DOI: 10.2478/auom-2018-0003
An. Şt. Univ. Ovidius Constanţa

Vol. 26(1),2018, 69–80

Tripotents: a class of strongly clean elements in rings

Grigore Călugăreanu

Abstract

Periodic elements in a ring generate special classes of strongly clean elements. In particular, elements b such that $b = b^3$, which are called *tripotents* and include idempotents, negative of idempotents and order 2 units, are strongly clean. Such elements are determined in 2×2 matrix rings over commutative domains or over arbitrary division rings and for rings of integers modulo n.

1 Introduction

An element t was called *nilpotent* in a ring R if $t^n = 0$ for a positive integer n. Among nilpotent elements, the particular case $n = 2$ (i.e. *zerosquare* elements) play a special rôle. Idempotents are also related to $n = 2$ so a natural idea is to consider elements $b \in R$ with $b = b^n$ for a positive integer $n \geq 3$. But these can be included in a larger subset of the ring: the *periodic elements*, introduced by H. Bell and studied merely for semigroups by several authors.

An element a in a unital ring R was called *clean* if there is an idempotent e and a unit u such that $a = e + u$, and *strongly clean* if $eu = ue$.

We show that periodic elements generate strongly clean elements and in particular, elements $b \in R$ with $b = b^n$ for a positive integer n are strongly clean when n is odd. The simplest special case are the elements called *tripotents*, that is $b = b^3$.

Key Words: periodic element, tripotent, strongly clean element, order two unit
2010 Mathematics Subject Classification: Primary 16U99,16U60 Secondary 11Z05,11N69
Received: 13.05.2017
Revised: 20.06.2017
Accepted:22.06.2017

It is readily seen that idempotents and negatives of idempotents are tripotents and among units only the order 2 units (also called *square roots of* 1) are tripotents. Thus, we call a tripotent *genuine* if it is not an idempotent or a negative of idempotent or an order 2 unit.

We show that 2×2 matrix rings over commutative (integral) domains or over arbitrary division rings do not possess genuine tripotents.

Idempotents, nilpotents and units are well-known in any ring $\mathbf{Z}_n$ for any positive integer $n \geq 2$. We completely determine the order 2 units and the genuine tripotents for these rings.

We denote by $\mathrm{Per}(R)$ the set of all the periodic elements, $\mathrm{Id}(R)$ the idempotents and $U(R)$ the units of a unital ring R. Clearly, $\mathrm{Id}(R) \subset \mathrm{Per}(R)$, $\mathrm{Per}(R) \cap N(R) = 0$ and $\mathrm{Per}(R) \cap U(R) = \{u \in U(R) | u^m = 1\}$.

In mostly all cases we use the simple notation $\overline{a}$ for an integer modulo n. However when necessary, we also use the notation $[a]_n$.

2 General results

Recall that an element a in a ring R was called *periodic* if $a^k = a^{k+m}$ for some positive integers k, m. Obviously tripotents are periodic.

The following result will be important.

Proposition 1. *Suppose a is a periodic element in a ring and $a^k = a^{k+m}$. If m is even then a^k is strongly clean and if m is odd, $-a^k$ is strongly clean.*

Proof. It is well-known (see [1]) that for every periodic element there is a power which is an idempotent. Since we need the details in our proof, suppose $k = qm + r$ is the division with quotient q and reminder $0 \leq r < m$ (with possible $q = 0$ if $m \geq k$). Observe that $a^k = a^{k+m} = a^{k+2m} = ... = a^{k+(q+1)m}$ and $(q+1)m > k$. We just have to multiply $a^k = a^{k+(q+1)m}$ with $a^{(q+1)m-k}$ and obtain the idempotent $a^{(q+1)m}$. In particular, if $m \geq k$ (and so $q = 0$), a^m is the required idempotent.

Together with $a^{(q+1)m}$, $1 - a^{(q+1)m}$ is also (the complementary) idempotent and it is orthogonal to a^k (because $a^k = a^{k+(q+1)m}$).

Next we show that $a^{(q+1)m} = a^{km}$ if $r \neq 0$. We first rewrite $a^k = a^{k+m}$ as $a^{qm+r} = a^{(q+1)m+r}$ and multiply this with a^{m-r}. Then $a^{(q+1)m} = a^{(q+2)m} = ...$, so our claim reduces to $k = qm + r \geq q + 1$ since both $m, r \geq 1$.

If $r = 0$, that is, m divides k then $a^k = a^{qm} = a^{(q+1)m}$ is already idempotent.

