Idempotents in Rings with Unity

Lamarr Widmer
widmer@messiah.edu

Abstract: If $*$ is a binary operation on a set S, an element a is an **idempotent for** $*$ if $a * a = a$. In this paper, we provide an alternative equivalent definition for idempotents in a ring with unity. This definition facilitates the calculations in several theorems characterizing the idempotents in rings of the form $\mathbb{Z}_n$. This material was developed by the author while teaching a one semester undergraduate class in modern algebra. Some of this material was presented to students in that class and we believe all of it is suitable for students after a basic introduction to rings.

We include numerous theorems determining the number of idempotents in $\mathbb{Z}_n$ for various factorizations of n. These theorems, along with specific examples and calculations, lead to the eventual general theorem which shows how the number of idempotents in $\mathbb{Z}_n$ is determined by the number of prime divisors of n.

Note: This is a pre-print. Notification of errors or suggestions to improve clarity are welcomed.

Definition 1: An element a in a ring R is **idempotent** if $a^2 = a$.
Definition 2: A ring with a multiplicative identity element is a **ring with unity**; the multiplicative identity element 1 is called **unity.**

Theorem 1: In any ring R with unity 1, a is an idempotent, if and only if, $a(a-1) = 0$.
proof:
Assume that R is a ring with unity 1 and that $a \in R$.
Then $a \in R$ is idempotent,
if and only if, $a^2 = a$,
if and only if, $a^2 - a = 0$,
if and only if, $a(a-1) = 0$. Q.E.D.

Theorem 2: If p is a prime number and k is a positive integer, then $\mathbb{Z}_{p^k}$ has only two idempotents.
proof: Let $\mathbb{Z}_{p^k}$ be as in the hypothesis. If a is an idempotent other than 0 and 1, then neither a nor $a-1$ is 0. No nonzero element is divisible by p^k and no two consecutive nonzero elements, $a-1$ and a, are both divisible by p. Therefore, no such product $a(a-1)$ can be equal to 0. Q.E.D.

Theorem 3: If p is an odd prime number, then $\mathbb{Z}_{2p}$ has exactly four idempotents, namely 0, 1, p and $p+1$.
proof:
Assume that p is an odd prime.
Then, if a is idempotent in $\mathbb{Z}_{2p}$, in $\mathbb{Z}_{2p}$ we have $a(a-1) = 0$. So, in $\mathbb{Z}$, we have $a(a-1) = q(2p)$ for some $q \in \mathbb{Z}$. So, either a or $a-1$ must be divisible by p.
Thus, we have only four possibilities.
If $a = 0$, then $a(a-1) = 0$ so that 0 is an idempotent in $\mathbb{Z}_{2p}$.
If $a = p$, then $a-1$ is even so that $a(a-1) = p(p-1) = 0$ in $\mathbb{Z}_{2p}$ and p is idempotent.
If $a-1 = 0$, then $a(a-1) = 0$ and $a = 1$ is idempotent.
If $a-1 = p$, then a is even in $\mathbb{Z}$ so that $a(a-1) = (p+1)p = 0$ in $\mathbb{Z}_{2p}$ and $p+1$ is idempotent. Q.E.D.

Theorem 4: If p is an odd prime and $p > 3$, then $\mathbb{Z}_{3p}$ has exactly four idempotents.

proof:
Assume that $p > 3$ is an odd prime. We know that 0 and 1 are idempotents in $\mathbb{Z}_{3p}$.
Then, if a is any idempotent in $\mathbb{Z}_{3p}$, in $\mathbb{Z}_{3p}$ we have $a(a-1) = 0$.
So, in $\mathbb{Z}$, we have $a(a-1) = q(3p)$ for some $q \in \mathbb{Z}_{3p}$. So, either a or $a-1$ is divisible by p.

