totient function.*

It follows from the above algorithm that

$$d_s \mid d_{s-1} \mid \cdots \mid d_0, \quad d_0 = (a, m),$$
$$m_s \mid m_{s-1} \mid \cdots \mid m_0 \mid m,$$
$$(d_i^1, m_s) = 1 \qquad \text{for} \quad i = 0, 1, 2, \ldots, s-1,$$
$$(a, m_s) = 1, \tag{11}$$
$$m = \left(d_0^1\right)^1 \left(d_1^1\right)^2 \ldots \left(d_{s-1}^1\right)^s . m_s, \tag{12}$$
$$a = a_0 d_0^1 d_1^1 \ldots d_{s-1}^1 d_s.$$

Relation (11) is employed as the starting point of the SMARANDACHE's proof of the above Proposition 8 through the EULER Theorem

$$a^{\varphi(m_s)} \equiv 1 \pmod{m_s}. \tag{13}$$

However, as we noted in the previous Section of this paper, $\varphi(m_s)$ is not the best exponent for which (13) is true for for every a coprime to m_s. The best exponent is given by CARMICHAEL's function $\lambda(m_s)$ as relations (7) and (9) show. Therefore an immediate check of the SMARANDACHE's proof implies that SMARANDACHE's result of Proposition 8 can be improved to the form:

Theorem 1. *If $a, m \in \mathbb{Z}$, $m \neq 0$, then*

$$a^{\lambda(m_s)+s} \equiv a^s \pmod{m}, \tag{14}$$

where m_s, and a are defined through as above and λ is the Carmichael's function.

3. Generalized Smarandache's algorithm

In this Section give another proof of a generalization of Proposition 8 based on the results quoted in Section 1.

R will again denote a residually finite DEDEKIND domain. Here the SMARANDACHE's algorithm acquires the following form:

Given two ideals $\mathfrak{A}, \mathfrak{M}$ with $\mathfrak{M} \neq (0)$, let

Let $\mathfrak{D}_0 = (\mathfrak{A}, \mathfrak{M})$, $\mathfrak{A} = \mathfrak{A}_0 \mathfrak{D}_0$, $\mathfrak{M} = \mathfrak{M}_0 \mathfrak{D}_0$, $(\mathfrak{A}_0, \mathfrak{M}_0) = R$.

If $\mathfrak{D}_0 \neq R$ then
$\mathfrak{D}_1 = (\mathfrak{D}_0, \mathfrak{M}_0)$, $\mathfrak{D}_0 = \mathfrak{D}_0^1 \mathfrak{D}_1$, $\mathfrak{M}_0 = \mathfrak{M}_1 \mathfrak{D}_1$, $(\mathfrak{D}_0^1, \mathfrak{M}_1) = R$.

If $\mathfrak{D}_1 \neq R$ then
$\mathfrak{D}_2 = (\mathfrak{D}_1, \mathfrak{M}_1)$, $\mathfrak{D}_1 = \mathfrak{D}_1^1 \mathfrak{D}_2$, $\mathfrak{M}_1 = \mathfrak{M}_2 \mathfrak{D}_2$, $(\mathfrak{D}_1^1, \mathfrak{M}_2) = R$.

$\vdots$

If $\mathfrak{D}_{s-1} \neq R$ then
$\mathfrak{D}_s = (\mathfrak{D}_{s-1}, \mathfrak{M}_{s-1})$, $\mathfrak{D}_{s-1} = \mathfrak{D}_{s-1}^1 \mathfrak{D}_s$, $\mathfrak{M}_{s-1} = \mathfrak{M}_s \mathfrak{D}_s$, $(\mathfrak{D}_{s-1}^1, \mathfrak{M}_s) = R$,

etc.