Finally, consider $[(1 - a^{(q+1)m}) - a^k]^m$. Since the two terms are orthogonal and the left one (the parenthesis) is idempotent, this gives $(1 - a^{(q+1)m}) + a^{km}$ if m is even and by the claim above, $= 1$. Thus $(1 - a^{(q+1)m}) - a^k$ is a unit

and so a^k is strongly clean. If m is odd we consider $[(1-a^{(q+1)m})+a^k]^m$ and similarly we obtain the conclusion $-a^k$ is strongly clean. □

Remark. As seen above, for a periodic element a with $a^k = a^{k+m}$, $a^{(q+1)m}$ is an idempotent. However, if $r = 0$ (recall that $k = qm + r$), this is not the smallest power of a which is idempotent: a^k is also idempotent.

An important special case, which will be studied in the sequel are the periodic elements $b \in R$ with $k = 1$. An element $b = b^n$ is called *n-idempotent* (also called *potent* element in [2]). More specific, for $n = 3$, such an element is called a *tripotent*. We denote by $n\mathrm{Id}(R)$ and $3\mathrm{Id}(R)$ the corresponding sets of elements. Idempotents (i.e. 2-idempotents) are clearly also n-idempotents for any $n \geq 3$. Notice that if b is a tripotent, so is the negative $-b$ and that $3\mathrm{Id}(R) \cap U(R) = \{u \in U(R) | u^2 = 1\} := U_2(R)$, that is, 1 and order 2 units (also called the *2-torsion subgoup* of $U(R)$). A tripotent will be called *genuine* if it is not idempotent (so $\neq 0, 1$), not the negative of an idempotent nor an order 2 unit.

If e is a nontrivial idempotent then the negative $-e$ is a tripotent which is not idempotent nor order 2 unit. However, the converse fails: $\overline{4}$ is a genuine tripotent in $\mathbf{Z}_{30}$ which is not the negative of an idempotent.

Since nontrivial n-idempotents are zero divisors, integral domains and division rings have only trivial n-idempotents.

In particular for tripotents, since $b = b^3$ is equivalent to $(b-1)b(b+1) = 0$, in any integral domain the only tripotents are $\{-1, 0, 1\}$.

By Proposition 1, *for odd n, n-idempotents are strongly clean* and *for even n, negative of n-idempotents are strongly clean.* This distinction is natural since the negative of a nonzero idempotent is not idempotent. In particular, *tripotents are strongly clean.*

From the proof of Proposition 1, we record:

Corollary 2. *If $b \in R$ is a tripotent then*

(i) b^2 and $1-b^2$ are both idempotents; the converse fails ($\overline{2}$ is not tripotent in $\mathbf{Z}_{12}$);

(ii) b and $1-b^2$ are orthogonal;

(iii) $1-b-b^2$ is an order 2 unit;

(iv) If b is not idempotent then $1+b-b^2$ is an order 2 unit.

(v) If $b \in R$ is a tripotent then $Rb \oplus R(1-b^2) = R$ is the Pierce decomposition into left (principal) ideals. A symmetric decomposition into right ideals also holds.

(vi) $\mathrm{Id}(R) = 3\mathrm{Id}(R)$ *holds for a ring R iff $U_2(R) = \{1\}$.*

For commutative rings recall (**129.1** [6]) that *for every group G, there is a (commutative unital) ring whose unit group is isomorphic to $\mathbf{Z}_2 \times G$.* This shows that rings with tripotents which are not idempotents abound. However unit groups without order 2 elements are in this sense exceptional. Indeed (see **129.4** [6]): *the unit group $U(R)$ of a (commutative unital) ring has trivial 2-component iff R is a subdirect sum of domains of characteristic 2.*

Example. In $\mathcal{M}_2(\mathbf{Z})$, the matrices $\begin{bmatrix} 2 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n \\ 0 & 0 \end{bmatrix} + I_2$ are strongly clean but not tripotent. However, if $\mathrm{char}(R) = 3$ then *any strongly clean element whose unit has order 2, is a tripotent.*

Indeed, $(e+u)^3 = e^3 + u^3 + 3eu + 3e = e + u$.

Remarks. If all tripotents are central in a ring R then the ring is Abelian and order 2 unit-central, but this is not necessarily. The free ring $\mathbf{Z}\langle x, y\rangle$ is an example of noncommutative unit-central ring with only trivial idempotents (so Abelian).

Notice that *if $2 \in U(R)$ then tripotent-central is equivalent to Abelian* (idempotent-central). This follows from a simple representation of tripotent as difference of two idempotents (see [3]), namely: if $b = b^3$ then $b = 2^{-1}(b^2 + b) - 2^{-1}(b^2 - b)$.

