Idempotent Integers: The complete class of numbers $n = \bar{p}\bar{q}$ that work correctly in RSA

A Mathematical Curiosity

Barry Fagin

Senior Associate Dean of the Faculty
Professor of Computer Science
United States Air Force Academy

2021 Conference on Geometry, Algebraic Number Theory and Applications

Take two positive numbers $\bar{p}, \bar{q}$.
Compute $n = \bar{p}\bar{q}$.
Pick e, d such that $ed \underset{(\bar{p}-1)(\bar{q}-1)}{\equiv} 1$.
What are the conditions on $\bar{p}, \bar{q}$ such that
$\forall a \in \mathbb{Z}_n, \forall e, d$ s.t. $ed \underset{(\bar{p}-1)(\bar{q}-1)}{\equiv} 1, a^{ed} \underset{n}{\equiv} a$?
In other words, what are the conditions on $\bar{p}, \bar{q}$ such that RSA works correctly?

Note: not asking about security.

70's: $\bar{p}, \bar{q}$ prime meets the conditions. If sufficiently large, system is believed to be secure due to computational intractability of factoring.

90's: Some Carmichael numbers C also can be factored into $\bar{p}, \bar{q}$ that meet the required conditions.

This work (since 2018) gives necessary and sufficient conditions, shows examples.

Cut to the chase

Answer is:

$\bar{p}, \bar{q}$ square free, $\gcd(\bar{p}, \bar{q}) = 1$ such that

$$(\bar{p} - 1)(\bar{q} - 1) \underset{\lambda(n)}{\equiv} 0$$

where λ denotes the Carmichael lambda function.

From n's point of view

Equivalently, a square-free n can be factored into $n = \bar{p}\bar{q}$ such that

$$(\bar{p} - 1)(\bar{q} - 1) \underset{\lambda(n)}{\equiv} 0$$

In that case, we say that n has an *idempotent* factorization, and that n is an idempotent integer.

The first 8 square-free n with $m \geq 3$ factors that admit idempotent factorizations are shown below:

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

Table: Values of n that admit idempotent factorizations

Idempotent factorizations where one of $\bar{p}, \bar{q}$ is prime and one is composite are *semi-composite*.

Idempotent factorizations where both are composite are *fully composite*.

The first 8 square-free n with $m \geq 3$ factors that admit fully composite factorizations are shown below:

n	$\bar{p}$	$\bar{q}$
210	10	21
462	22	21
570	10	57
1155	21	55
1302	6	217
1330	10	133
1365	15	91
1785	21	75

Table: Values of n that admit fully composite factorizations

Values of n exist with 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.

2730 = 2*3*5*7*13 is the smallest number with more than one fully composite idempotent factorization: 10*273 and 21*130.

max n	2^{12}	2^{15}	2^{18}	2^{21}	2^{24}	2^{27}	2^{30}
R_{sf}	.61	.37	.28	.21	.17	.13	.11
R_N	.09	.09	.08	.07	.06	.05	.04
R_{cpu}	-	2.7s	11.3	10.6	13.3	9.8	10.4

Proportion of integers with idempotent factorizations

# factors	0	1	2	3	4	5	6	7
3	184510285	34215577	0	15189	0	0	0	0
4	132479584	11347214	4448	15678	28	235	0	315
5	50515758	1733232	6530	13743	93	599	1	441
6	10004651	242377	6143	6906	167	586	12	302
7	931270	35473	2994	1597	124	286	22	102
8	29211	2956	477	158	39	43	5	6
9	99	28	7	2	1	0	1	1

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			

Factor distribution of idempotent factorizations $< 2^{30}, \geq 8$ factorizations

Idempotent factorizations of Carmichael numbers

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

$$(\bar{p} - 1)(\bar{q} - 1) \underset{\lambda(C)}{\equiv} 0$$

$$\iff (\bar{p}\bar{q} - 1) - \bar{p} - \bar{q} + 2 \underset{\lambda(C)}{\equiv} 0$$

$$\iff (C - 1) - \bar{p} - \bar{q} + 2 \underset{\lambda(C)}{\equiv} 0$$

$$\iff -\bar{p} - \bar{q} + 2 \underset{\lambda(C)}{\equiv} 0$$

$$\iff \bar{p} + \bar{q} \underset{\lambda(C)}{\equiv} 2$$

Curioser and curioser: Maximally Idempotent Integers

Consider an idempotent integer n with m factors.