First case: Assume a is a multiple of 3. So a is either 0, p or $2p$.
If $a = 0$, then 0 is an idempotent.
If $a = p$, then exactly one of the integers $a+1$ or $a-1$ is divisible by 3.
If $a+1$ is divisible by 3, then $(a+1)a = 0$ in $\mathbb{Z}_{3p}$ and $a+1 = p+1$ is an idempotent.
If $a-1$ divisible by 3, then $a(a-1) = 0$ in $\mathbb{Z}_{3p}$ and $a = p$ is an idempotent.
If ,$a = 2p$ then exactly one of the integers $2p+1$ or $2p-1$ is divisible by 3.
If $2p+1$ is divisible by 3, then $(2p+1)(2p) = 0$ in $\mathbb{Z}_{3p}$ and $2p+1$ is an idempotent.
If $2p-1$ is divisible by 3, then $2p(2p-1) = 0$ in $\mathbb{Z}_{3p}$ and $2p$ is an idempotent.

Second case: Assume that $a-1$ is a multiple of p. So $a-1$ is either 0, p or 2p.
If $a-1 = 0$, then $a(a-1) = 0$ and $a = 1$ is an idempotent.
If $a-1 = p$, then exactly one of the integers a or $a-2$ is divisible by 3.
If a is divisible by 3, then $a(a-1) = 0$ in $\mathbb{Z}_{3p}$ and $a = p+1$ is an idempotent.
If $a-2$ is divisible by 3, then $(a-1)(a-2) = 0$ in $\mathbb{Z}_{3p}$ and $a-1 = p$ is an idempotent.
If $a-1 = 2p$, then exactly one of the integers a or $a-2$ is divisible by 3.
If a is divisible by 3, then $a(a-1) = 0$ in $\mathbb{Z}_{3p}$ and $a = 2p+1$ and is an idempotent.
If $a-2$ is divisible by 3, then $(a-1)(a-2) = 0$ in $\mathbb{Z}_{3p}$ and $a-1 = 2p$ is an idempotent.

In either case, there are four idempotents: 0, 1, and two others. Q.E.D.

Theorem 4: If $p > 3$, is prime, then $\mathbb{Z}_{4p}$ has exactly four idempotents.

Proof: Assume that $p > 3$ and that p is prime.
We immediately have that 0 and 1 are idempotents in $\mathbb{Z}_{4p}$.
For any other element a which is an idempotent in $\mathbb{Z}_{4p}$, we must have $a(a-1) = 0$.
So, in $\mathbb{Z}$, $a(a-1) = q(4p)$ for some $q \in \mathbb{Z}$. Thus, either a or $a-1$ is divisible by p.

If a is divisible by p, then $a \in \{p, 2p, 3p\}$.
When $a = p$, either $p-1$ or $p+1$ is divisible by 4. So, either p or $p+1$ is idempotent in $\mathbb{Z}_{4p}$
When $a = 2p$, neither $2p-1$ nor $2p+1$ is divisible by 2. So, neither p nor $p+1$ is idempotent in $\mathbb{Z}_{4p}$. Therefore, $a = 2p$ is not possible if a is an idempotent.
When $a = 3p$, either $3p-1$ or $3p+1$ is divisible by 4. So, either $3p$ or $3p+1$ is idempotent in $\mathbb{Z}_{4p}$.

If $a-1$ is divisible by p, then $a-1 \in \{p, 2p, 3p\}$.
When $a-1 = p$, either $a = p+1$ or $a-2 = p-1$ is divisible by 4. So, either p or $p+1$ is idempotent in $\mathbb{Z}_{4p}$.
Likewise, $a-1 = 2p$ and $a-1 = 3p$ yield the same results as above.

We conclude that $\mathbb{Z}_{4p}$ has four idempotents: 0, 1 and two others. Q.E.D.

Theorem 6: If p is a prime and $p > 5$, then Z_{5p} has exactly four idempotents.

proof: Assume that p is a prime and $p > 5$. We immediately have that 0 and 1 are idempotents in Z_{5p}. For any other element b which is an idempotent, we must have $b(b-1) = 0$ in $\mathbb{Z}_{5p}$. Then in $\mathbb{Z}$, we have $b(b-1) = q(5p)$ for some $q \in \mathbb{Z}$. This requires that either b or $b-1$ be divisible by p

First case: $p \equiv_5 1$.

