information

MDPI

Article

Idempotent Factorizations of Square-Free Integers

Barry Fagin

Department of Computer Science, US Air Force Academy, Colorado Springs, CO 80840, USA; barry.fagin@usafa.edu; Tel.: +1-719-333-7377

Received: 20 June 2019; Accepted: 3 July 2019; Published: 6 July 2019

Abstract: We explore the class of positive integers n that admit *idempotent factorizations* $n = \bar{p}\bar{q}$ such that $\lambda(n) \mid (\bar{p}-1)(\bar{q}-1)$, where λ is the Carmichael lambda function. Idempotent factorizations with $\bar{p}$ and $\bar{q}$ prime have received the most attention due to their cryptographic advantages, but there are an infinite number of n with idempotent factorizations containing composite $\bar{p}$ and/or $\bar{q}$. Idempotent factorizations are exactly those $\bar{p}$ and $\bar{q}$ that generate correctly functioning keys in the Rivest–Shamir–Adleman (RSA) 2-prime protocol with n as the modulus. While the resulting $\bar{p}$ and $\bar{q}$ have no cryptographic utility and therefore should never be employed in that capacity, idempotent factorizations warrant study in their own right as they live at the intersection of multiple hard problems in computer science and number theory. We present some analytical results here. We also demonstrate the existence of *maximally idempotent* integers, those n for which all bipartite factorizations are idempotent. We show how to construct them, and present preliminary results on their distribution.

Keywords: cryptography; abstract algebra; Rivest–Shamir–Adleman (RSA); computer science education; cryptography education; number theory; factorization

MSC: [2010] 11Axx 11T71

1. Introduction

Certain square-free positive integers n can be factored into two numbers $(\bar{p}, \bar{q})$ such that $\lambda(n) \mid (\bar{p}-1)(\bar{q}-1)$, where λ is the Carmichael lambda function. We call such $(\bar{p}, \bar{q})$ an *idempotent factorization* of n, and $(n, \bar{p}, \bar{q})$ an idempotent tuple. We say that $n = \bar{p}\bar{q}$ admits an idempotent factorization. (Overbars indicate that $\bar{p}, \bar{q}$ are not necessarily prime.)

When n is prime, all factorizations are trivially idempotent ($p = 1$ or $q = 1$). For p and q prime, the factorization $n = \bar{p}\bar{q}$ is idempotent due to Euler's Theorem and the exponent cycle length property of λ. If p and q are sufficiently large, such factorizations have useful cryptographic properties, and are the basis for the 2-prime Rivest–Shamir–Adleman (RSA) cryptosystem [1]. Carmichael numbers [2] also easily form idempotent products.

These, however, are not the only idempotent factorizations. While they do not use the term themselves, Huthnance and Warndof [3] describe idempotent factorizations $n = \bar{p}\bar{q}$, where $\bar{p}$ and $\bar{q}$ are either primes or Carmichael numbers, noting that such integers generate correct RSA keys. These values are in fact a subset of idempotent factorizations as we define them here, as there are an infinite number of idempotent tuples $(n, \bar{p}, \bar{q})$ with composite $\bar{p}$ and/or $\bar{q}$ where neither $\bar{p}$ nor $\bar{q}$ are Carmichael numbers. We emphasize that, like the subset of idempotent tuples noted in [3], these numbers should never be used cryptographically [4]. We merely note that idempotent factorizations are exactly those $\bar{p}, \bar{q}$ that "fool" RSA in the sense that such $n, \bar{p}, \bar{q}$ supplied to the 2-prime RSA protocol will generate keys that encrypt and decrypt messages correctly.

An idempotent factorization of the form $n = \bar{p}q$ or $n = p\bar{q}$ with one composite and one prime is a *semi-composite* idempotent factorization. A factorization of the form $n = \bar{p}\bar{q}$ with both components

composite is a *fully composite* idempotent factorization (implying n has at least four factors). Trivial factorizations ($\bar{p}$ or $\bar{q} = 1$) and factorizations of n where n is a semiprime ($\bar{p}$ and $\bar{q}$ prime) will not be considered further.

