P: ISSN No. 0976-8602 RNI No. UPENG/2012/42622 VOL.-9, ISSUE-4, October 2020

E: ISSN No. 2349-9443 Asian Resonance

Carmichael Numbers On Computer Security

Paper Submission: 10/10/2020, Date of Acceptance: 27/10/2020, Date of Publication: 28/10/2020

Uttam Kumar Shukla
Assistant Professor,
Dept. of Mathematics,
Madhupur College, SKMU Dumka
Madhupur, Jharkhand, India

Abstract

Carmicael numbers are very crucial type of fermat psedoprime numbers**.** Since they would pass fermat's primality test for any base a . Carmichael numbers define as composite numbers n such that $n \mid a^{n-1} - 1$ holds if gcd(*a,n*) = 1 . In this paper, We make here to give a new concept of carmichael numbers and RSA (Rivest-Shamir-Adleman) Code . It is an alyorithm used by modern computers to eneryt and decrypt message. It is an asymmetric cryptoyraphic algorithim and I also introduce how to RSA work on it**.** Some of the results on these developments concentrate on computational aspects of public- key Cryptography, Carmichael lambda function. Our work on primality will provide a new insight into fundamental research.

Keywords: Psedoprime, Fermat's Psedoprime, Absolutely Psedoprime, Poulet Number Euler Psedoprimes, Strong Psedoprimes, Super Psedoprime, RSA –Algorithm.

2010 Mathematics Subject Classification: 05A19, 11Y16, 11A51, 05A10

Introduction

Nowadays public-key cryptography enlisted great significance in everyday life, especially in the field of computer security. One of the most common public-key system is the RSA- algorithm, which is based on factorization of an integer into its prime factors. Therefore it is necessary to determine bigger and bigger prime to ensure that prime factorization of large integers in appropriate time. In order to seek for primes with ever increasing digits several tests were devised, Many of them are based on fermat's little theorem because of their efficiency. Carmichael numbers are very crucial type of Fermat pseudoprime numbers since they would pass Fermat's primality test for any base a .They also lead to other types of pseudoprimes, which are named after the corresponding tests Euler Psedoprimes, strong pseudoprimes and superpseudo primes.

The study of Carmichael numbers strike up in 1640, when Pierre de Fermat, in a letter to Bernard Frenicle, stated his now - "Little Theorem" became to famous: Fermat's Little Theorem. Let *p* be a prime and $a \in \mathbb{N}$. Then $P \mid a^p - a$**.** From this, mathematicians speculated as to whether the converse was also true, i.e if *p* divides $a^p - a$ for every natural number a then *p* is a prime. Of course , we know now that this assertion is incorrect , though it was not shown to be so until R.D. Carmichael computed the 1rst counterexamples in 1910 [1]. Counterexamples to this conjecture thus bear the name of Carmichael.

Objective of the Study

1. To introduce new concept of Carmichael number.
2. Carmichael number makes relationship with RSA (Rivest – Shamir – Adlemen) on public-key cryptography.

Review of the Literature

Various Subspecies of Pseudoprimes have been defined, such as "strong" and "Euler "pseudoprimes. They are even more sparse than ordinary pseuoprimes (which are some times called "Fermat pseudoprimes "by contrast) m there by providing an even batter primality test in particular, strong pseudoprimes correspond to the "Miller-Rabin test" see [5,9,10,11]. Chernick noted that if $p = 6m + 1$, $q = 12m + 1$ and $r = 18m + 1$ are all prime then pqr is a Carmichael number.

In 1993 Computations by Richard Pinch [12] have yielded 8,241 Carmichael number up to 10^{12}, 19,279 up to 10^{13} and 105,212 up to 10^{15}. [8] In other hand Alford, Granville and carl [1994] introduce there are infinitely many Carmichael numbers. [13] Yacobi O and Yacov Y, [2005] "A new related massage Attack on RSA "have show new attacks on RSA-encryption assuming know explicit linear relations between the messages.

[14] Romeo. M,[2013] " Generalization of Carmichael number -1 " He explained about Carmichael and its uses on fermat primality test and generalization of Riemann by pothesis innovatively.

Definition1.1

An integer $n > 1$ is called a Carmichael number if n is composite and $\gcd(a , n) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$ for all $a \in Z$.

Initially it is not at all clear that there should be any Carmichael numbers , but the first few were found by Robert Carmichael [1], [2] in the early 20th century and they are 561, 1105, 1729, 2465, 2821.

It is possible to verify that an integer n is a Carmichael number without using the
Dentition , so not having to check $a^{n-1} \equiv 1 \mod n$ for all a that are relatively prime to n.
For preference we can check a property of the prime factorization of n known as Korselt's criterion.