If $a = p$, then $a - 1 = p - 1 \equiv_5 0$ and then $a = p$ is idempotent.

If $a = 2p$, then neither $a - 1$ nor $a + 1$ is divisible by 5. So, neither $a = 2p$ nor $a + 1$ is idempotent.

If $a = 3p$, then neither $a - 1$ nor $a + 1$ is divisible by 5. So, neither $a = 3p$ nor $a + 1$ is idempotent.

If $a = 4p$, then $a \equiv_5 4$ and $a + 1$ is divisible by 5. So, $a + 1 = 4p + 1$ is idempotent.

Second case: $p \equiv_5 2$

If $a = p$, then neither $a - 1$ nor $a + 1$ is divisible by 5. So, neither a nor $a + 1$ is idempotent.

If $a = 2p \equiv_5 4$, then $a + 1 = 2p + 1$ is divisible by 5 and $a + 1 = 2p + 1$ is idempotent.

If $a = 3p \equiv_5 1$, then $a - 1$ is divisible by 5 and $a = 3p$ is idempotent.

If $a = 4p \equiv_5 3$, then neither $a - 1$ nor $a + 1$ is divisible by 5. So, neither $4p$ nor $4p + 1$ is idempotent.

Third case: $p \equiv_5 3$

If $a = p$, then neither $a - 1$ nor $a + 1$ is divisible by 5. So, neither p nor $p + 1$ is idempotent.

If $a = 2p \equiv_5 1$, then $a - 1 = 2p - 1$ is divisible by 5 and $a = 2p$ is idempotent

If $a = 3p \equiv_5 4$, then $a + 1$ is divisible by 5 and $a + 1 = 3p + 1$ is idempotent.

If $a = 4p \equiv_5 2$ then neither $a - 1$ nor $a + 1$ is divisible by 5. So, neither $4p$ nor $4p + 1$ is idempotent.

Fourth case: $p \equiv_5 4$

If, $a = p$, then $a + 1 = p + 1 \equiv_5 0$ and then $a + 1 = p + 1$ is idempotent.

If $a = 2p \equiv_5 3$, then neither $a - 1$ nor $a + 1$ is divisible by 5. So, neither $2p$ nor $2p + 1$ is idempotent.

If $a = 3p \equiv_5 2$, then neither $a - 1$ nor $a + 1$ is divisible by 5. So, neither $3p$ nor $3p + 1$ is idempotent.

If $a = 4p \equiv_5 1$, then $a - 1 = 4p - 1 \equiv_5 0$. So, $a = 4p$ is idempotent.

In every case, we find that $\mathbb{Z}_{5p}$ has exactly four idempotents, including 0 and 1. Q.E.D.

Theorem 7: If $p \geq 7$ is a prime number, then the ring $\mathbb{Z}_{6p}$ has exactly eight idempotents.

proof: Let p and $\mathbb{Z}_{6p}$ be as in the hypothesis. We immediately have that 0 and 1 are idempotents in $\mathbb{Z}_{6p}$. Now let b be any other idempotent $\mathbb{Z}_{6p}$. Then we have $b(b-1) = 0$ in $\mathbb{Z}_{6p}$. This means that in $\mathbb{Z}$, we have $b(b-1) = q(6p)$. So, either b or $b-1$ must be divisible by p.
Since p is a prime with $p \geq 7$, we know that either $p \equiv_6 1$ or $p \equiv_6 5$.