2. Idempotent Factorizations of a Carmichael Number

Carmichael numbers C have the property $C - 1 \underset{\lambda(C)}{\equiv} 0$. Let $C = \bar{p}\bar{q}$ be a factorization of C. For a factorization of a Carmichael number to be idempotent, we have

$$\begin{aligned} & (\bar{p}-1)(\bar{q}-1) \underset{\lambda(C)}{\equiv} 0, \\ \iff & (\bar{p}\bar{q}-1)-\bar{p}-\bar{q}+2 \underset{\lambda(C)}{\equiv} 0, \\ \iff & (C-1)-\bar{p}-\bar{q}+2 \underset{\lambda(C)}{\equiv} 0, \\ \iff & -\bar{p}-\bar{q}+2 \underset{\lambda(C)}{\equiv} 0, \\ \iff & \bar{p}+\bar{q} \underset{\lambda(C)}{\equiv} 2. \end{aligned}$$

3. Maximally Idempotent Integers

If all bipartite factorizations of n are idempotent, we say that n is *maximally idempotent*.

Let $n = p_1p_2p_3$, with all p_i prime. Let $a = p_1 - 1, b = p_2 - 1, c = p_3 - 1, \lambda(n) = \text{lcm}(a, b, c) = \lambda$. Suppose that $\bar{p} = p_1p_2, q = p_3$ is an idempotent factorization. We have

$$\begin{aligned} & [(a+1)(b+1)-1]c \underset{\lambda}{\equiv} 0, \\ \iff & (ab+a+b+1-1)c \underset{\lambda}{\equiv} 0, \\ \iff & abc+ac+bc \underset{\lambda}{\equiv} 0, \\ \iff & ac+bc \underset{\lambda}{\equiv} 0. \end{aligned}$$

Similarly, for the other two factorizations, we have $ab + bc \underset{\lambda}{\equiv} 0$ and $ab + ac \underset{\lambda}{\equiv} 0$. Thus, n is maximally idempotent $\iff ac + bc \underset{\lambda}{\equiv} 0$ & $ab + bc \underset{\lambda}{\equiv} 0$ & $ab + ac \underset{\lambda}{\equiv} 0$. For these three conditions to all be true, $ab \equiv ac \equiv bc \underset{\lambda}{\equiv} x$. For $a < b < c \leq \lambda = \text{lcm}(a, b, c)$, the only possibility is $x = 0$.

This gives the following theorem:

Theorem 1. *Let $n = p_1p_2p_3$ with each p_i prime. Let $a = p_1 - 1, b = p_2 - 1, c = p_3 - 1, \lambda(n) = lcm(a, b, c) = \lambda$. n is maximally idempotent $\iff (ab \equiv ac \equiv bc \underset{\lambda}{\equiv} 0)$.*

For the system of three nonlinear modular equations above consider the terms ab, ac, bc. If all of them are $\underset{\lambda}{\equiv} 0$, all three equations are satisfied. If exactly two of them are $\underset{\lambda}{\equiv} 0$, only one equation is satisfied. If exactly one is $\underset{\lambda}{\equiv} 0$, no equations are satisfied. If none are $\underset{\lambda}{\equiv} 0$, there are three possibilities: No equations are satisfied, one is satisfied if $ab \underset{\lambda}{\equiv} -ac$, or three are satisfied if $ab \underset{\lambda}{\equiv} -ac, ab \underset{\lambda}{\equiv} -bc$. Thus, no integer $n = p_1p_2p_3$ can have exactly two idempotent factorizations.

Since the equations for maximal idempotency are all sums of products of two or more a_i with no duplicates, and that these sums are all $\underset{\lambda}{\equiv} 0$, we have the following result:

Theorem 2. *Let $n = p_1p_2...p_m$ with all p_i prime, $a_i = p_i - 1, \lambda(n) = lcm(a_1, a_2...a_m) = \lambda$. $\forall i \neq j \prod a_ia_j \underset{\lambda}{\equiv} 0 \rightarrow$ n is maximally idempotent.*

The maximally idempotent integer $137555 = 5 \times 11 \times 41 \times 61$ shows the converse of this theorem is false. $\lambda(137555) = 120$, and $60 \times 40 \underset{\lambda}{\equiv} 0$, but $4 \times 10 \underset{120}{\not\equiv} 0, 10 \times 40 \underset{120}{\not\equiv} 0$, etc.

As shown previously, a Carmichael number C is maximally idempotent $\iff \forall\, \bar{p}\bar{q} = C, \bar{p} + \bar{q} \underset{\lambda(C)}{\equiv} 2$.