If all elements are tripotents (rings which satisfy the identity $x^3 = x$ were investigated by Hirano and Tominaga - see [7]), the ring may not be Boolean (e.g. $\mathbf{F}_3$).

It is easy to see that 0 *is the only tripotent in the Jacobson radical,* 1 *and order 2 units are the only (nonzero) tripotents in any local ring and, in any ring with only trivial idempotents, the only nontrivial tripotents (i.e. $\neq 0, 1$) are order 2 units.*

There is a large bibliography on strongly clean matrices the last 10 years (see [5] for a comprehensive survey).

Even for integral 2×2 matrices, a complete characterization for strongly clean elements is not available yet (but see [4], for extensive results).

It is far more easy to determine the 2×2 tripotents even over any commutative domain.

Proposition 3. *Let D be a commutative (integral) domain. The matrix ring $\mathcal{M}_2(D)$ has no genuine tripotents.*

Proof. Since $B^3 = B$ implies $\det B(1 - \det^2 B) = 0$, tripotents have $\det B \in \{0, \pm 1\}$.

If $\det B = \pm 1$, B is a unit, so it must be an order 2 unit.

If $\det B = 0$, Cayley-Hamilton gives $B^2 - \mathrm{Tr}(B)B = 0_2$. Since also $B = B^3 = \mathrm{Tr}(B)B^2 = \mathrm{Tr}^2(B)B$, we get $B = 0_2$ or $\mathrm{Tr}^2(B) = 1$. Hence $B^2 = B$, that is B is idempotent or $B^2 = -B$ which are negatives of idempotents. □

Remarks. 1) By computation, the tripotent 2×2 matrices over a commutative domain are:

I_2, $-I_2$; $\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$ with $a^2 + bc = 1$ and 0_2, $\begin{bmatrix} a+1 & b \\ c & -a \end{bmatrix}$ with $a^2 + a + bc = 0$, and $\begin{bmatrix} a-1 & b \\ c & -a \end{bmatrix}$ with $a^2 - a + bc = 0$.

2) The result fails if the domain hypothesis is dropped: in $\mathcal{M}_2(\mathbf{Z}_{24})$, $\overline{3}I_2$ is a genuine tripotent. Actually, if b is any genuine tripotent in a ring R, bI_n is a genuine tripotent in $\mathcal{M}_n(R)$.

If the commutativity hypothesis is dropped but D is a division ring, we can prove the following

Proposition 4. *Let D be any division ring. The matrix ring $\mathcal{M}_2(D)$ has no genuine tripotents.*

Proof. Since 0_2 is an idempotent, we start with $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0_2$, matrix with at least one nonzero entry.

We first show that we can always suppose that the (1,1)-entry $a \neq 0$.

First observe that *if X and Y are similar matrices and X is a tripotent then so is Y* (indeed, $X^3 = X \Longleftrightarrow (UXU^{-1})^3 = UXU^{-1}$). Now, if $d \neq 0$, for $U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = U^{-1}$ we obtain $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & c \\ b & a \end{bmatrix}$, which has nonzero (1,1)-entry. Therefore, if $b \neq 0$ we may suppose $a = d = 0$. Now for $V = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ we get $V\begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix}V^{-1} = \begin{bmatrix} -b & b \\ c-b & b \end{bmatrix}$ which has nonzero (1,1)-entry. The $c \neq 0$ is similar because *a matrix is a tripotent iff its transpose is a tripotent.*

Next, for the above matrix A, suppose $a \neq 0$. If $U = \begin{bmatrix} 1 & 0 \\ -ca^{-1} & 1 \end{bmatrix}$ then $UA = B = \begin{bmatrix} a & b \\ 0 & d - ca^{-1}b \end{bmatrix}$.

(i) If $d - ca^{-1}b \neq 0$ then B is invertible, and so is A (because U is invertible). Hence it is an order 2 unit.

(ii) If $d - ca^{-1}b = 0$ then $B = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$. Since $A = U^{-1}B$, if A is a tripotent, $(U^{-1}B)^3 = U^{-1}B$ and so $(BU^{-1})^3 = BU^{-1}$, that is $BU^{-1} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ ca^{-1} & 1 \end{bmatrix} = \begin{bmatrix} a + bca^{-1} & b \\ 0 & 0 \end{bmatrix}$ is tripotent.

Further, notice that $\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}^3 = \begin{bmatrix} x^3 & x^2y \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}$ is equivalent to $x^3 = x$ and $x^2y = y$, and if the matrix is not zero then $x \neq 0$ (indeed, $x = 0$ implies $y = 0$). Thus $x^2 = 1$ and so $x \in \{\pm 1\}$, with arbitrary y.