Case 1: $p \equiv_6 1$
If $a = p \equiv_6 1$, then $(a-1) \equiv_6 0$ and p is an idempotent. Since $(a+1) \equiv_6 2$, $p+1$ is not an idempotent
If $a = 2p \equiv_6 2$, then $(a+1) = (2p+1) \equiv_6 3$ and $2p+1$ is an idempotent. Since $(a-1) = (2p-1) \equiv_6 1$, $2p$ is not an idempotent.
If $a = 3p \equiv_6 3$, then both $a-1$ and $a+1$ are divisible by 2 and therefore, both $3p$ and $3p+1$ are idempotents.
If $a = 4p \equiv_6 4$, then $(a-1) = (4p-1) \equiv_6 3$ and $4p$ is an idempotent. And $(a+1) = 4p+1 \equiv_6 5$ so that $(a+1) = (4p+1)$ is not an idempotent.
If $a = 5p \equiv_6 5$, then $(a+1) = (5p+1) \equiv_6 0$, so that $a+1 = 5p+1$ s an idempotent and $5p$ is not.

Case 2: $p \equiv_6 5$
If $a = p \equiv_6 5$, then $a+1 = 0$ so that $a+1$ is idempotent and a is not idempotent, as above.
If $a = 2p \equiv_6 4$, then, as above, a is idempotent and $a+1$ is not idempotent.
If $a = 3p \equiv_6 3$, then, as above, both a and $a+1$ are idempotent.
If $a = 4p \equiv_6 2$, then, as above, $a+1$ is idempotent and a is not idempotent.
If $a = 5p \equiv_6 1$, then, as above, a is idempotent and $a+1$ is not idempotent.

In either case, $\mathbb{Z}_{6p}$ has exactly eight idempotents, including 0 and 1. Q.E.D.

Examples: In $\mathbb{Z}_{30}$, the idempotents are 0, 1, 6, 10, 15, 16, 21, 25
In $\mathbb{Z}_{42}$, the idempotents are 0, 1, 7, 15, 21, 22, 28, 36

Theorem 8: In any ring R with unity 1, an element $a \in R$ is idempotent if and only if $1-a$ is idempotent.

proof: Let $a \in R$, where R is a ring with unity.

(1) Assume that a is idempotent. So $a^2 = a$.
And then $(1-a)^2 = 1-a-a+a^2 = 1-a-a+a = 1-a$. So $1-a$ is idempotent.

(2) Assume that $1-a$ is idempotent.
Then by our result in (1), $1-(1-a) = a$ is idempotent. Q.E.D.

Example: In $M_2(\mathbb{Z}_6)$,

$A = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$ is idempotent and $I - A = \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix}$ is also idempotent.

Theorem 9: If $p \geq 11$ is a prime number, then $\mathbb{Z}_{8p}$ has only four idempotents.

proof: Let $p \geq 11$ be a prime number. Then 0 and 1 are idempotents in $\mathbb{Z}_{8p}$.
Now let b be any other idempotent in $\mathbb{Z}_{8p}$. So, we have $b(b-1) = 0$ in $\mathbb{Z}_{8p}$.
This means that in $\mathbb{Z}$, we have $b(b-1) = q(8p)$. So, either b or $b-1$ must be divisible by p.
Since p is a prime with $p \geq 11$, we have four possibilities: $p \equiv_8 1$, $p \equiv_8 3$, $p \equiv_8 5$ or $p \equiv_8 7$.

Case 1: $p \equiv_8 1$

If $a = p \equiv_8 1$, then $a - 1 \equiv_8 0$ and $a = p$ is idempotent, while $a + 1 \equiv_8 2$ so that $a+1$ is not idempotent.

If $a = 2p \equiv_8 2$, then neither $a-1$ nor $a+1$ is divisible by 4. So, neither a nor $a+1$ is idempotent.

If $a = 3p \equiv_8 3$, then neither $a-1$ nor $a+1$ is divisible by 8. So, neither a nor $a+1$ is idempotent.

If $a = 4p \equiv_8 4$, then neither $a-1$ nor $a+1$ is divisible by 2, So neither a nor $a+1$ is idempotent.

If $a = 5p$, we know from above that neither $3p$ nor $3p+1$ is idempotent. So, by Theorem 8, neither $1-3p = 1+5p$ nor $1-(3p+1) = -3p = 5p$ is idempotent.