4. Strong Impostors and Idempotent Factorizations

We have shown [5] that square-free composite numbers $\bar{s}$ with the property $\lambda(\bar{s})|2(\bar{s}-1)$ produce semi-composite idempotent tuples $(n, \bar{s}, r)$ when paired with any prime r coprime to $\bar{s}$. We called these $\bar{s}$ *strong impostors* because they behave as prime numbers to the 2-prime RSA protocol. Strong impostors include the Carmichael numbers, which have been long known to have this property, but are not limited to them. It can easily be shown that the product of any two odd coprime strong impostors s_1, s_2 is idempotent.

5. Examples

The first 16 square-free n with $m \geq 3$ factors that admit idempotent factorizations are shown in Table 1.

Table 1. Values of n that admit idempotent factorizations.

n	p or $\bar{p}$	$\bar{q}$
30	5	6
42	7	6
66	11	6
78	13	6
102	17	6
105	7	15
114	19	6
130	13	10
138	23	6
165	11	15
170	17	10
174	29	6
182	13	14
186	31	6
195	13	15
210	10	21

6 and 15 are strong impostors, but 10, 14, and 21 are not. In addition, $210 = 2 \times 3 \times 5 \times 7$ is the smallest square-free n that can be factored into two composite factors. It can be so factored in three ways, of which (10, 21) is fully composite and idempotent.

Values of n also exist which admit multiple idempotent factorizations. $n = 273$ has idempotent factorizations of (3, 91), (7, 39) and (13, 21), all of which are semi-composite. $n = 1365$ has both semi-composite and fully composite idempotent factorizations: (7, 195), (13, 105) and (15, 91). The latter is the product of two odd strong impostors.

The first 16 maximally idempotent n with three and four prime factors are shown in Table 2, along with the two 5-factor cases $< 2^{30}$. Carmichael numbers are underlined.

Table 2. Maximally idempotent integers with 3, 4 and 5 factors.

3 Factors	λ	4 Factors	λ	5 Factors	λ
$273 = 3 \times 7 \times 13$	12	$\underline{63{,}973} = 7 \times 13 \times 19 \times 37$	36	$72{,}719{,}023 = 13 \times 19 \times 37 \times 73 \times 109$	216
$455 = 5 \times 7 \times 13$	12	$\overline{137{,}555} = 5 \times 11 \times 41 \times 61$	120	$213{,}224{,}231 = 11 \times 31 \times 41 \times 101 \times 151$	300
$\underline{1729} = 7 \times 13 \times 19$	36	$145{,}607 = 7 \times 11 \times 31 \times 61$	60		
$2109 = 3 \times 19 \times 37$	36	$245{,}791 = 7 \times 13 \times 37 \times 73$	72		
$2255 = 5 \times 11 \times 41$	40	$356{,}595 = 5 \times 19 \times 37 \times 73$	72		
$2387 = 7 \times 11 \times 31$	30	$270{,}413 = 11 \times 13 \times 31 \times 61$	60		
$3367 = 7 \times 13 \times 37$	36	$536{,}389 = 7 \times 19 \times 37 \times 109$	108		
$3515 = 5 \times 19 \times 37$	72	$667{,}147 = 13 \times 19 \times 37 \times 73$	72		
$4433 = 11 \times 13 \times 31$	60	$996{,}151 = 13 \times 19 \times 37 \times 109$	108		
$4697 = 7 \times 11 \times 61$	60	$1{,}007{,}903 = 13 \times 31 \times 41 \times 61$	120		
$4921 = 7 \times 19 \times 37$	36	$1{,}847{,}747 = 11 \times 17 \times 41 \times 241$	240		
$5673 = 3 \times 31 \times 61$	60	$1{,}965{,}379 = 13 \times 19 \times 73 \times 109$	216		
$6643 = 7 \times 13 \times 73$	72	$2{,}060{,}863 = 7 \times 37 \times 73 \times 109$	216		
$6935 = 5 \times 19 \times 73$	72	$2{,}395{,}897 = 7 \times 31 \times 61 \times 181$	180		
$7667 = 11 \times 17 \times 41$	80	$2{,}778{,}611 = 11 \times 41 \times 61 \times 101$	600		
$8103 = 3 \times 37 \times 73$	72	$3{,}140{,}951 = 11 \times 31 \times 61 \times 151$	300		

Maximally idempotent integers are rare. Below 2^{30} there are 15189 with three prime factors, 315 with 4, and 2 with 5.