Some such integers have the property that *all* their $(2^{m-1} - 1)$ factorizations are idempotent.

We call these integers *maximally idempotent*.

Examples of MI integers

3 factors	λ	4 factors	λ	5 factors	λ
273 = 3*7*13	12	63973 = 7*13*19*37	36	72719023 = 13*19*37*73*109	216
455 = 5*7 *13	12	137555 = 5*11*41*61	120	213224231 = 11*31*41*101*151	300
1729 = 7*13*19	36	145607 = 7*11*31*61	60		
2109 = 3*19*37	36	245791 = 7*13*37*73	72		
2255 = 5*11*41	40	356595 = 5*19*37*73	72		
2387 = 7*11*31	30	270413 = 11*13*31*61	60		
3367 = 7*13*37	36	536389 = 7*19*37*109	108		
3515 = 5*19*37	72	667147 = 13*19*37*73	72		
4433 = 11*13*31	60	996151 = 13*19*37*109	108		
4697 = 7*11*61	60	1007903 = 13*31*41*61	120		
4921 = 7*19*37	36	1847747 = 11*17*41*241	240		
5673 = 3*31*61	60	1965379 = 13*19*73*109	216		
6643 = 7*13*73	72	2060863 = 7*37*73*109	216		
6935 = 5*19*73	72	2395897 = 7*31*61*181	180		
7667 = 11*17*41	80	2778611 = 11*41*61*101	600		
8103 = 3*37*73	72	3140951 = 11*31*61*151	300		

Maximally idempotent integers with 3,4 and 5 factors

(Carmichael numbers underlined)

Stats $< 2^{30}$

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

The smallest and smallest known maximally idempotent integers with m factors for $3 \leq m \leq 9$ are shown below:

m	n	factorization
3	273	3*7*13
4	63973	7*13*19*37
5	72719023	13*19*37*73*109
6	13006678091	11*31*41*61*101*151
7	7817013532691	11*31*41*61*101*151*601
8	14611527595214719606286 11	31*211*421*631*2521*4201*6301*12601
9	35 digits	61*2021*3061*6121*8161*12241*24481*40801*122401

Smallest or smallest known (m=8,9) maximally idempotent integers with m factors

Maximally idempotent Carmichael numbers

What about the Carmichael numbers? It turns out they have maximally idempotent examples too. Of the Carmichael numbers below 10^{21}, there are 4765 maximally idempotent 3-Carmichaels, 99 MI 4-Carmichaels, and 7 MI 5-Carmichaels. Computer searches have discovered a total of 16 MI 5-Carmichaels, and two MI 6-Carmichaels. No examples with 7 or more factors are known.

Some examples of MI Carmichael numbers

Smallest with 5 factors:
C=661*991*3301*4951*9901, $\lambda = 9900$.

Smallest known with 6 factors:
C=2017*7057*12097*21169*42337*84673, $\lambda = 84762$

Above obtained by extending
C=2017*7057*12097*21169*42337, $\lambda = 84762$

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

Constructing large maximally idempotent integers with k-cliques

Random primes in modern cryptography are hundreds of bits long, found efficiently using probabilistic algorithms. Do similarly large MI integers exist, and if so can they be found? The answer is yes, and probabilistic techniques are not required. They can be constructed explicitly, of any size desired. Let's see how ...

Let $n = p_1 * p_2 ... * p_m$. Let $a_i = p_i - 1$. Not difficult to show that any idempotent factorization of n is a linear sum of terms made up of one or more products of the $a_i's$, a sum which must be $\underset{\lambda(n)}{\equiv} 0$. For example, if we require $(p_1p_2 - 1)(p_3p_4 - 1) \underset{\lambda(n)}{\equiv} 0$, that implies:

$$p_1p_2p_3p_4 - p_1p_2 - p_3p_4 + 1 \underset{\lambda(n)}{\equiv} 0$$

$$(a_1 + 1)(a_2 + 1)(a_3 + 1)(a_4 + 1) - (a_1 + 1)(a_2 + 1) - (a_3 + 1)(a_4 + 1) + 1 \underset{\lambda(n)}{\equiv} 0$$

which, while messy when expanded out, is clearly of the form required.

