A7185

Scan

Shut

Report (see foot of first page for details)

~~7046~~

~~CB~~ 7185

A16090

Idempotents

C.P. Schut

Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam,
The Netherlands

In this note we summarize some well-known properties of natural number idempotents, and we explain some regularities that occur in certain sequences of idempotents.

1980 Mathematics Subject Classification: 11A07, 11A41.
Keywords & phrases: idempotents, congruences, Chinese remainder theorem.

1. Introduction

In this note we study idempotents in $\mathbb{N}$. By an <u>idempotent modulo n</u> we mean a number $m \in \mathbb{N}$ such that m^2 is congruent to m if we calculate modulo n: $m^2 \equiv m \bmod n$ (i.e. $\exists\, k \in \mathbb{N}$ such that $m^2 = m + kn$).

The most well-known idempotents are probably 5 and 6, which are the only idempotents modulo 10; 25 and 76 are the idempotents modulo 10^2; and 625 and 376 are the idempotents modulo 10^3. We shall disregard the trivial idempotents, 0 and 1.

In section 2 we give a classification of the idempotents modulo 10^k, $k \geq 1$, using elementary notions, like congruences, only. It is well known [1] that the idempotents modulo an arbitrary base number n can be classified using the prime number decomposition of n and the Chinese remainder theorem. We state and prove these classification results in section 3. Only in section 3 the reader is assumed to have some familiarity with rings of integers. In section 4 we briefly study sequences of idempotents modulo n^k where $k \in \{1, 2, \ldots, 10\}$ and $n = 2a$, a odd, and prove, completely elementarily, a regularity result concerning these sequences.

2. Idempotents modulo 10^k

In this section we classify the idempotents modulo 10^k, $k \geq 1$, using elementary calculations.

Theorem 2.1.

1. *For every $k \geq 1$ there are four idempotents modulo 10^k, among which 2 non-trivial ones.*
2. *If n and m are the two non-trivial idempotents modulo 10^k, then $n + m = 10^k + 1$.*
3. *If n is idempotent modulo 10^k and $n \equiv 5$ modulo 10, then n^2 is idempotent modulo 10^{k+1}.*
4. *If n is idempotent modulo 10^k and $n \equiv 6$ modulo 10, and if $n^2 \equiv m \cdot 10^k + n \bmod 10^{k+1}$, in which $0 \leq m < 10$, then $(10 - m) \cdot 10^k + n$ is idempotent modulo 10^{k+1}.*

Proof

1. If $m \cdot 10^k + n$ is idempotent modulo 10^{k+1}, with $0 \leq m < 10$ and $n < 10^k$, then it will be clear that n is idempotent modulo 10^k. For, if $(m \cdot 10^k + n)^2 = m \cdot 10^k + n + x \cdot 10^{k+1}$ for some x, then $m^2 \cdot 10^{2k} + 2mn \cdot 10^k + n^2 = m \cdot 10^k + n + x \cdot 10^{k+1}$. Modulo 10^k this produces $n^2 \equiv n$.

Report AM-R9101
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

Thus, when searching idempotents modulo 10^{k+1}, it suffices to look for numbers of the kind $m \cdot 10^k + n$, with n idempotent modulo 10^k.
The proof of part 1 proceeds with induction with respect to k. For $k = 1$, the only idempotents are 0, 1, 5 and 6, because $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 6$, $7^2 \equiv 9$, $8^2 \equiv 4$, and $9^2 \equiv 1$ modulo 10. Now assume that the theorem holds for some $k \geq 1$. Then we have:

$$\begin{aligned}(m \cdot 10^k + n)^2 &\equiv (m \cdot 10^k + n) \bmod 10^{k+1} \\ (m \cdot 10^k)^2 + 2mn \cdot 10^k + n^2 &\equiv (m \cdot 10^k + n) \bmod 10^{k+1} \\ m(2n-1)10^k &\equiv (n - n^2) \bmod 10^{k+1} \\ m(2n-1) &\equiv \frac{n-n^2}{10^k} \bmod 10.\end{aligned}$$

The last step is permitted, because:
(*i*) one can read "$+ \, x \cdot 10^{k+1}$" instead of "mod 10^{k+1}";
(*ii*) $n - n^2$ can be divided by 10^k, because of the idempotency of n modulo 10^k.
Simply dividing the penultimate formula by 10^k produces the last one.