Though we give a more explicit proof of the above SMARANDACHE's result in this more general setting, the original SMARANDACHE's ideas can also be employed here if the well ordering principle of the set of positive integers used by SMARANDACHE over the set

$$1 = d_s \leq d_{s-1} \leq \cdots \leq d_0, \quad d_0 = (a, m),$$

is replaced in R through the norm function $\mathcal{N}$ over the set

$$1 = \mathcal{N}(\mathfrak{D}_s) \leq \mathcal{N}(\mathfrak{D}_{s-1}) \leq \cdots \leq \mathcal{N}(\mathfrak{D}_0), \quad \mathfrak{D}_0 = (\mathfrak{A}, \mathfrak{M}),$$

by means of the following elementary results:

Lemma 15 ([Gilm72, Exercise 8,p.467])**.** *If R is a Dedekind domain and $\mathfrak{A},\mathfrak{B}$ are two non–zero ideals with finite norm $\mathcal{N}(\mathfrak{A}),\mathcal{N}(\mathfrak{B})$, then $\mathfrak{AB}$ also has finite norm and*

$$\mathcal{N}(\mathfrak{AB}) = \mathcal{N}(\mathfrak{A}).\mathcal{N}(\mathfrak{B}). \tag{15}$$

Note that there follows from the subsequent Exercise 9, [Gilm72] that the truth of (15) for every couple of non–zero ideals in a residually finite domain R forces that R is DEDEKIND.

Lemma 16. *Let R be a residually finite Dedekind domain. If $\mathfrak{A},\mathfrak{B}$ are two ideals of R with $\mathfrak{A} \subsetneqq \mathfrak{B}$, then $\mathcal{N}(\mathfrak{A}) \gneqq \mathcal{N}(\mathfrak{B})$.*

Proof. As already mentioned if R is DEDEKIND then $\mathfrak{A} \subset \mathfrak{B}$ holds if and only if there exists an ideal $\mathfrak{C}$ such that $\mathfrak{A} = \mathfrak{BC}$. If $\mathcal{N}(\mathfrak{A}) = \mathcal{N}(\mathfrak{B})$, then $\mathcal{N}(\mathfrak{C}) = 1$, i.e. $\mathfrak{C} = R$. Consequently, $\mathfrak{A} = \mathfrak{BC} = \mathfrak{B}$, which is impossible due to $\mathfrak{A} \subsetneqq \mathfrak{B}$. □

That the SMARANDACHE's algorithm also terminates in this more general setting follows from the next result:

Theorem 2. *Let $\mathfrak{M} = \mathfrak{P}_1^{\alpha_1}\mathfrak{P}_2^{\alpha_2}\dots\mathfrak{P}_k^{\alpha_k}$ and $\mathfrak{A} = \mathfrak{P}_1^{\beta_1}\mathfrak{P}_2^{\beta_2}\dots\mathfrak{P}_k^{\beta_k}$ be decompositions of ideals $\mathfrak{M}$ and $\mathfrak{A}$ into the product of distinct prime ideals of R with $0 \le \alpha_i$ and $0 \le \beta_i$ for $i = 1,2,\dots,k$. Then the generalized Smarandache's algorithm terminates for s given by*

$$s = \max\left\{0, \left\lceil \frac{\alpha_i}{\beta_i} \right\rceil \ : \ \text{for } i = 1,2,\dots,k \text{ with } \beta_i \neq 0\right\}.$$

Proof. We shall discuss the contribution of every prime ideal $\mathfrak{P}$ separately. Let $\mathfrak{P}^\alpha \| \mathfrak{M}$ and $\mathfrak{P}^\beta \| \mathfrak{A}$. If $\beta \neq 0$, put

$$\alpha = K\beta + q, \qquad 0 < q \le \beta,$$

and $K = 0$ if $\beta = 0$.

If $\mathfrak{D}_0 = (\mathfrak{A},\mathfrak{M})$ and $\mathfrak{P}^{\gamma_0} \| \mathfrak{D}_0$, then $\gamma_0 = \min\{\alpha,\beta\}$. Consequently, if $\mathfrak{M} = \mathfrak{M}_0\mathfrak{D}_0$, then $\mathfrak{P}^{\mu_0} \| \mathfrak{M}_0$, where $\mu_0 = \alpha - \gamma_0$. Thus if $\alpha \le \beta$ or $\beta = 0$, i.e. if $K = 0$, then $\mathfrak{P}^0 \| \mathfrak{M}_0$, and $\mathfrak{P}$ does not contribute more to the whole process.