Since $BU^{-1} \neq 0_2$ (otherwise $B = 0_2$ and $A = 0_2$) is a tripotent, $BU^{-1} = \begin{bmatrix} \pm 1 & b \\ 0 & 0 \end{bmatrix}$ is idempotent if the (1,1)-entry is $+1$ or is a negative of idempotent if the (1,1)-entry is -1. Then so is $U^{-1}B = A$, and the proof is complete. □

Remark. The property fails for $n \times n$ matrices with $n \geq 3$. Indeed, for any unital ring R, in $\mathcal{M}_3(R)$ the matrix $B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is a genuine tripotent and the example can be obviously generalized for any $n \geq 3$. Actually, the left-upper 2×2 corner may be replaced by any order 2 unit.

Finally a useful observation.

Proposition 5. *Let $R = R_1 \times ... \times R_k$ be a finite direct product of rings and $a = (a_1, ..., a_k) \in R$. The element a is a tripotent, or idempotent, or order 2 unit, or negative of idempotent iff so are all a_i, $1 \leq i \leq k$, respectively.*

Just to simplify the wording in the sequel, let us say that elements in a (finite) subset of a ring are *of the same sort* if either all are idempotents, or else all are order 2 units, or all are negative of idempotents ("different sort", for denial). Hence

Corollary 6. *With above notations, a is a genuine tripotent iff $\{a_1, ..., a_k\}$ are of different sort.*

3 The tripotents of $\mathbf{Z}_n$

Since local rings are strongly clean and so are direct products, in every $\mathbf{Z}_n$, all elements (including tripotents) are (strongly) clean.

In order to determine all the tripotents, we first single out the order 2 units.

The order 2 units.

It is well-known that $\overline{u} \in U(\mathbf{Z}_n)$ iff $(u; n) = 1$ and consequently there are $\varphi(n)$ - the Euler's (totient) function - units in $\mathbf{Z}_n$.

More precisely, if $n = p_1^{r_1}...p_k^{r_k}$ then $|U(\mathbf{Z}_n)| = \varphi(n) = n(1 - \frac{1}{p_1})...(1 - \frac{1}{p_k}) = p_1^{r_1 - 1}(p_1 - 1)...p_k^{r_k - 1}(p_k - 1)$, that is, $U(\mathbf{Z}_n)$ is a (finite Abelian) group

of order $\varphi(\dot{n})$. Moreover, $U(\mathbf{Z}_n)$ is cyclic iff $n = 2, 4$, any power of an odd prime or twice any power of an odd prime, is referable to Gauss.

Obviously $-\overline{1} = \overline{n-1}$ is always an order 2 unit in $\mathbf{Z}_n$ and $\overline{1} \in U_2(\mathbf{Z}_n)$.

Theorem 7. *Let $n = p_1^{r_1}...p_k^{r_k}$. If $p_1 = 2$ and $r_1 = 1$, then $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^{k-1} = \mathbf{Z}_2 \times ... \times \mathbf{Z}_2$, $k-1$ copies, if $p_1 = 2$ and $r_1 = 2$ or else $p_1 \geq 3$, then $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^k = \mathbf{Z}_2 \times ... \times \mathbf{Z}_2$, k copies, and if $p_1 = 2$ and $r_1 > 2$ then $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^{k+1} = \mathbf{Z}_2 \times ... \times \mathbf{Z}_2$, $k+1$ copies.*

Proof. The following is well-known (see [6], chapter XVIII, **128**).

For any *odd* prime p, or $p = 2$, $r \leq 2$, $U(\mathbf{Z}_{p^r}) \cong \mathbf{Z}_{p^r - p^{r-1}}$ with $|U(\mathbf{Z}_2)| = 1$, $U(\mathbf{Z}_{2^r}) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{r-2}}$ for any $r > 2$ and, for a finite (ring) direct product (sum) $U(R_1 \times ... \times R_k) = U(R_1) \times ... \times U(R_k)$. In the case we deal with, $U(\mathbf{Z}_n) = U(\mathbf{Z}_{p_1^{r_1}} \times ... \times \mathbf{Z}_{p_k^{r_k}}) = U(\mathbf{Z}_{p_1^{r_1}}) \times ... \times U(\mathbf{Z}_{p_k^{r_k}}) \cong \mathbf{Z}_{p_1^{r_1-1}(p_1-1)} \times ... \times \mathbf{Z}_{p_k^{r_k-1}(p_k-1)}$ for odd primes or $p_1 = 2$, $r_1 \leq 2$, and $U(\mathbf{Z}_n) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{r_1-2}} \times \mathbf{Z}_{p_2^{r_2-1}(p_2-1)} \times ... \times \mathbf{Z}_{p_k^{r_k-1}(p_k-1)}$ if $p_1 = 2$, $r_1 > 2$.