If $a = 6p$, we know from above that neither $2p$ nor $2p+1$ is idempotent. So, by Theorem 8, neither $1-2p = 6p+1$ nor $1-(2p+1) = -2p = 6p$ is idempotent.

If $a = 7p$, we know from above that p is idempotent while $p+1$ is not idempotent. So, by Theorem 8, $1-p = 7p+1$ is idempotent while $1-(p+1) = -p = 7p$ is not idempotent.

Case 2: $p \equiv_8 3$

If $a = p \equiv_8 3$, then, as above, neither a nor $a + 1$ is idempotent.

If $a = 2p \equiv_8 6$, then, as above, neither a nor $a + 1$ is idempotent.

If $a = 3p \equiv_8 1$, then, as above a is idempotent while $a + 1$ is not idempotent.

If $a = 4p \equiv_8 4$, then, as above, neither a nor $a + 1$ is idempotent.

If $a = 5p \equiv_8 7$, then, as above, a is idempotent while $a + 1$ is not idempotent.

If $a = 6p \equiv_8 2$, then, as above, neither a nor $a + 1$ is idempotent.

If $a = 7p \equiv_8 5$, then, as above, neither a nor $a + 1$ is idempotent.

Case 3: $p \equiv_8 5$

If $a = p \equiv_8 5$, then, as above, neither a nor $a + 1$ is idempotent.

If $a = 2p \equiv_8 2$, then, as above, neither a nor $a + 1$ is idempotent.

If $a = 3p \equiv_8 7$, then, as above, $a + 1$ is idempotent while a is not idempotent.

If $a = 4p \equiv_8 4$, then, as above, neither a nor $a + 1$ is idempotent.

If $a = 5p \equiv_8 1$, then, as above, a is idempotent while $a + 1$ is not idempotent.

If $a = 6p \equiv_8 6$, then, as above, neither a nor is $a + 1$ idempotent.

If $a = 7p \equiv_8 3$, then, as above, neither a nor is $a + 1$ idempotent.

Case 4: $p \equiv_8 7$

In this case, the values of $p, 2p, 3p, 4p, 5p, 6p, 7p$ are congruent modulo 8, respectively, to $7, 6, 5, 4, 3, 2, 1$. Then, as above, $a = p$ will correspond to the idempotent $p + 1$ while $a = 7p$ will correspond to the idempotent $7p$.

In every case, we have four idempotents: 0, 1 and two others. Q.E.D.

Examples: The idempotents of $\mathbb{Z}_{88}$ are 0, 1, 33 and 56 .
The idempotents of $\mathbb{Z}_{104}$ are 0, 1, 40 and 65 .

Theorem 10: If $p \geq 11$ is a prime number, then $\mathbb{Z}_{9p}$ has only four idempotents.

proof: Let $p \geq 11$ be a prime number. Then 0 and 1 are idempotents in $\mathbb{Z}_{9p}$.
Now let b be any other idempotent in $\mathbb{Z}_{9p}$. Then we have $b(b-1) = 0$ in $\mathbb{Z}_{9p}$.
This means that in $\mathbb{Z}$, we have $b(b-1) = q(8p)$. So, either b or $b-1$ must be divisible by p.
Since p is a prime with $p \geq 11$, we have six possibilities. That is, p may be congruent to 1, 2, 4, 5, 7 or 8 modulo 9.