Recall $\lambda(n) = lcm(a_1, a_2 ... a_m)$. If we can find suitable set of a_i with $a_i + 1$ prime and with every $a_i a_j \underset{\lambda(n)}{\equiv} 0$, the product of the corresponding p_i will be maximally idempotent. Can construct such a set by identifying cliques in the *congruence graph* for a highly composite number L_0.

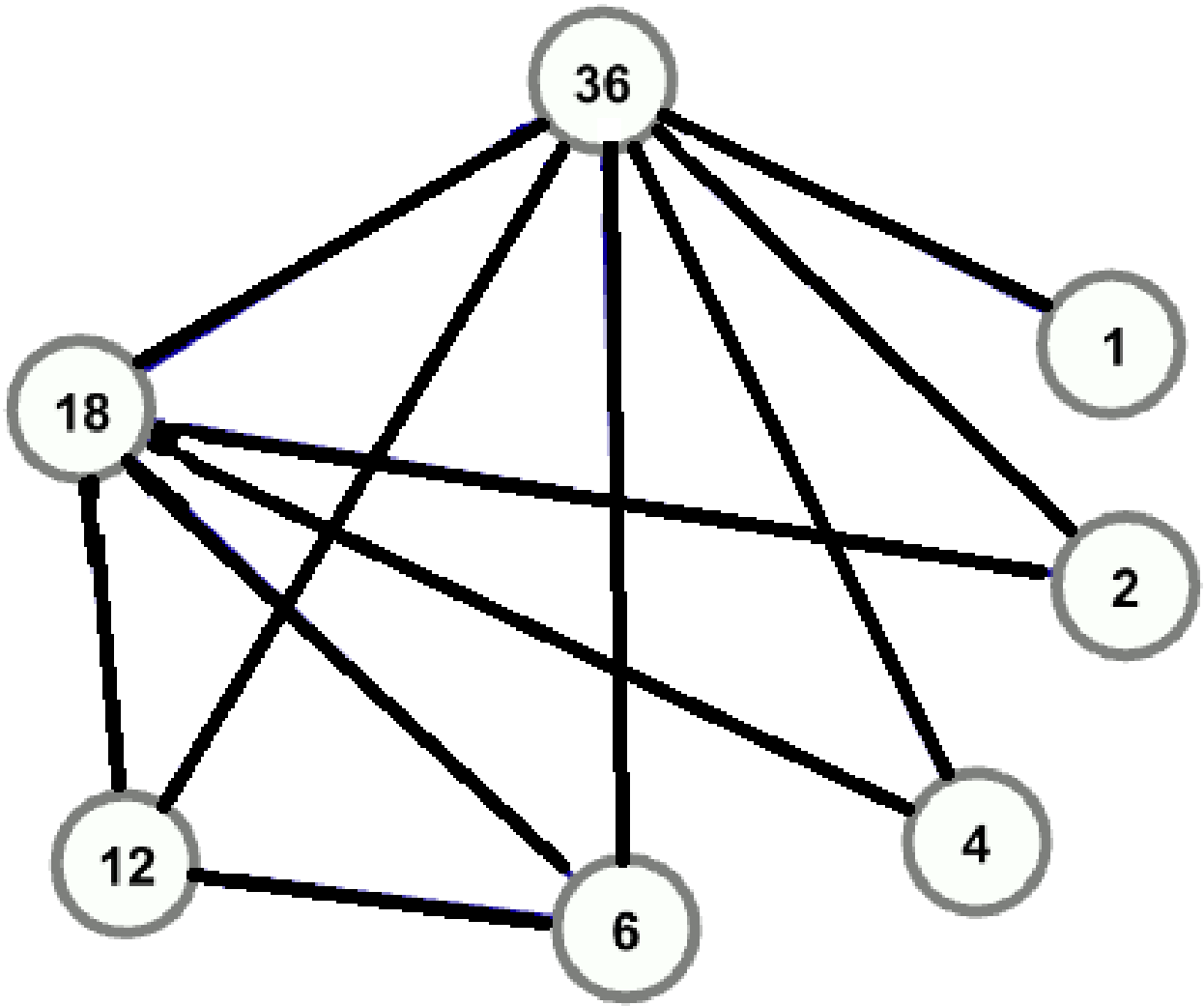
How it's done

1) Choose L_0 a highly composite number. 2) Make nodes in a graph corresponding to all divisors a_i of L_0 such that $a_i + 1$ is prime. 3) Connect all node pairs a_i, a_j such that $a_i a_j \underset{L_0}{\equiv} 0$. We call the resulting graph a congruence graph.