Since p_i and $p_i - 1$ are coprime, each $\mathbf{Z}_{p_i^{r_i-1}(p_i-1)} \cong \mathbf{Z}_{p_i^{r_i-1}} \times \mathbf{Z}_{p_i-1}$, so finally

$$U(\mathbf{Z}_n) \cong \mathbf{Z}_{p_1^{r_1-1}} \times ... \times \mathbf{Z}_{p_k^{r_k-1}} \times \mathbf{Z}_{p_1-1} \times ... \times \mathbf{Z}_{p_k-1}$$

in the first case and

$$U(\mathbf{Z}_n) \cong \mathbf{Z}_{2^{r_1-2}} \times \mathbf{Z}_{p_2^{r_2-1}} \times ... \times \mathbf{Z}_{p_k^{r_k-1}} \times \mathbf{Z}_2 \times \mathbf{Z}_{p_2-1} \times ... \times \mathbf{Z}_{p_k-1}$$

in the second case.

Thus, we have already $U(\mathbf{Z}_n)$ decomposed into cyclic groups which give p_i-components ($i \in \{1, ..., k\}$), but also q-components with a divisor q of some $p_i - 1$. Excepting $p_1 = 2$, all the other p_i are odd and so $p_i - 1$ is even.

The elements in $U_2(\mathbf{Z}_n)$ form the socle of the 2-component of $U(\mathbf{Z}_n)$, and so is a (finite) elementary 2-group (i.e. a finite direct sum of $\mathbf{Z}_2$). Since for $p_i \geq 3$ each $p_i - 1$ is even, it will provide an $\mathbf{Z}_{2^{t_i}}$ in the decomposition of $\mathbf{Z}_{p_i-1}$ and so one $\mathbf{Z}_2$ in the decomposition of its socle.

Hence, if $p_1 = 2$ and $r_1 = 1$, then $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^{k-1} = \mathbf{Z}_2 \times ... \times \mathbf{Z}_2$, $k-1$ copies, if $p_1 = 2$ and $r_1 = 2$ or else $p_1 \geq 3$, then $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^k = \mathbf{Z}_2 \times ... \times \mathbf{Z}_2$, k copies, and if $p_1 = 2$ and $r_1 > 2$ then $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^{k+1} = \mathbf{Z}_2 \times ... \times \mathbf{Z}_2$, $k+1$ copies. □

Using Proposition 5 we can immediately determine the order 2 units

Corollary 8. *A unit in $\mathbf{Z}_n$ is of order 2 iff each p-component has order at most 2 but at least one component has order 2. For $p > 2$ in $\mathbf{Z}_{p^k}$, $-\overline{1}$ is the only order 2 unit and in $\mathbf{Z}_{2^k}$ there are 3 order 2 units: $-\overline{1}, \overline{2^{k-1}-1}$ and $\overline{2^{k-1}+1}$.*

For the sake of completeness, in what follows we recall some elementary facts on idempotents and order 2 units.

Lemma 9. *Let R be a unital ring. Then*

(i) If $e \in R$ is an idempotent then $2e-1 \in U_2(R)$. If 4 is not a zero divisor, the converse holds.

(ii) If 2 is invertible and $u \in U_2(R)$ then $2^{-1}(u+1)$ is an idempotent.

(iii) Let R be a unital ring with $2 \in U(R)$. The map $f : \mathrm{Id}(R) \longrightarrow U_2(R)$ given by $f(e) = 2e-1$ is bijective.

(iv) The function $f(x) = 2x-1$ defined on an unspecified ring R is injective iff 2 is a unit.

(v) Let e', e be commuting idempotents. Then $2ee' - e - e' + 1$ is an idempotent.

(vi) Let R be a ring with commuting idempotents. Then $f(\mathrm{Id}(R))$ is a subgroup of $U_2(R)$.

Proof. (vi) Since we deal with order two units (i.e. $u^{-1} = u$), $f(\mathrm{Id}(R))$ is obviously closed to inverses. As for products $f(e)f(e') = (2e-1)(2e'-1) = 2(2ee' - e - e' + 1) - 1 = f(2ee' - e - e' + 1)$ and we use (i). □

Further, in the special case $R = \mathbf{Z}_n$ we can add

Corollary 10. *(i) If n is any* odd *positive integer, then $U_2(\mathbf{Z}_n) = f(\mathrm{Id}(R)) = 2\mathrm{Id}(R) - 1$. The number of order 2 units is equal to the number of idempotents, and this is 2^k if n has exactly k (distinct) prime divisors.*

(ii) f is injective on $\mathrm{Id}(\mathbf{Z}_n)$ for any n divisible by 4.