If $K \ge 1$, then $\gamma_0 = \beta$ and $\mu_0 = \alpha - \beta > 0$, i.e. $\mathfrak{P}^{\alpha-\beta} \neq R$, and we can continue in the SMARANDACHE's algorithm. If $\mathfrak{D}_1 = (\mathfrak{D}_0,\mathfrak{M}_0)$ and $\mathfrak{P}^{\gamma_1} \| \mathfrak{D}_1$, then $\gamma_1 = \min\{\gamma_0,\mu_0\}$. Since $\mathfrak{M}_0 = \mathfrak{M}_1\mathfrak{D}_1$, $\mathfrak{P}^{\mu_1} \| \mathfrak{M}_1$ with $\mu_1 = \mu_0 - \gamma_1$. Consequently, $\mu_1 = 0$ if $\beta < \alpha \le 2\beta$, i.e. if $K = 1$, or $\mu_1 = \alpha - 2\beta$ provided $K > 1$. Thus if $K = 1$, then $\mathfrak{P}^0 \| \mathfrak{M}_1$, and the contribution of $\mathfrak{P}$ terminates. If $K > 1$ then $\mu_1 = \alpha - 2\beta$ and $\gamma_1 = \beta$, etc.

In the last but one step, $\mu_{K-1} = \alpha - K\beta$ and $\mathfrak{P}^{\gamma_{K-1}} \| \mathfrak{D}_{K-1}$ with $\gamma_{K-1} = \min\{\gamma_{K-2},\mu_{K-2}\} = \beta$. Then $\mathfrak{P}^{\gamma_K} \| \mathfrak{D}_K$ implies $\gamma_K = \min\{\gamma_{K-1},\mu_{K-1}\} = \alpha - K\beta$ and $\mathfrak{M}_{K-1} = \mathfrak{M}_K\mathfrak{D}_K$ yields $\mu_K = \mu_{K-1} - \gamma_{K-1} = 0$, i.e. $\mathfrak{P} \nmid \mathfrak{M}_K$.

This shows that the SMARANDACHE's algorithm really stops after

$$\max\left\{0, \left\lceil \frac{\alpha_i}{\beta_i} \right\rceil \ : \ i = 1,2,\dots,k \text{ with } \beta_i \neq 0\right\}$$

steps, and the proof is finished. □

Lemma 10 immediately then proves:

Corollary 2.1. *If $[x] \in R_{\mathfrak{M}}$ belongs to the divisor $\mathfrak{T} = \prod_{j\in J_{\mathfrak{T}}} \mathfrak{P}_j^{\beta_j}$, where $1 \le \beta_j \le \alpha_j$ for every $j \in J_{\mathfrak{T}}$ then*

$$\nu([x]) = \begin{cases} 1, & \text{if } \mathfrak{T} = 1 \quad (\text{i.e. if } J_{\mathfrak{T}} = \emptyset), \\ s, & \text{otherwise.} \end{cases}$$

It follows from the last Corollary that SMARANDACHE's number s is a more suitable tool for extension of the $(p-1)$–power version of FERMAT Theorem, while $\nu([x])$ does this for its p–power version.

Moreover we have:

Theorem 3. *If* $\mathfrak{D}_0 = (\mathfrak{A}, \mathfrak{M})$ *and* $\mathfrak{D} = \langle \mathfrak{D}_0 \rangle$, *then*

$$\mathfrak{M}_s = \frac{\mathfrak{M}}{\mathfrak{D}}.$$

Proof. Let $\mathfrak{P}^\alpha \| \mathfrak{M}$ but $\mathfrak{P} \nmid \mathfrak{D}$. Then $\mathfrak{P}^\alpha \| \mathfrak{M}_s$ and $\mathfrak{P} \nmid \mathfrak{D}_0$. Consequently,

$$\mathfrak{P}^\alpha \| \mathfrak{M}_i, \quad i = 0, 1, \ldots, s,$$

i.e. $\mathfrak{P}^\alpha \| \mathfrak{M}_s$.

Let $\mathfrak{P} | \mathfrak{M}$ and also $\mathfrak{P} | \mathfrak{D}$. We claim that $\mathfrak{P} \nmid \mathfrak{M}_s$. In the opposite case

$$\mathfrak{P} \mid \mathfrak{M}_s \mid \mathfrak{M}_{s-1} \mid \cdots \mid \mathfrak{M}_0 \mid \mathfrak{M},$$

and simultaneously $\mathfrak{P} | \mathfrak{D}_0$. Therefore $\mathfrak{P} | \mathfrak{D}_1 = (\mathfrak{D}_0, \mathfrak{M}_0)$, and thus $\mathfrak{P} | \mathfrak{D}_2 = (\mathfrak{D}_1, \mathfrak{M}_1)$, etc. , $\mathfrak{P} | \mathfrak{D}_s = (\mathfrak{D}_{s-1}, \mathfrak{M}_{s-1})$. A contradiction, since $\mathfrak{D}_s = 1$. □