For any congruence graph, λ of any subset of its nodes is their lcm, which in turn must divide L_0. For all pairs of nodes in a k-clique, $a_i a_j$ is congruent to 0 mod L_0. Therefore all $a_i a_j$ are congruent to zero mod the lcm of any subset of divisors of L_0, including the members of the clique themselves.

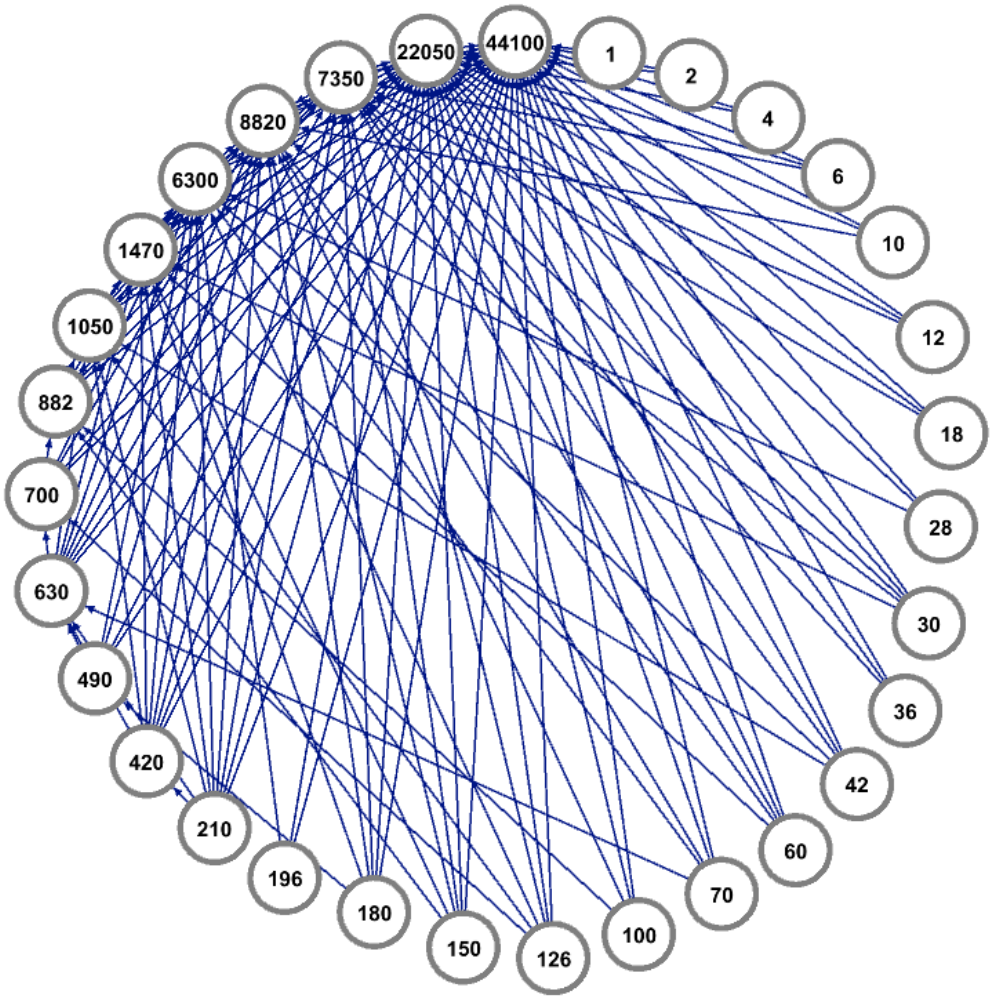
Thus every $a_i a_j \underset{\lambda}{\equiv} 0$, where λ is the lcm of every node in the clique. This means that every k-clique corresponds to a maximally idempotent integer with k factors. Similarly, any divisor of a maximally idempotent integer constructed in this way is also maximally idempotent. Thus a k-clique in a congruence graph contains $\binom{k}{m_i}$ maximally idempotent integers with $3 \leq m_i \leq k$ factors, for a total of $2^k - \binom{k}{2} - \binom{k}{1}$ (we ignore the primes and semiprimes).