(iii) For $n = 2^s m$ with odd m and $s > 2$, $\overline{\frac{n}{2} - 1}$ is an order 2 unit in $\mathbf{Z}_n$ which is not image of idempotent through f.

Proof. (i) Let e, e' be idempotents in $\mathbf{Z}_n$ for $n = 2^s m$ with odd m and $s \geq 2$. Suppose $f(e') = f(e)$ that is $2(e' - e) = 0$. Since $0 \leq e' - e \leq n - 1$, if $e' \neq e$, this means $e' - e = \dfrac{n}{2} = 2^{s-1}m$ and so $e + 2^{s-1}m$ is an idempotent. Hence $(e + 2^{s-1}m\ )^2 = e + 2^{s-1}m$ and so $2e = 1 - 2^{s-1}m$, a contradiction in a ring of integers modulo even number. Therefore $e' = e$.

(iii) Indeed, $(2^{s-1}m - 1)^2 = 2^s m(2^{s-2}m - 1) + 1 \equiv 1 \ (\mathrm{mod} n)$ and $2^{s-1}m - 1 = f(2^{s-2}m)$, with nilpotent $2^{s-2}m$. □

With this at hand we can prove the following

Proposition 11. *For every even n, the order 2 units are obtained as images of idempotents through f with only one exception: if 8 divides n. In this case $f(\mathrm{Id}(\mathbf{Z}_n)$ is an index 2 subgroup of $U_2(\mathbf{Z}_n)$ and $U_2(\mathbf{Z}_n) - f(\mathrm{Id}(\mathbf{Z}_n) =$*

$\overline{\frac{n}{2}-1}\cdot f(\mathrm{Id}(\mathbf{Z}_n)$*, that is, the order 2 units which are not images of idempotents form a coset modulo* $\overline{\frac{n}{2}-1}$.

Proof. Suppose $n = 2^s p_2^{r_2}...p_k^{r_k}$ for odd primes p_i ($i \in \{2,...,k\}$). Again from Theorem 7, we already know that $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^{k+1}$ if $s > 2$, $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^k$ if $s = 2$ and $U_2(\mathbf{Z}_n) \cong \mathbf{Z}_2^{k-1}$ is $s = 1$. Since the number of idempotents is 2^k in all cases, the order 2 units are obtained from idempotents using the map f given above, bijective in the second case and just surjective in the third.

So order 2 units are always obtained from idempotents through f, excepting the case $s > 2$. In this case f provides only half of the order 2 units (by Lemma 10, $|f(\mathrm{Id}(\mathbf{Z}_n))| = 2^k$) and, according to Lemma 9, this subset is an index 2 subgroup of $U_2(\mathbf{Z}_n)$. By Lemma 9 (iii) $\overline{\frac{n}{2}-1}$ is an order 2 unit which is not in $f(\mathrm{Id}(\mathbf{Z}_n))$, so the remaining order 2 units are in the coset $\overline{\frac{n}{2}-1}\cdot f(\mathrm{Id}(\mathbf{Z}_n)$. □

Examples. 1) $\mathrm{Id}(\mathbf{Z}_{30}) = \{\overline{0}, \overline{1}, \overline{6}, \overline{10}, \overline{15}, \overline{16}, \overline{21}, \overline{25}\}$. These are mapped onto $U_2(\mathbf{Z}_{30}) = \{\overline{1}, \overline{11}, \overline{19}, \overline{29}\}$: $f(\overline{0}) = f(\overline{15}) = \overline{29}$, $f(\overline{1}) = f(\overline{16}) = \overline{1}$, $f(\overline{6}) = f(\overline{21}) = \overline{11}$ and $f(\overline{10}) = f(\overline{25}) = \overline{19}$.