Carmichael number never reveals its compositeness under a Fermat test , unless a happens to be a divisor of N , a situation which can be avoided by 1rst testing whether
gcd (a,N) > 1. Although the Carmichael numbers are rather scarce , there do exist enough of them to create frustration when a number of Fermat tests all yield the result $a^{n-1} \equiv 1 \pmod{N}$.

Example 1.1

Show that 561 = 3.11.17 is a Carmichael number. First we note that
561 = 3.11.17 is composite. I want to show that for any a coprime to 561, $a^{561} \equiv 1 \pmod{561}$. To do so, suffices to show that
$a^{560} \equiv 1 \pmod{3}$;
$a^{560} \equiv 1 \pmod{11}$; and
$a^{560} \equiv 1 \pmod{17}$.
Now by Fermat's theorem, $a^2 \equiv 1 \pmod{3}$; $a^{10} \equiv 1 \pmod{11}$ and $a^{16} \equiv 1 \pmod{17}$ for every number a coprime to 3, 11, and 17. Since 560 is a multiple of 2, 10, and 16, it follows that each of the displayed congruences is true.

According to ([3], p.200) Euler's theorem is the key result behind the widely used RSA cryptosystem, developed by R.L. Rivest, A. Shamir, and L. Adleman (1977). Suppose two parties, call them Tom and shamir, wish to send messages back and forth to each other, and want them to be incomprehensible to a third party, say Eve. The idea is to encrypt each message, to transform the plaintext message into a message that would be unreadable except to the intended receiver. Even if the encrypted message is broadcast publicly, or sent over the internet, Eve, reading the encrypted message, should not be able to determine in a reasonable amount of time what the original message is. Any message in words can be translated into a sequence of numbers by replacing the letters of the message by numbers in some agreed-upon way. For example, we could count the alphabet and replace each letter by the corresponding two-digit number.

The 1rst characterization of Carmichael numbers has been done by A. Korselt in 1899[5].

Theorem 1.1

An odd composite number m is a Carmichael number iff m is square-free and $(p - 1)|(m -1)$ for every prime p dividing m.

Proof 1.1

Suppose m is square-free and p -1 divides m - 1 for all primes p dividing m. Let b be coprime to m. Then for all p dividing m , b is coprime to p, so $b^{m-1} \equiv 1 \pmod{p}$ by Fermat's theorem. Since p -1 divides m -1, $b^{m-1} \equiv 1 \pmod{p}$. Now since m is square-free, m is the least common multiple of the primes which divide m. So if $b^{m-1} \equiv 1 \pmod{p}$ for all p dividing m, then $b^{m-1} \equiv 1 \pmod{m}$. So m is Carmichael. Conversely, suppose m is Carmichael, and suppose p is any (odd) prime divisor of m. Let $m = p^e q$, where $\gcd(p , q) = 1$. Let b be a primitive root modulo p^e , and let a be a number such that
$a \equiv b \pmod{p^e}$
$a \equiv 1 \pmod{q}$
Then a is coprime to m. If m is Carmichael, then
$a^{m-1} \equiv 1 \pmod{m}$
so $a^{m-1} \equiv 1 \pmod{p^e}$

But the order of a modulo p^e is $p^e(p - 1)$. So $p^{e-1}(p - 1)$ divides m - 1, and hence p -1 divides m - 1 Also, if $e > 1$, then p divides m - 1. But since p divides m, p cannot divide m - 1. Thus $e = 1$. Since this is true for all primes p dividing m, therefore m must be square-free.

Carmichael numbers and RSA Codes

This subsection we follow solely ([3], p.426). In ([3], Chapter l0.A) resp. appendix C we examined the RSA cryptosystem, which encrypts a message word a by replacing a by $a^e \pmod{m}$ where the modulus m is the product of two large prime numbers p and q. To find a large prime p we could proceed as follows: first pick an interval of numbers of the desired size and sieve out all the composite numbers with small prime numbers as factors, as in ([3], Section 6.G). Then we use the a – pseudoprime test or the strong a- pseudoprime test to test the remaining unsieved numbers for primeness, as in ([3], Section 10.B).

Suppose, after sieving, we found a potential prime number q, and we used the a-pseudoprime test repeatedly, checking $a^{q-1} \equiv 1 \pmod{q}$ for a collection of numbers a. If q is prime, q will pass this test for any a. If q is composite and Carmichael, q will also pass this test for any a not relatively prime to q. If q is composite and not Carmichael, then the set of a (mod q) for which $a^{q-1} \equiv 1 \pmod{q}$ is a proper subgroup of the group of units of $\mathbb{Z}/_q\mathbb{Z}$, so the probability that q passes the a - pseudoprime test for a randomly selected number a is at most 1/2. For such numbers q, repeated testing with randomly chosen numbers a will almost surely reveal that q is composite.