This together with Lemma 8 gives the following extension of SMARANDACHE's contribution to the individual type FERMAT–EULER Theorem to residually finite DEDEKIND domains:

Theorem 4. *Let* R *be a residually finite Dedekind domain and* $\mathfrak{M}$ *its non–zero ideal. Then given an element* $a \in R$, *let* $s, \mathfrak{M}_s$ *be determined by the above Smarandache's algorithm for* $\mathfrak{A} = (a)$, *and* $\mathfrak{M}$. *Then*

$$a^{\varphi_R(\mathfrak{M}_s)+s} \equiv a^s \pmod{\mathfrak{M}}. \tag{16}$$

It follows from the above discussion that the exponent $\varphi_R(\mathfrak{M}_s)$ is not the best possible. The best one is given by the order of the cyclic group $C(a)$ in $R_{\mathfrak{M}}$. The "next" best exponent is given by the exponent of the maximal subgroup of the multiplicative semigroup of $R_{\mathfrak{M}}$ belonging to the idempotent belonging to the unitary divisor $\mathfrak{D} = \langle ((a), \mathfrak{M}) \rangle$. In the case when $R = \mathbb{Z}$ this is given through the CARMICHAEL function. The reader is again referred to [LaPo96] for how the corresponding values can be computed in the case of algebraic number fields. The necessary facts can also be found in [Naka79]. For other residually finite commutative rings the corresponding numbers can be computed using (3) and Lemma 12 and its Corollaries 12.1, 12.2.

4. APPLICATIONS

As noticed by SMARANDACHE in [Smar81] his algorithm can be easily implemented. Namely:

`Step 1:` $A := a, M := m, i := 0$
`Step 2: COMPUTE` $d = (a, m)$ `AND` $M' = M/d$
`Step 3: IF` $d = 1$ `THEN` $s = i$ `and` $m_s = M'$`; STOP`
`Step 4: IF` $d \neq 1$ `THEN` $A := d, M := M', i := i + 1$`; GOTO 2`

In conjunction with the above given form of individual FERMAT–EULER Theorem the SMARANDACHE's algorithm can be used for a effective determinations of:

- The highest power in which a prime from a given set $\{p_1, p_2, \ldots, p_k\}$ of primes divides a given integer n. Simply apply the above algorithm with $a = p_1 \ldots p_k$ and $m = n$.
- the least power k for which a given number x belongs to a subgroup of the multiplicative semigroup of $\mathbb{Z}_n$, the residues modulo n. Again apply the the algorithm with $a = x$, and $m = n$.

Adaptation of the above ideas to other residually finite rings along above lines is left to the reader.

5. Acknowledgement

The author would like to express his thanks to Professor M.R.Popov from Tempe, AZ, for calling his attention to F.Smarandache's paper [Smar81].

References

[Gilm72] Gilmer,R.: *Multiplicative Ideal Theory*, M.Dekker, Inc., 1972

[Naka79] Nakagoshi,N.: *The structure of the multiplicative group of residue classes modulo* $\mathfrak{P}^{N+1}$, Nagoya Math. J. **73**, 1979, 41 – 60

[Nark74] Narkiewicz,W.: *Elementary and Analytic Theory of Algebraic Numbers,* PWN, Warsaw 1974

[LaPo96] Laššák,M., Porubský,Š.: *Fermat–Euler theorem in algebraic number fields*, J. Number Theory **60**, No.2 (1996), 254–290

[Schw81] Schwarz,Š.: *The role of semigroups in the elementary theory of numbers*, Math. Slovaca **31** (1981), 369–395

[Smar81] Smarandache,F.: *Une generalisation du theoreme d'Euler*, Bul. Univ. Brasov, Ser. C **23** (1981), 7–12 (Collected Papers, Vol.I, Editura Societătii Tempus, Bucurest 1996, pp.184–191); MR 84j:10006

Department of Mathematics, Institute of Chemical Technology, Technická 5, 166 28 Prague 6, Czech Republic

E-mail address: porubsks@@vscht.cz