Case 1: $p \equiv_9 1$
If $a = p \equiv_9 1$, $(a-1) = p \equiv_9 0$ and $a = p$ is idempotent and $(a+1) \equiv_9 2$ so that $a+1$ is not idempotent.
If $a = 2p \equiv_9 2$, neither $a-1$ nor $a+1$ is divisible by 9 and therefore, neither a nor $a+1$ is idempotent.
If $a = 3p \equiv_9 3$, neither $a-1$ nor $a+1$ is divisible by 3 and therefore, neither a nor $a+1$ is idempotent.
If $a = 4p \equiv_9 4$, neither $a-1$ nor $a+1$ is divisible by 9 and therefore, neither a nor $a+1$ is idempotent.
If $a = 5p \equiv_9 5$, neither $a-1$ nor $a+1$ is divisible by 9 and therefore, neither a nor $a+1$ is idempotent.
If $a = 6p \equiv_9 6$, neither $a-1$ nor $a+1$ is divisible by 3 and therefore, neither a nor $a+1$ is idempotent.
If $a = 7p \equiv_9 7$, neither $a-1$ nor $a+1$ is divisible by 9 and therefore, neither a nor $a+1$ is idempotent.
If $a = 8p \equiv_9 8$, then $a-1$ is not divisible 9 by and therefore a is not idempotent. Since $a+1$ is divisible by 9, $a+1 = 8p+1$ is idempotent.

Case 2: $p \equiv_9 2$
In this case we have $a = 4p \equiv_9 8$, so that $a+1 = 4p+1$ is idempotent.
And we have $a = 5p \equiv_9 1$, so that $a = 5p$ is idempotent.

Case 3: $p \equiv_9 4$
In this case we have $a = 2p \equiv_9 8$, so that $a+1 = 2p+1$ is idempotent.
And we have $a = 7p \equiv_9 1$, so that $a = 7p$ is idempotent.

Case 4: $p \equiv_9 5$
In this case we have $a = 2p \equiv_9 1$, so that $a = 2p$ is idempotent.
And we have $a = 7p \equiv_9 8$, so that $a + 1 = 7p + 1$ is idempotent.

Case 5: $p \equiv_9 7$
In this case we have $a = 4p \equiv_9 1$, so that $a = 4p$ is idempotent.
And we have $a = 5p \equiv_9 8$, so that $a + 1 = 5p + 1$ is idempotent.

Case 6: $p \equiv_9 8$
In this case we have $a = p \equiv_9 8$, so that $a + 1 = p + 1$ is idempotent.
And we have $a = 8p \equiv_9 1$, so that $a = 8p$ is idempotent.

In all cases, $\mathbb{Z}_{9p}$ has only four idempotents. Q.E,D.

Examples:
In $\mathbb{Z}_{99}$, the idempotents are 0, 1, 45 and 55.
In $\mathbb{Z}_{117}$, the idempotents are 0, 1, 27 and 91.
In $\mathbb{Z}_{153}$, the idempotents are 0, 1, 18 and 136.

Observations, calculations and examples

The most fundamental calculation in the exploration of our topic is that of finding the idempotents of a ring. Any ring has an identity 0, which is, by definition, an idempotent. A ring with no unity element may have no other idempotent e.g. the ring $2\mathbb{Z}$. In a ring with unity 1, we have at least two idempotents, namely 0 and 1. In a ring $\mathbb{Z}_n$, the search for idempotents is facilitated by checking the equation $a(a-1)=0$ rather than $a^2=a$. Our worksheet for these calculations is shown in the following examples. In the second and third columns, we mark the entries which complete the necessary factors to satisfy the equation $a(a-1)=0$ We note the pairs of idempotents specified by our Theorem 8 which are evident in this worksheet and their absence would indicate a calculation error. These worksheets reveal the pattern at the heart of our final theorem, Theorem 12.

Example: $\mathbb{Z}_{143}$ $143=11\times13$

n=13q	n-1	n+1	idempotent
13	12	14	
26	25	27	
39	38	40	
52	51	53	
65	64	66 *	66
78	77*	79	78
91	90	92	
104	103	105	
117	116	118	
130	129	131	

Example: $\mathbb{Z}_{56}$ $56=2^3\times7$

n=8q	n-1	n+1	idempotent
8	7*	9	8
16	15	17	
24	23	25	
32	31	33	
40	39	41	
48	47	49*	49