Carmichael numbers are very much rarer than primes. So if we had a number q which passed repeated a-pseudoprime tests, it would be reasonable for us to assume that q is prime, not Carmichael. But suppose we were wrong? Suppose q were Carmichael? Suppose p and q are coprime Carmichael numbers. Let $m = pq$ and set up an RSA

code with modulus m. Believing that p and q are primes, we would assume that

$\varphi(m) = (p - 1)(q - 1)$. As in ([3], Section 10.A) , we would pick an encoding exponent e by choosing any number e coprime to (p-1)(q-1). We would find the decoding exponent via Bezout's identity: since {e , $(p - 1)(q - 1)$} = 1, there is some d; k so that $ed - k(p - 1)(q - 1) = 1$. Then for any integer a,

$a^{ed} = a^{1 + k(p-1)(q-1)}$

If p; q are primes, we know by Euler's Theorem that

$a^{1 + k(p-1)(q-1)} \equiv a \pmod{m}$:

But what happens if p and q are not primes, but are Carmichael numbers? Then the construction still works:

Theorem 2.1

If p and q are primes or Carmichael numbers, then for any $a < m$, $a^{1 + k(p-1)(q-1)} \equiv a \pmod{m}$.

Proof 2.1

First note that since p and q are each assumed to be either prime or Carmichael, each is square-free. Since p and q are coprime, it follows that m is square-free. Hence

$a^{1 + k(p-1)(q-1)} \equiv a \pmod{m}$

if

$a^{1 + k(p-1)(q-1)} \equiv a \pmod{c}$

Where c is any prime divisor of m. If c is a prime divisor of m, then c divides p or c divides q.

Suppose c divides p. If $c = p$, then $c - 1 = p - 1$; if p is Carmichael, $c - 1$ divides p-1 by Korselt's criterion. Now by Fermat's theorem, for any a coprime to c,

$a^{c-1} \equiv 1 \pmod{c}$,

so

$a^{h(c-1) + 1} \equiv a \pmod{c}$

For every h, and in particular if $h = k(q - 1)(p - 1) = (c - 1)$, an integer since $c - 1$ divides $p - 1$. But this last congruence is also true if a is divisible by c, and so it is true for every a. Thus for any prime c dividing m,

$a^{(p-1)(q-1) + 1} \equiv a \pmod{c}$:

Since m is square-free, it follows that

$a^{(p-1)(q-1) + 1} \equiv a \pmod{m}$:

for ever $a < m$, as we wished to show.

Hereby to set RSA codes, Carmichael numbers like as well as psedoprimes. Undoubtedly, if $C = ab$ is a product of Carmichael numbers then the prime factors of C will be much less than C, so it will be easy to find if a and b were psedoprime. So the security of the RSA code will be less than it would be if a and b are psedoprimes.

How RSA works 2.2

If Shamir wants to send a message to Tom, Shamir chooses two different large psedoprimes a and b that he keeps confidential, and sets $C = ab$. He selects an encrypting exponent e coprime to $\varphi(C) = (a - 1)(b - 1)$. Then shamir finds a number L so that

$eL \equiv 1 \pmod{\varphi(C)}$.

Then L is the inverse of e modulo $\varphi(C)$. Shamir can find L by solving the equation

$ex + \varphi(C)y = 1$

for x. Since e and $\varphi(C)$ are co prime, Shamir can solve this equation proficiently by the extended Euclidean Algorithm. Thus

$eL = 1 + \varphi(C)k$

for some k. Shamir keeps L confidential but broadcasts C and e to Tom. Tom has a message that consists of a sequence of numerical words. Each word is a number p that is smaller than C. To encrypt the word p, Tom computes

$m = p^e \pmod{C}$'

That is, Tom finds the number $m < C$ that is congruent to pe modulo C. He broadcasts the encrypted word m to Shamir. Shamir computes

$p^1 = m^L \pmod{C}$

Then p' will be the original word p of Tom. For since $eL \equiv 1 \pmod{\varphi(C)}$, we have

$p^1 \equiv m^L \equiv (p^e)^L = p^{1 + k\varphi(C)} \equiv p \pmod{C}$

for some integer k, Since both p and p^1 are numbers less than C, then $p = p^1$.

Carmichael lambda function and Euler totient function

Defnition 3.1

Let n be a positive integer. Then the Carmichael lambda function λ(n) is defined as follows:

λ (1) = 1 = φ (1);

λ (2) = 1 = φ (2);

λ (4) = 2 = φ (4);

$\lambda(2^k) = 2^{k-2} = \frac{1}{2}\varphi(2^k)$ for $k \geq 1$

$\lambda(p^k) = (p-1)p^{k-1} = \varphi(p^k)$ for any odd prime p and $k \geq 1$.