From the beginning of the proof it very simply follows that $n \equiv 0$, 1, 5 or 6 modulo 10. This implies that $(2n-1) \equiv 1$ or -1, according to the value of n. From this it follows that for every n there is exactly one m so that $m \cdot 10^k + n$ is idempotent modulo 10^{k+1}. For $n \equiv 0$ or 1, $m = 0$, which produces the trivial idempotents 0 and 1. Thus, if there are 4 idempotents for some k, among which 2 non-trivial ones, the same thing holds for $k + 1$. This proves part 1.

2. If n is a non-trivial idempotent modulo 10^k, then $1 < n < 10^k$ and $1 < 10^k + 1 - n < 10^k$. Since $(10^k + 1 - n)^2 \equiv (1-n)^2 = 1 - 2n + n^2 \equiv 1 - n$ modulo 10^k, $10^k + 1 - n$ is also a non-trivial idempotent modulo 10^k. This one unequals n, because from $n \equiv (10^k + 1 - n) \bmod 10^k$ it follows that $2n \equiv 1 \bmod 10^k$, which is false for every n. This immediately produces $n + m = 10^k + 1$ if n and m are the non-trivial idempotents modulo 10^k.

3. Let m and n be as in part 1. Then it again follows:

$$\begin{aligned}(m \cdot 10^k + n)^2 &\equiv (m \cdot 10^k + n) \bmod 10^{k+1} \\ (m \cdot 10^k)^2 + 2mn \cdot 10^k + n^2 &\equiv (m \cdot 10^k + n) \bmod 10^{k+1}.\end{aligned}$$

Because $n \equiv 5$ modulo 10, it follows that $2n \equiv 0$ modulo 10, and hence $2mn \cdot 10^k \equiv 0$ modulo 10^{k+1}. This implies:

$$(m \cdot 10^k + n) \equiv n^2 \bmod 10^{k+1},$$

which was to be proved.

4. Consider the first two equations mentioned under item 3. If $n \equiv 6$ modulo 10, then $2n \equiv 2$ modulo $10 \Rightarrow 2mn \cdot 10^k \equiv 2m \cdot 10^k$ modulo 10^{k+1}. Subtracting $2m \cdot 10^k$ from both sides of the equation produces

$$((-m) \cdot 10^k + n) \equiv n^2 \bmod 10^{k+1},$$

or rather

$$((10-m) \cdot 10^k + n) \equiv n^2 \bmod 10^{k+1},$$

which was to be proved. ∎

3. Idempotents modulo arbitrary n

One may wonder whether there are any non-trivial idempotents modulo other bases than 10^k. The answer is the following:

Theorem 3.1.
If $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_\ell^{k_\ell}$, in which $p_1, p_2, \ldots, p_\ell$ are different prime numbers, there are exactly 2^ℓ different idempotents modulo n.

Proof
First take $n = p^k$, p prime, $k \in \mathbb{N}$. For an $m \in \mathbb{N}$ we write $\overline{m}$ for its representation as an element of the ring $\mathbb{Z}/n\mathbb{Z}$. That is, $\exists\, k \in \mathbb{N}$ such that $m = \overline{m} + kn$. If $\overline{m}^2 = \overline{m}$ in $\mathbb{Z}/n\mathbb{Z}$, then $\overline{m} \cdot (\overline{m} - \overline{1}) = \overline{0}$, or, in other words, $m(m-1) = c \cdot p^k$ for some integral c. This implies either $p|m$ or $p|m-1$. Those cases can't occur together, because m and $m-1$ are mutually indivisible. This furthermore implies that $p^k|m$ or $p^k|m-1$. But this means that $\overline{m} = \overline{0}$ or $\overline{m} = \overline{1}$. Thus modulo p^k there are only $2 = 2^\ell$ idempotents.
Next the general case. Let $R := \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{k_\ell}\mathbb{Z}$. It is well known that $\mathbb{Z}/n\mathbb{Z} \cong R$ (Chinese remainder theorem), in which $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ corresponds with $(\overline{1}, \overline{1}, \ldots, \overline{1}) \in R$. Let $(\overline{m_1}, \overline{m_2}, \ldots, \overline{m_\ell})$ be an arbitrary idempotent in R. Then $\overline{m_i^2} \equiv \overline{m_i}$ modulo $p_i^{k_i}$ for every $i \in \{1, 2, \ldots, \ell\}$. But from the result of the previous paragraph it follows that $\overline{m_i} \in \{\overline{0}, \overline{1}\}$ for every i. And because the idempotent has ℓ coordinates, there are 2^ℓ idempotents in R, and thus in $\mathbb{Z}/n\mathbb{Z}$. ■