There are no maximally idempotent integers with six or more factors below 2^{32}. The smallest 6-factor maximally idempotent integer M(6) is $11 \times 31 \times 41 \times 61 \times 101 \times 151$. The smallest maximally idempotent integer with seven factors known to the author is $(\lambda(\mathrm{M}(6)) + 1) \times \mathrm{M}(6) = 601 \times \mathrm{M}(6)$.

5.1. Cumulative Statistics for Idempotent Factorizations of the Carmichael Numbers

An analysis of maximally idempotent Carmichael numbers $< 10^{18}$ is shown in Table 3 [6].

Table 3. Maximally idempotent integers among the Carmichael numbers.

Proportion of Maximally Idempotent Integers			
# factors	Carmichael #'s $< 10^{18}$	integers $< 2^{30}$	ratio
3	5.5862×10^{-4}	1.4145×10^{-5}	39.5
4	2.3543×10^{-5}	2.9336×10^{-7}	80.3
5	7.1344×10^{-7}	1.8626×10^{-9}	383.0

As expected, maximally idempotent integers are found at higher proportions in the Carmichael numbers, although they remain rare. There is only one 5-factor maximally idempotent Carmichael number in the results above: C598349 = $661 \times 991 \times 3301 \times 4951 \times 9901$. It is the smallest such Carmichael number.

6. Constructing Maximally Idempotent Integers

Knowing sufficient conditions for the existence of idempotent factorizations and maximal idempotency suggests constructive approaches. We may construct a set of maximally idempotent integers sharing a given λ in the following way:

(1) Pick some prime p, let $\lambda = p - 1$. (2) Find all the divisors of λ a_i such that $p_i = a_i + 1$ is prime. (3) Construct the *divisor graph* of λ by creating a node for each a_i, with an edge from each a_i to every node a_j such that $\lambda / a_i \mid a_j$. Any two such nodes will have the property $a_i a_j \underset{\lambda}{\equiv} 0$. Thus, by Theorem 2, every k-clique with $k \geq 3$ in the resulting graph corresponds to a maximally idempotent integer with k prime factors. Each node a_i corresponds to a prime factor $p_i = a_i + 1$, with a maximally idempotent n equal to the product of all corresponding p_i in the subgraph. It follows that all divisors of such constructed integers with more than two factors are also maximally idempotent.

For example, consider $p = 37, \lambda = 36$. The resulting divisors a_i with $p_i = a_i + 1$ prime are $1, 2, 4, 12, 18, 36$. This produces the divisor graph of Figure 1.

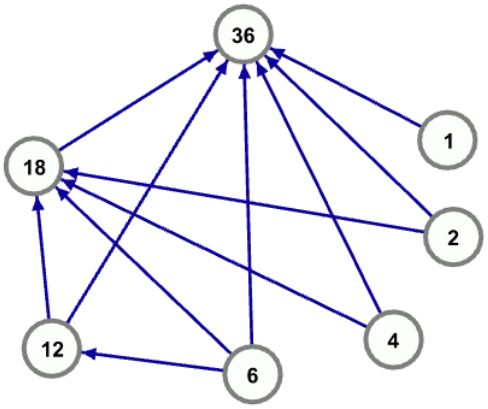

Figure 1. Divisor graph for $\lambda = 36$.

This graph contains six 3-cliques and one 4-clique. These correspond to seven maximally idempotent integers with $\lambda = 36$. Five of the six 3-cliques correspond to integers in Table 2. The 4-clique is the smallest maximally idempotent integer with four factors, also shown in Table 2.

To construct a maximally idempotent integer with a large number of factors, choose p such that $\lambda = p - 1$ is highly composite. The divisor graph will then have a large number of nodes, high connectivity and a greater likelihood of k-cliques for larger k.

For example, we may choose $p = 44{,}101, \lambda = 44{,}100 = (2 \times 3 \times 5 \times 7)^2$. The procedure above yields the 31-node graph shown in Figure 2.