Congruence graph for $L_0 = 36$



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 the previous table. The 4-clique is the smallest maximally idempotent integer with four factors, also shown in the previous table.

Congruence graph for $L_0 = 44100$



This is the congruence graph of the smallest L_0 that contains a 10-clique, corresponding to a maximally idempotent integer with 36 digits.

Congruence graph stats

k	L_0	divisors	nodes	edges	digits in max MI
3	$2^2 3$	6	5	6	3
4	$2^2 3^2$	9	7	11	5
5	$2^3 3^3$	16	9	15	9
6	$2^2 3^4 5$	30	17	58	16
7	$2^2 3^2 11^2$	27	15	46	21
8	$2^7 3^4$	40	20	71	25
9	$2^4 3^5 5$	60	30	149	32
10	$2^2 3^2 5^2 7^2$	81	31	129	36
11	$2^4 3^2 5^2 7^2$	135	53	311	45
12	$2^6 3^2 5^2$	126	51	381	58
13	$2^6 3^2 5^2 7^2$	1889	71	424	57
14	$2^8 3^5 5^2$	162	63	386	66
15	$2^6 3^3 5^2 7^2$	252	93	743	72
16	$2^7 3^3 5^2 7^2$	288	104	963	84
17	$2^2 3^2 5^2 7^2 11^2$	243	73	531	87
18	$2^8 3^3 5^2 7^2$	324	115	1203	99
19-22	$2^4 3^2 5^2 7^2 11^2$	405	125	1237	120
23-24	$2^6 3^2 5^2 7^2 11^2$	567	168	1866	143
25-26	$2^7 3^2 5^2 7^2 11^2$	648	195	2326	161
27-28	$2^4 3^4 5^2 7^2 11^2$	675	200	2976	181
29	$2^8 3^2 5^2 7^2 11^2$	729	215	2738	182
30-34	$2^6 3^4 5^2 7^2 11^2$	945	275	4657	232
35-39	$2^8 3^4 5^2 7^2 11^2$	1215	353	6374	272
40-41	$2^8 3^6 5^2 7^2 11^2$	1701	471	9453	315

Smallest L_0 where k-cliques first appear in congruence graph

Because I was bored

The largest k-clique currently constructed by the author has 141 nodes, corresponding to a maximally idempotent integer of 2081 digits. It contains approximately 10^{43} maximally idempotent integers as divisors.

Graph theory and number theory: Together again

Idempotent factorizations can also be constructed from a congruence graph. It can be shown that any complete (j, k) bipartite subgraph of a congruence subgraph corresponds to an idempotent factorization of an integer n with j and k factors respectively, where n is the product of the p_i's of the corresponding a_i's.

For example, the congruence graph for $L_0 = 36$ has a complete $(2, 2)$ bipartite subgraph on $(4, 6)$ and $(18, 36)$, corresponding to the idempotent partition $\bar{p} = 5 * 7, \bar{q} = 19 * 37$. n=5*7*19*37 is not maximally idempotent, but it does have the indicated fully composite idempotent factorization.

The Bottom Line

Complete subgraphs of congruence graphs correspond to maximally idempotent integers, while complete bipartite graphs correspond to idempotent integers. These are sufficient conditions for maximal idempotency, not necessary ones.

Another way to look at idempotency

Let $N = \bar{p}\bar{q}$. Let the *idempotency polynomial* $I_N(x)$ be given by

$$I_N(x) = x^2 - (N+1)x + N$$

ICBS $(N = \bar{p}\bar{q})$ is an idempotent factorization $\iff$ $(\bar{p}, \bar{q})$ are roots of $I_N(x) mod \lambda(N)$.

A Curious Conjecture

Consider the function D(x) defined by

$$D(x) = \frac{\lambda(x)}{gcd(\lambda(x), x-1)}$$

$D(x)$ is the product of all the factors of $\lambda(x)$ that are not in $x-1$, and is therefore the smallest number containing them. We have $1 \leq D(x) \leq \lambda(x)$.
$D(x) = 1 \iff$ x is prime or a Carmichael number,
$D(x) = \lambda(x) \iff gcd(\lambda(x), x-1)) = 1$.