Corollary 3.2.
1. *Let ℓ, n, p_i etc. be defined as above. Then there is a group of ℓ basical idempotents modulo n so that every idempotent modulo n can simply be written as the sum (modulo n) of zero or more basical idempotents.*
2. *These basical idempotents are equal to $\widetilde{m_i} \cdot \prod_{j \neq i} p_j^{k_j}$, in which $\widetilde{m_i}$ equals the inverse of $\prod_{j \neq i} p_j^{k_j}$ modulo $p_i^{k_i}$.*

Proof
1. $(\overline{1}, \overline{0}, \ldots, \overline{0})$, $(\overline{0}, \overline{1}, \ldots, \overline{0})$, …, $(\overline{0}, \overline{0}, \ldots, \overline{1})$ are ℓ different idempotents in R. It may be clear that every idempotent in R can simply be written as the sum of a number of these "vectors" (0 is the sum of 0 ones). And because $R \cong \mathbb{Z}/n\mathbb{Z}$, the idempotents in that ring can be written as the sum (modulo n) of 0 or more basical idempotents.
2. Consider the sum $\sum_{j=1}^{q} (\overline{1}, \ldots, \overline{1})$ in R, in which $q := \widetilde{m_i} \cdot \prod_{j \neq i} p_j^{k_j}$. For $j \neq i$ one finds on the j-th coordinate of that sum a $\overline{0}$, because $\overline{1}$ has the additive order $p_j^{k_j}$ in $\mathbb{Z}/p_j^{k_j}\mathbb{Z}$, and q is a multiple of that order. On the i-th coordinate of that sum one finds $\widetilde{m_i} \cdot \prod_{j \neq i} p_j^{k_j}$ modulo $p_i^{k_i}$. Considering the definition of $\widetilde{m_i}$, it follows exactly that there is a $\overline{1}$ on that coordinate. From the isomorphy of R with $\mathbb{Z}/n\mathbb{Z}$ it follows that $\sum_{j=1}^{q} \overline{1} = \overline{q}$ is a basical idempotent in $\mathbb{Z}/n\mathbb{Z}$.
P.S.: $\widetilde{m_i}$ is well defined because for every $j \neq i$ the integer $p_j^{k_j}$ is mutually indivisible with $p_i^{k_i}$, and thus a unit in $\mathbb{Z}/p_i^{k_i}\mathbb{Z}$. This also holds for the product $\prod_{j \neq i} p_j^{k_j}$. ■

Examples
1. In the hexadecimal numeration, 0 and 1 are the only idempotents modulo $(10^k)_{16}$ for every k.

I need seq A7185

2. Let n be 100. $p_2^{k_2} = 25$ and $\widetilde{m_1} \equiv \overline{25}^{-1} \bmod 4 = \overline{1} \Rightarrow \underline{q = 25}$ is one basical idempotent modulo 100. $p_1^{k_1} = 4$ and $\widetilde{m_2} \equiv \overline{4}^{-1} \bmod 25 = \overline{19} \Rightarrow q = 19 \cdot 4 = \underline{76}$ is the other basical idempotent modulo 100. This exactly lines up with the results of section 1.

3. Let n be 30. $p_2^{k_2} \cdot p_3^{k_3} = 3 \cdot 5 = 15$ and $\widetilde{m_1} \equiv \overline{15}^{-1} \bmod 2 = \overline{1} \Rightarrow \underline{q = 15}$ is the first basical idempotent modulo 30. $p_1^{k_1} \cdot p_3^{k_3} = 2 \cdot 5 = 10$ and $\widetilde{m_2} \equiv \overline{10}^{-1} \bmod 3 = \overline{1} \Rightarrow \underline{q = 10}$ is the second basical idempotent modulo 30. $p_1^{k_1} \cdot p_2^{k_2} = 2 \cdot 3 = 6$ and $\widetilde{m_3} \equiv \overline{6}^{-1} \bmod 5 = \overline{1} \Rightarrow \underline{q = 6}$ is the third basical idempotent modulo 30.