2) For $n = 24$, the idempotents are $\mathrm{Id}(\mathbf{Z}_{24}) = \{\overline{0}, \overline{1}, \overline{9}, \overline{16}\}$. These are mapped by f into $\{\overline{23}, \overline{1}, \overline{17}, \overline{7}\}$ but there are another four order 2 units, namely $\{\overline{5}, \overline{11}, \overline{13}, \overline{19}\}$. As noticed in Lemma 9, since $\overline{7}\cdot\overline{17} = \overline{23}$, $\overline{7}\cdot\overline{23} = \overline{17}$, $\overline{17}\cdot\overline{23} = \overline{7}$, $\{\overline{1}, \overline{7}, \overline{17}, \overline{23}\}$ is an index 2 subgroup of $U_2(\mathbf{Z}_{24})$ and $\{\overline{5}, \overline{11}, \overline{13}, \overline{19}\}$ *are not images* of idempotents through f. However this is a coset $\overline{11}\cdot f(\mathrm{Id}(\mathbf{Z}_{24})) = \overline{11}\cdot\{\overline{1}, \overline{7}, \overline{17}, \overline{23}\} = \{\overline{5}, \overline{11}, \overline{13}, \overline{19}\}$ ($\overline{\frac{n}{2}-1} = \overline{11}$ in Lemma 9 (iii)).

The genuine tripotents.

As observed in Corollary 6, $[x]_n$ *is a genuine tripotent iff all* $[x]_{p_1^{r_1}}$, ...,$[x]_{p_k^{r_k}}$ *are (tripotents but) of different sort.*

First we prove the following

Proposition 12. *If* $n = p^s q^r$ *with different* odd *primes* p, q *and* $s, r \geq 0$ *then* $\mathbf{Z}_n$ *has no genuine tripotents.*

Proof. Suppose $[x]_n$ is a tripotent in $\mathbf{Z}_n$. Then $[x]_{p^s} = \overline{x}$ is a tripotent in $\mathbf{Z}_{p^s}$ and $[x]_{q^r} = \widehat{x}$ is a tripotent in $\mathbf{Z}_{q^r}$. As already noticed, these can be only $\overline{0}, \overline{1}$ or $\overline{-1}$. Excepting $(\overline{0}, \widehat{0})$, $(\overline{1}, \widehat{1})$ and $(\overline{-1}, \widehat{-1})$ which are clearly of the same sort, we have three other possibilities (and symmetric): $(\overline{0}, \widehat{1})$ both idempotents, $(\overline{-1}, \widehat{1})$ both in $U_2(\mathbf{Z}_n)$ and $(\overline{0}, \widehat{-1})$ both negatives of idempotents. Therefore,

in all possible cases $[x]_{p^s}$ and $[x]_{q^r}$ are *of the same sort*, that is, there are no genuine tripotents. □

Remarks. (i) Since $\gcd(p^s; q^r) = 1$, there are integers c, d such that $cp^s + dq^r = 1$. Then cp^s and dq^r are the only (two) nontrivial (complementary) idempotents. For $\overline{0}$ and $\overline{1}$, the negatives give $\overline{0}$ and $-\overline{1}$, the last known as order 2 unit.

Thus, $-cp^s$ and $-dq^r$ are the only (two) nontrivial negatives of idempotents.

(ii) This fails for three or more primes. For $n = 3 \cdot 5 \cdot 7 = 105$ take $[6]_n$. Then $\phi([6]_n) = ([6]_3, [6]_5, [6]_7) = ([0]_3, [1]_5, -[1]_7)$, components which are of different sort and $[6]_{105}$ is a genuine tripotent.

The only case left is $p_1 = 2$. By the above discussion, an element $[x]_n \in \mathbf{Z}_n$ for $n = 2^s p_2^{r_2} ... p_k^{r_k}$ is a genuine tripotent iff $[x]_{2^s}, [x]_{p_2^{r_2}}, ..., [x]_{p_k^{r_k}}$ are of different sort.

Since $\mathbf{Z}_{2^s}$ are local, the odd classes are units and the even classes are nilpotents. Such rings have only trivial idempotents. Therefore, the situation is similar to the odd case, but excepting $\overline{0}, \overline{1}, -\overline{1}$ we may have extra order 2 units. Not for $\mathbf{Z}_2$ or $\mathbf{Z}_4$ but for all $\mathbf{Z}_{2^s}$ with $s \geq 3$.

Hence we can state the following

Proposition 13. *Let $n = 2^s p_2^{r_2} ... p_k^{r_k}$ and $[x]_n \in \mathbf{Z}_n$.*

(i) If $k = 2$ and $s \leq 2$, $\mathbf{Z}_n$ has no genuine tripotents.

(ii) If $k = 2$ and $s \geq 3$, $\mathbf{Z}_n$ has genuine tripotents. These are listed depending on the reminder of the division of $p_2^{r_2}$ to 2^s.

(iii) If $k > 2$, $\mathbf{Z}_n$ has genuine tripotents.

Proof. (i) Exactly like the odd case (Proposition 12).