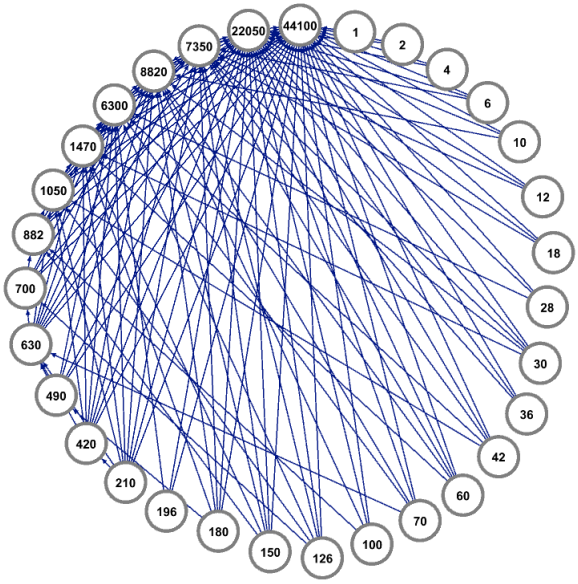

Figure 2. Divisor graph for $\lambda = 44{,}100$.

This graph has a total of 1293 k-cliques with $k \geq 3$. The largest clique has 10 nodes, corresponding to the 10-factor maximally idempotent integer $n = 211 \times 421 \times 631 \times 1051 \times 1471 \times 6301 \times 7351 \times 8821 \times 22{,}051 \times 44{,}101$.

We may define a function $\mu(p)$ as the number of maximally idempotent integers M with $\lambda(p) = p - 1$ that can be constructed in this way. The domain of this function is the primes. The range is the set of numbers y that are the total number of k-cliques in the divisor graph for some p with $\lambda(p) = p - 1$, $k \geq 3$. The first 16 nonzero values of $\mu(p)$ are shown in Table 4.

Table 4. Nonzero values of $\mu(p)$.

p	$\mu(p)$
13	2
31	1
37	7
41	1
61	11
67	1
73	14
89	1
97	2
109	9
113	2
127	2
156	11
181	19
193	8
199	3

By this definition and computer analysis of the graph in Figure 2, the value of $\mu(44{,}101)$ is 1293.

7. Cumulative Statistics on Idempotent Factorizations

Cumulative statistics for idempotent factorizations for $n < 2^{30}$ are shown below (Tables 5–7). R_{sf} indicates the ratio of numbers with idempotent factorizations to the total number of candidates n, those square-free numbers with > 2 factors. R_N indicates the ratio to all n in the indicated interval. The first entry in R_{cpu} is the computation time in seconds on the author's computer for the indicated interval. Remaining entries are the ratio of computation time of the current interval to the previous interval. An entry of the form i:j in row with #factors = F indicates that there are j integers $< 2^{30}$ with F prime factors and i idempotent factorizations.

All answers are rounded to the indicated number of decimals. We ignore order when counting factorizations.

Table 5. Proportion of integers with idempotent factorizations.

Max n	$\mathbf{2^{12}}$	$\mathbf{2^{15}}$	$\mathbf{2^{18}}$	$\mathbf{2^{21}}$	$\mathbf{2^{24}}$	$\mathbf{2^{27}}$	$\mathbf{2^{30}}$
R_{sf}	0.61	0.37	0.28	0.21	0.17	0.13	0.11
R_N	0.09	0.09	0.08	0.07	0.06	0.05	0.04
R_{cpu}	-	2.7	11.3	10.6	13.3	9.8	10.4

Table 6. Factor distribution of idempotent factorizations $< 2^{30}$ (<8 factorizations).

# Factors	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
3	184,510,285	34,215,577	0	15,189	0	0	0	0
4	132,479,584	11,347,214	4448	15,678	28	235	0	315
5	50,515,758	1,733,232	6530	13,743	93	599	1	441
6	10,004,651	242,377	6143	6906	167	586	12	302
7	931,270	35,473	2994	1597	124	286	22	102
8	29,211	2956	477	158	39	43	5	6
9	99	28	7	2	1	0	1	1

Table 7. Factor distribution of idempotent factorizations $< 2^{30}$ (≥8 factorizations).

# Factors						
5	8:2	9:6	11:18	15:2		
6	8:3	9:10	11:31	15:20		
7	8:3	9:5	10:1	11:24	15:3	31:1
8	8:1	9:2	11:4			

8. Idempotent Tuples and RSA

Unlike factorizations of n with p and q prime, idempotent factorizations of n with composite $\bar{p}$ and/or $\bar{q}$ offer no cryptographic utility. Like the Carmichael numbers, they should never be used in practice [4]. Nonetheless, all idempotent factorizations of n produce correct results if used in the 2-prime RSA protocol. Given $n = \bar{p}\bar{q}$, choosing any integers (e, d) with $ed \underset{(\bar{p}-1)(\bar{q}-1)}{\equiv} 1$ yields public and private keys that work correctly. This arises from the definition of idempotency.