$\lambda(p_1^{k1} p_2^{k2} \ldots\ldots p_r^{kr}) = \text{lcm}(\lambda(p_1^{k1}), \lambda(p_2^{k2}), \ldots\ldots, \lambda(p_r^{kr}))$ where $p_1, p_2, p_3, \ldots\ldots p_r$ are distinct primes and $k_i \geq 1$ for $1 \leq i \leq r$.

([6], p.19) further introduces the Euler totient function. For every n € N the value φ (n) is defined as the number of all natural numbers not greater than n that are coprime to n, i.e., $\varphi(n) = |\{m \in \mathbb{N} : 1 \leq m \leq n, \gcd(m,n) = 1\}|$ where | . | denotes the number of elements. We can easily find that

φ (1) = 1 , φ (2) = 1 , φ (3) = 2 , φ (4) = 2 , φ (5) = 4 , φ (6) = 2 , φ (7) = 6 ……

And that all other values of φ are even. If p is prime, then clearly $\varphi(p) = p - 1$ and $\varphi(pk) = (p - 1)p^{k-1}$ for every $k \in \mathbb{N}$,

Another interesting property of the Euler totient function can be expressed as follows:

$\gcd(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$.

And let us recall Gauss's well-known formula $\Sigma\varphi(d) = N$ for all $N \in \mathbb{N}$.

Limitations

The method used to search for and count numbers of the form (8) depends almost entirely on sieving. An array of 32,000,000 bits represents values of q = 6m + 1 from

$m = m_0$ to $m = m_0 + 31, 999, 999$. For each “small” prime from 5 to an appropriate maximum, each q is marked as composite when divisible by a small prime (i.e., the bit is turned on). With a slight program addition it can be determined if r = 12m+1 or s = 18m+1 has a factor, and if it does then q is also marked as composite even though q itself might actually be prime. Typically, in the vicinity of $U_3 = 10^{41}$, about 18,000 numbers survive this sieving process which takes about 27 seconds on an Athlon/1.2 GHz computer. No additional tests are required since all

three components of ([8]) must be prime and therefore the survivors are Carmichael numbers of the required form. The only additional processing needed is to determine the sizes of all the survivors and to do appropriate bookkeeping which takes about 1 second.

Conclusion

In this paper, Thus consisted of a brief summary of what Carmichael number are and what are they used for .It also presented some well known algorithms . Our results extend from some recent works to the exact literature, generalization and integration.

References

1. *R. D. Carmichael, Note on a new number theory function, Bulletin of the American Mathematical Society, 16 (1910), 232-238.*
2. *R. D. Carmichael, On composite P which satisfy the Fermat congruence $a^{p-1} \equiv 1 \bmod P$, Amer. Math. Monthly 19 (1912), 22-27.*
3. *L. N. Childs, A Concrete Introduction to Higher Algebra, 3 ed., Undergraduate Texts in Mathematics, Springer Science+Business Media, Inc., 2009.*
4. *B. Fine and G. Rosenberger, Number Theory - An Introduction via the Distribution of Primes, Birkhäuser, Boston, 2007.*
5. *Richard Crandall and Carl Pomerance, Prime Numbers: A Computational Perspective, Springer (2001).*
6. *M. Krizek, F. Luca, and L. Somer, 17 Lectures on Fermat Numbers - From Number*
7. *Theory to Geometry, Springer Verlag, 2001.*
8. *H. Riesel, Prime Numbers and Computer Methods for Factorization, 2 ed., Progress*
9. *in Mathematics, vol. 126, Birkhäuser, Boston, 1994.*
10. *W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael*
11. *numbers, Ann. Math. 140 (1994), 703–722.*
12. *Kenneth H. Rosen, Elementary Number Theory and its Applications, Addison-Wesley (1988).*
13. *P. Ribenboim, The New Book of Prime Number Records, Springer (1995).*
14. *Neal Koblitz, A Course in Number Theory and Cryptography, Springer (1987).*
15. *R.G.E Pinch, "The Carmichael number up to10^{15} " , Math.comp 61(1993) , 381-391.*
16. *Oded Yacobi and Yacov Yacobi " Public Key Cryptography –PKC-2005, 8th International workshop on*
17. *Theory and Practice in PKC Les Diablerets, Switzerland January 23-26, 2005.*
18. *R. Mestrovic, "Generalazation of Carmichael Numbers. Ar XIV: 1305.1867 VI [Math.NT] May 2013.*