(ii) The genuine tripotents are exactly the classes $[x]_n$ such that $[x]_{2^s} \in \{\overline{3}, \overline{5}, ..., \overline{2^s - 3}\}$ and $[x]_{p_2^{r_2}} = \overline{0}$, because only such components are of different sort. Such tripotents do exist: suppose $p_2^{r_2} = 2^s c + d$ is the division with quotient c and reminder d. If $d \neq 1, 2^s - 1$ then $p_2^{r_2}$ is a genuine tripotent, and if $d \in \{1, 2^s - 1\}$ then $3p_2^{r_2}$ is a genuine tripotent.

More precisely, we have to check the reminders modulo 2^s of the multiples of $p_2^{r_2}$, which are less then n (i.e. $2^s - 1$ such multiples).

If $d \neq 1, 2^s - 1$, then $\overline{p_2^{r_2}}$ and all odd multiples $k\overline{p_2^{r_2}}$ with $kd \in \{3, 5, ..., 2^s - 3\}$ are genuine tripotents (and the number of these is the integer part $\left[\frac{2^s - 3}{d}\right]$). If $d \in \{1, 2^s - 1\}$ then $\overline{p_2^{r_2}} \in U_2(\mathbf{Z}_n)$, so is not genuine. Now the odd multiples

$k\overline{p_2^{r_2}}$ such that $k \in \{3, 5, ..., 2^s - 3\}$ are all the genuine tripotents (and these are exactly $2^{s-1} - 2$).

(iii) Now we can vary the 2-component as in (ii) but also the other (at least two) p_i-components in $\{\overline{0}, \overline{1}, -\overline{1}\}$ in order to have components of different sort. A similar discussion shows that such tripotents do exist and how these can be listed. □

Examples. 1) In $\mathbf{Z}_{24}$ take $\overline{3}$ or $\overline{21}$. For both $[3]_3 = [21]_3 = \overline{0}$ and $[3]_8 = \overline{3}$ respectively, $[21]_8 = \overline{5}$. These are the only two genuine tripotents.

2) In $\mathbf{Z}_{56}$ we have only $\overline{21}$ and $\overline{35}$ with the 7-component $\overline{0}$ (see (ii) in the previous proof).

3) In $\mathbf{Z}_{30}$ take $\overline{4}$: now $\phi(\overline{4}) = ([0]_2, [1]_3, -[1]_5)$ so this is a tripotent and a genuine one (components of different sort). There is only one other possibility: $([0]_2, -[1]_3, [1]_5)$, that is $\overline{26} = -\overline{4}$.

More general, one can check that *for any odd positive integer* p, $\overline{p+1}$ *is a genuine tripotent in* $\mathbf{Z}_{2p(p+2)}$ *and so is the negative* $\overline{2p^2+3p-1}$.

If p is a prime, these are the only genuine tripotents: there are no possible components of different sort if a tripotent is odd, so the 2-component must be $\overline{0}$ (i.e. the tripotent is even). There are only two possibilities: p-component $\overline{1}$ and $p+2$-compotent $-\overline{1}$, which gives $\overline{p+1}$ or vice-versa, with its negative $\overline{2p^2+3p-1}$.

References

[1] H. E. Bell *A commutativity study for periodic rings*. Pacific J. of Math. **70** (1) (1977), 29-36.

[2] H. E. Bell, A. Yaqub *On generalized periodic-like rings*. International J. of Math. and Math. Sciences. Volume 2007, 5 pages.

[3] A.M. Bikchentaev, R.S. Yakushev *Representation of tripotents and representations via tripotents*. Linear Algebra and its Applications **435** (2011) 2156–2165.

[4] H. Chen *On* 2×2 *strongly clean matrices*. Bull. Korean Math. Soc. **50** (1) (2013), 125–134.

[5] A. J. Diesl, T. J. Dorsey *Strongly clean matrices over arbitrary rings*. Journal of Algebra **399** (2014), 854–869.

[6] L. Fuchs *Infinite Abelian Groups*. Vol. 2, Academic Press 1973.

[7] Y. Hirano and H. Tominaga *Rings in which every element is the sum of two idempotents*. Bull. Austral. Math. Soc. **37** (2) (1988), 161-164.

[8] D. Khurana, G. Marks, A. K. Srivastava *On unit-central rings*. Trends in Math., Springer, Advances in Ring Theory, 205-212.

[9] T. Y. Lam *A first course in noncommutative rings*. Second Edition, GMT 131, Springer Verlag, 2001.

Grigore Călugăreanu,
Department of Mathematics,
Babeş - Bolyai University,
str. Kogălniceanu 1, Cluj-Napoca, Romania.
Email: calu@math.ubbcluj.ro