Example: $\mathbb{Z}_{14}$ $14 = 2 \times 7$

n=7q	n-1	n+1	idempotent
7	6*	8*	7, 8

Example: $\mathbb{Z}_{30}$ $30 = 2 \times 3 \times 5$

n=15q	n-1	n+1	idempotent
15	14*	16*	15,16

n=10q	n-1	n+1	idempotent
10	9*	11	10
20	19	21*	21

n=6q	n-1	n+1	idempotent
6	5*	7	6
12	11	13	
18	17	19	
24	23	25*	25

Example: $\mathbb{Z}_{105}$ $105 = 3 \times 5 \times 7$

n=15q	n-1	n+1	idempotent
15	14*	16	15
30	29	31	
45	44	46	
60	59	61	
75	74	76	
90	89	91*	91

n=21q	n-1	n+1	idempotent
21	20*	22	21
42	41	43	
63	62	64	
84	83	85*	85

n=35q	n-1	n+1	idempotent
35	34	36*	36
70	69*	71	70

Example: $\mathbb{Z}_{210}$ $210 = 2 \times 3 \times 5 \times 7$

n=105q	n-1	n+1	idempotent
105	104*	106*	105,106

n=70q	n-1	n+1	idempotent
70	69*	71	70
140	139	141*	141

n=42q	n-1	n+1	idempotent
42	41	43	
84	83	85*	85
126	125*	124	126
168	167	169	

n=30q	n-1	n+1	idempotent
30	29	31	
60	59	61	
90	89	91*	91
120	119 *	121	120
150	149	151	
180	179	181	

n=35q	n-1	n+1	idempotent
35	34	36*	36
70	69	71	
105	104	106	
140	139	141	
175	174*	176	175

n=21q	n-1	n+1	idempotent
21	20*	22	21
42	41	43	
63	62	64	
84	83	85	
105	104	106	
126	125	127	
147	146	148	
168	167	169	
189	188	190*	190

n=14q	n-1	n+1	idempotent
14	13	15*	15
28	27	29	
42	41	43	
56	55	57	
70	69	71	
84	83	85	
98	97	99	
112	111	113	
126	125	127	
140	139	141	
154	153	155	
168	167	169	
182	181	183	
196	195	197	196

Theorem 11: If f_1 and f_2 are relatively prime positive integers, then there is exactly one integer q such that $1 \leq q < f_1$ and $a = qf_2$ and $1 - a$ are idempotent in $\mathbb{Z}_{f_1 f_2}$.

Proof: Let f_1 and f_2 be as in the hypothesis. We assume that a is an idempotent other than 0 or 1 in $\mathbb{Z}_{f_1 f_2}$. This means that $a(a-1) = 0$ in $\mathbb{Z}_{f_1 f_2}$.

If a is divisible by f_1 , then f_2 is congruent modulo f_1 to a generator of $\mathbb{Z}_{f_1}$. So, there is an integer q such that $1 \leq q < f_1$ and $a = qf_2 \equiv_{f_1} 1$.
So, we have $a(a-1) = qf_2(qf_2 - 1) = 0$ and a is idempotent.
And then by Theorem 8, $1 - a = 1 - qf_2$ is idempotent.
Q.E.D.

Theorem 12: If the integer m has n prime factors, then the ring $\mathbb{Z}_m$ has 2^nidempotents.
Proof: We assume that the integer m has n prime factors.
If $n = 0$, then $\mathbb{Z}_m$ is the trivial ring $\mathbb{Z}_1$ which has $1 = 2^0$ idempotent.
Otherwise, we have $\mathbb{Z}_m = p_1^{e^1} p_2^{e^2} \ldots p_n^{e^n}$.
Now the set $S = \{p_1 , p_2 , \ldots , p_n\}$ has 2^n subsets. Then there are 2^{n-1} sets of the form$\{A , S - A\}$, where $A \subseteq S$. One of these sets is $\{\phi , S\}$.
By Theorem 11, each of the $2^{n-1} - 1$ other $\{A , S - A\}$ sets corresponds to two idempotents, none of which is 0 or 1.
Therefore, the total number of idempotents in $\mathbb{Z}_m$ is $2 + 2(2^{n-1} - 1) = 2 + 2^n - 2 = 2^n$.
Q.E.D.