A Curious Conjecture

Let $\bar{p}$ be square-free. Let q, $\bar{q}_c$, $\bar{q}$ be square-free and coprime to $\bar{p}$. ICBS:

a) If $\bar{p}$ is a prime or a Carmichael number, it is idempotent with and only with q prime, or $\bar{q}_c$ a Carmichael number, or $\bar{q}$ a composite non-Carmichael number with $\bar{p} \underset{D(\bar{q})}{\equiv} 1$. Since $D(6) = 2$, all primes $\bar{p} \geq 5$ and all Carmichael numbers are idempotent with $\bar{q} = 6$.

b) Otherwise $\bar{p}$ is idempotent with and only with $q \underset{D(\bar{p})}{\equiv} 1$ and either q prime, or $q = \bar{q}_c$ a Carmichael number, or $q = \bar{q}$ a composite non-Carmichael number such that $\bar{p} \underset{D(\bar{q})}{\equiv} 1$.

A Curious Conjecture

We call an idempotent factorization $n = \bar{p}\bar{q}$ *pure* if $\bar{p}$ and $\bar{q}$ are composite non-Carmichael numbers.

Curious Conjecture: For any composite square-free $\bar{p}$ there exists a $\bar{q}$ for which $\bar{p}\bar{q}$ is a pure idempotent factorization.

In other words, for any composite non-Carmichael $\bar{p}$, you can find a fully composite non-Carmichael $\bar{q}$ such that $(\bar{p}, \bar{q})$ will work with RSA.

It just might take a while ...

A Curious Conjecture

If $\bar{p} - 1$ is prime, the required $\bar{q}_{\text{¢}}$ must be very special indeed. It must be square-free, coprime to $\bar{p}$, and of the form $kD(\bar{p}) + 1$ as previously noted. (Note if $\bar{p} - 1$ is prime, $D(\bar{p}) = \lambda(\bar{p})$, its maximum value). Additionally, $\lambda(\bar{q}_{\text{¢}})$ must have exactly one prime factor not contained in $\bar{q}_{\text{¢}} - 1$, and that factor must be $\bar{p} - 1$.

A Curious Conjecture

Despite these constraints, we conjecture that such a $\bar{q}_{¢}$ always be found, and have verified this conjecture for all $\bar{p} < 2^{15}$. The upper limit is smaller than previous calculations because excluding Carmichael numbers can significantly increase the search time. For $\bar{p} = 7214, D(\bar{p}) = \lambda(\bar{p}) = 3606$, and almost 500 million candidates of the form $kD(\bar{p}) + 1$ must be examined until the required non-Carmichael $\bar{q}_{¢} = 1772915178061$ is found $(k = 491657010, \bar{q}_{¢} - 1 = 2^2 * 3^2 * 5 * 13 * 29^2 * 601 * 1499, \lambda(\bar{q}_{¢}) = 489474180 = 2^2 * 3^2 * 5 * 13 * 29 * 7213)$.

Some other CPU-intensive examples

$$\bar{p} = 32322, \bar{q} = 8,438,920,096,321$$
$$\bar{p} = 32610, \bar{q} = 2,461,654,462,177$$
$$\bar{p} = 30594, \bar{q} = 554,147,100,501,913$$

Is any of this actually useful?

Isn't this a pure math conference?

Mostly a mathematical curiosity. It does serve to remind cryptographers and cryptography teachers that requiring p,q to be prime is for security, not correctness.

Answered original question from cryptography classroom, explains a situation cryptography teachers might encounter.

Is any of this actually interesting?

Seems to lie at the intersection of hard problems in number theory and computer science. Solution to systems of modular equations. Graph theory. Relating factors of p and q ($\lambda(\bar{p}\bar{q})$) to factors of (p-1) and (q-1).

Shameless Self-Promotion

Some papers from 2018 on, just google me. Some sequences in OEIS.

Bibliography

Pinch's table of Carmichael numbers, "On Using Carmichael Numbers for Public Key Encryption Systems".

Rivest, Shamir and Adelman's original paper

Python's numbthy library, by Robert Campbell

See papers for more extensive set of citations.