Theorem 3. *A factorization of square-free n into $(\bar{p}, \bar{q})$ with $n = \bar{p}\bar{q}$ and $(\bar{p}, \bar{q}) > 1$ produces correctly functioning keys for 2-prime RSA iff the factorization is idempotent.*

We note a well-known property of the Carmichael function: $\lambda(n)$ is the smallest positive integer such that $\forall a \in Z_n, a^{\lambda(n)+1} \underset{n}{\equiv} a$. It follows by induction that $\forall a \in Z_n, a^{k\lambda(n)+1} \underset{n}{\equiv} a \ \forall k \geq 0$.

Proof. ($\rightarrow$): Let $n = \bar{p}\bar{q}$ produce correctly functioning keys for 2-prime RSA. Encryptions and decryption keys (e, d) are chosen such so that $ed - 1 \underset{(\bar{p}-1)(\bar{q}-1)}{\equiv} 0$. By hypothesis, we have $a^{ed} \underset{n}{\equiv} a \ \forall a \in Z_n$. Since $ed - 1$ is a multiple of $(p-1)(q-1)$, we have

$$a^{ed} \underset{n}{\equiv} a^{ed-1}a \underset{n}{\equiv} a^{k(p-1)(q-1)}a \underset{n}{\equiv} a$$

for all $k > 0$. Writing $(p-1)(q-1)$ as $m\lambda(n) + r, 0 \leq r < \lambda$, we have $\forall a \in Z_n$:

$$a^{k(p-1)(q-1)}a \underset{n}{\equiv} a^{k(m\lambda(n)+r)}a \underset{n}{\equiv} a.$$

We must show $r = 0$.

By the exponent cycle length property of λ, we have

$$a^{k(m\lambda(n)+r)}a \underset{n}{\equiv} a^{km\lambda(n)}a^{kr}a \underset{n}{\equiv} a^{km\lambda(n)+1}a^{kr} \underset{n}{\equiv} aa^{kr} \underset{n}{\equiv} a^{kr+1} \underset{n}{\equiv} a.$$

$\forall a \in Z_n, \ \forall k \geq 0$. Choosing $k = 1$, we have $a^{r+1} \underset{n}{\equiv} a \ \forall a \in Z_n$. $\lambda(n)$ is the smallest positive integer for which this is possible, so $r = 0$.

($\leftarrow$): By hypothesis, let n be a square-free positive integer, $n = \bar{p}\bar{q}$, $(\bar{p}-1)(\bar{q}-1) = m\lambda(n)$ for some positive integer l. Let (e, d) be positive integers such that $ed - 1 \underset{(\bar{p}-1)(\bar{q}-1)}{\equiv} 0$. We have

$$a^{ed} \underset{n}{\equiv} a^{ed-1}a \underset{n}{\equiv} a^{k(p-1)(q-1)}a \underset{n}{\equiv} a^{km\lambda(n)}a \underset{n}{\equiv} a^{km\lambda(n)+1} \underset{n}{\equiv} a$$

by the exponent cycle length property of λ. □

For example, consider the idempotent tuple $n = 1365, \bar{p} = 15, \bar{q} = 91$. Note that both $\bar{p}$ and $\bar{q}$ are composite. Possible (e, d) pairs include (13, 97), (19, 199), (71, 71), (17, 593), (11, 1031), (83, 167) and so forth. The reader may confirm that, for any such (e, d), $\forall a \in Z_{1365}, a^{ed} \underset{1365}{\equiv} a$.

9. Conclusions and Future Work

We conjecture that, for any square-free $\bar{p}$, a composite non-Carmichael $\bar{q}$ can be found such that $n = \bar{p}\bar{q}$ is an idempotent factorization. We have verified this conjecture for all square-free $\bar{p} < 2^{14}$. For certain $\bar{p} - 1$ prime, the resulting $\bar{q}$ can be quite large, requiring the use of heuristic algorithms for these cases. This is work in progress.