The remaining three non-trivial idempotents modulo 30 are: $\overline{6} + \overline{10} = \overline{16}$; $\overline{6} + \overline{15} = \overline{21}$; and $\overline{10} + \overline{15} = \overline{25}$.

4. Sequences of idempotents

We regard sequences of idempotents constructed in the following way: choose an odd number $a \in \mathbb{N}$ and calculate the idempotents modulo $(2a)^k$, $k \in \{1, 2, \ldots, 10\}$. An interesting regularity appears. Below we give the sequences for $a = 3, 5$ and 7.

1. For $N = 10$ $(a = 5, N = 2a)$, the idempotents modulo N^1 to N^{10} are:

A7185 A16090 idempotents: $a(n)^2 \equiv a(n)$ mod

A7185	A16090
5	6
25	76
625	376
625	9376
90625	9376
890625	109376
2890625	7109376
12890625	87109376
212890625	787109376
8212890625	1787109376

2. For $N = 6$ $(a = 3)$, the idempotents modulo N^1 to N^{10} are the following (on the left: decimal enumeration; on the right: heximal enumeration):

A259986	A259987	A259988	A259989
3	4	3	4
9	28	13	44
81	136	213	344
81	1216	213	5344
6561	1216	50213	5344
29889	16768	350213	205344
76545	203392	1350213	4205344
636417	1043200	21350213	34205344
3995649	6082048	221350213	334205344
24151041	36315136	2221350213	3334205344

%N Idempotents: \$ a(n) sup 2 ~==~ a(n) \$ mod

%O 1,1

%R (this, call it Schut91)

3. For $N = 14$ ($a = 7$), the idempotents modulo N^1 to N^{10} are the following (on the left: decimal enumeration; on the right: tetradecimal enumeration):

A259990 A259991

7	8	7	8
49	148	37	A8
2401	344	C37	1A8
2401	36016	C37	D1A8
386561	151264	A0C37	3D1A8
5764801	1764736	AA0C37	33D1A8
58471553	46941952	7AA0C37	633D1A8
374712065	1101076992	37AA0C37	A633D1A8
4802079233	15858967552	337AA0C37	AA633D1A8
149429406721	139825248256	7337AA0C37	6AA633D1A8

One notices that among the non-trivial idempotents modulo $(2a)^3$ and $(2a)^4$, two are always equal in these examples. With regard to this the following result holds:

Theorem 4.1.
Let $n = 2a$, a odd. Then a^4 is idempotent modulo n^3 and modulo n^4.

Proof
1. a^4 is idempotent modulo n^3: $(a^4)^2 \bmod n^3 \equiv (a^4)^2 \bmod 8a^3$. Now $(a^4)^2 \bmod 8a^3 \equiv a^4$ if we can find a $k \in \mathbb{N}$ such that $a^4(a^4 - 1) = k \cdot 8a^3$. The candidate is $k = \frac{a(a^4-1)}{8}$, but this is indeed a natural number, because a is odd, which implies that $8 \mid a(a-1)(a+1)(a^2+1) \Rightarrow 8 \mid a(a^4 - 1)$.
2. a^4 is idempotent modulo n^4: The reasoning is completely analogous to 1. We should find a $k' \in \mathbb{N}$ such that $a^4(a^4 - 1) = k' \cdot 16a^4$. But $a^4 - 1 = (a-1)(a+1)(a^2+1)$ and a is odd, so either $4 \mid a - 1$ or $4 \mid a + 1$. This produces $16 \mid a(a-1)(a+1)(a^2+1) \Rightarrow k' = \frac{a^4-1}{16} \in \mathbb{N}$. ■

/////

REFERENCE

[1]. D.M. BURTON, (1970), *A First Course in Rings and Ideals*, Addison-Wesley, page 216, exercise 19.

$10 sup n $.