Rather than view idempotency as an all-or-nothing property of a bipartite factorization, it may be viewed as a ratio between 0 and 1. In that case, the previous definition of idempotent factorizations could be regarded as indicating *full* idempotency because all (e, d) pairs have the desired idempotency property. A value of 0 corresponds to *minimal idempotency*, in which no non-trivial (e, d) pairs are functional RSA keys. Values in between indicate the *idempotency ratio* for a given $n = \bar{p}\bar{q}$ factorization, based on the fraction of (e, d) pairs for which $a^{ed} \underset{n}{\equiv} a \ \forall a \in Z_n$.

The (e, d) pairs that lend idempotency to a factorization of $n = \bar{p}\bar{q}$ are exactly those for which $ed \underset{L}{\equiv} 1$, where $L = \text{lcm}((\bar{p} - 1)(\bar{q} - 1), \lambda(\bar{p}\bar{q}))$. The desired (e, d) are then exactly those solutions to the 2-variable system of nonlinear modular equations $ed \underset{m_1}{\equiv} 1, ed \underset{m_2}{\equiv} 1 ... ed \underset{m_j}{\equiv} 1$, where $m_1, m_2 ... m_j$ are the prime power factors of L. Determining whether or not such systems have solutions and calculating their exact number are known NP-complete problems. Thus, simple, efficient calculations of idempotency ratios are likely to prove elusive. This is work in progress.

We conjecture that, due to redundancy in the equations for idempotency, no non-maximally idempotent integer n can have exactly one of its factorizations be non-idempotent. No counterexamples below 2^{30} have been found. This suggests the question of the maximum number of idempotent factorizations an integer n with m prime factors can have without being maximally idempotent. Other questions include the asymptotic density of various kinds of idempotent factorizations, calculations of various idempotency ratios, the development of efficient algorithms to find idempotent factorizations, and more rigorous bounds on maximally idempotent integers.

Finding idempotent factorizations connects factoring, graph theory, number theory, complexity theory, and cryptography. They depend on the relationship of products of primes p_i and their immediate predecessors $a_i = p_i - 1$, so necessary and sufficient conditions for their existence beyond their defining equations are likely to prove elusive.

Various files related to idempotent factorizations are available at the Online Encyclopedia of Integer Sequences [7–10]. Some of these ideas first appeared in preliminary form in [11].

Acknowledgments: The author wishes to thank his department colleague Carlos Salazar for asking an interesting question, and for Karl Herzinger of the USAFA Department of Mathematics for his assistance and review of this article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystem. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Carmichael, R.D. Note on a New Number Theory Function. *Bull. Am. Math. Soc.* **1910**, *16*, 232–238. [CrossRef]
3. Huthnance, E.D.; Warndof, J. On Using Primes for Public Key Encryption Systems. *Appl. Math. Lett.* **1988**, *1*, 225–227. [CrossRef]
4. Pinch, R.G.E. On Using Carmichael Numbers for Public Key Encryption Systems. In Proceedings of the IMA International Conference on Cryptography and Coding, Cirencester, UK, 17–19 December 1997; pp. 265–269.
5. Fagin, B. Composite Numbers That Give Valid RSA Key Pairs For Any Coprime p. *Information* **2018**, *9*, 9. [CrossRef]
6. Pinch, R.G.E. The Carmichael Numbers up to 10^{21}. In Proceedings of the Conference on Algorithmic Number Theory, Turku, Finland, 8–11 May 2007; pp. 129–131.

7. Fagin, B.; OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. Squarefree n with ≥ 3 factors That Admit Idempotent Factorizations $n = \bar{p}\bar{q}$. Available online: http://oeis.org/A306330 (accessed on 4 July 2019).
8. Fagin, B.; OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. Squarefree n with Fully Composite Idempotent Factorizations. Available online: http://oeis.org/A306508 (accessed on 4 July 2019).
9. Fagin, B.; OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. Maximally Idempotent Integers with ≥ 3 Factors. Available online: http://oeis.org/A306812 (accessed on 4 July 2019).
10. Fagin, B.; OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. "Strong Impostors" ≠ 0 (mod 4). Available online: http://oeis.org/A318555 (accessed on 4 July 2019).
11. Fagin, B. Teaching RSA: What Happens When One of Your Primes Isn't? In Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19), Minneapolis, MN, USA, 27 February–2 March 2019; p. 1286.