Chapter 6

On Primality and Pseudoprimes

6.1 Pseudoprimes to a Base.

Chinese Mathematicians (2500 years ago) make a claim: Integer $n > 1$ is prime iff $n|(2^n - 2)$.

It is true for all $n \in \mathbb{N}, n \leq 340$. There exists a composite integer n with $n|(2^n - 2)$ and hence converse of Fermat's little theorem is not true, given in the following example (6.1.1), by Pierre Frederic Sarrus in 1919 [58].

Example 6.1.1. Let $n = 341 = 11 \times 31$. By FLT we have $2^{10} \equiv 1(\text{mod } 11)$. Now $2^5 = 32 \equiv 1(\text{mod } 31) \Rightarrow 2^{10} \equiv 1(\text{mod } 31)$ by squaring. By result 1.2.1(vi), $2^{10} \equiv 1(\text{mod } 11 \times 31)$ i.e. $2^{10} \equiv 1(\text{mod } 341)$.

Thus $2^{341} = (2^{10})^{34} \times 2 \equiv 1^{34} \times 2 \equiv 2(\text{mod } 341)$, and 341 is composite.

Above such example lead to following definition.

Definition 6.1.1. *Let b be a nonzero integer. A composite number n such that $b^n \equiv b(mod\ n)$ is called a pseudoprime to the base b (or with respect to the base b.)*

If $\gcd(b, n) = 1$ then the congruence $b^n \equiv b(\text{mod n})$ is equivalent to the congruence $b^{n-1} \equiv 1(\text{mod n})$ [result 1.2.1(v)].

Pseudoprimes defined above are also called Fermat pseudoprimes.

Example 6.1.1 shows that 341 is a pseudoprime to the base 2.

This chapter is a reviewed based chapter [31],[58].

Result 6.1.1. [58] Any composite number is a pseudoprime to the base 1. Any odd composite number is a pseudoprime to both the bases 1 and -1.

If n is an odd pseudoprime to base b, then n is also pseudoprime to the bases -b and $n-$b, since $b^n \equiv b(\text{mod n}) \Rightarrow (-b)^n = -b^n \equiv -b(\text{mod n})$ and
$(n-b)^n \equiv (-b)^n \equiv -b \equiv (n-b)(\text{mod n})$.

Result 6.1.2. If n is a pseudoprime to the bases a and b, then $(ab)^n \equiv ab(\text{mod } n)$.

Proof. Here n is a composite number and $a^n \equiv a(\text{mod n})$, $b^n \equiv b(\text{mod n})$, which implies $(ab)^n = a^n b^n \equiv ab(\text{mod n})$ by result 1.2.1(iii). Hence n is a pseudoprime to the base ab. □

We generalize result (6.1.2):
(a) If n is a pseudoprime to the base a, then it is also a pseudoprime to the base a^k for any $k \in \mathbb{N}$.
(b) If n is a pseudoprime to bases $a_1, a_2, \cdots, a_k$, then it is also a pseudoprime to the base $a_1 a_2 \cdots a_k$.
It is possible that n is a pseudoprime to bases a and b but need not be a pseudoprime to base $a+b$. For example 341 is a pseudoprime to the bases 2 and 1.
Now $3^{10} \equiv 1(\text{mod } 11)$, $3^{30} \equiv 1(\text{mod } 31)$ by FLT.
$\Rightarrow 3^{30} \equiv 1(\text{mod } 11)$ and hence $3^{30} \equiv 1(\text{mod } 11 \times 31)$.
$\Rightarrow 3^{341} \equiv (3^{30})^{11} \times 3^{11} \equiv 1^{11} \times 3^{11} \equiv 3^{11} \equiv 168(\text{mod } 341)$
i.e. $3^{341} \not\equiv 3(\text{mod } 341)$ i.e. 341 is not a pseudoprime to the base 3.
Thus 341 is a pseudoprime to the bases 1, 2 but it is not a pseudoprime to the base $1+2$.
It is possible that n is a pseudoprime to the base ab but it is neither pseudoprime to the base a nor to the base b.
For example , 15 is a pseudoprime to the base $4(=2\times 2)$ but 15 is not a pseudoprime to the base 2.
$[4^2 = 16 \equiv 1(\text{mod } 15) \Rightarrow 4^{15} = (4^2)^7 \times 4 \equiv 4(\text{mod } 15)$ and $2^{15} = 4^7 \times 2 \equiv 8(\text{mod } 15)$
i.e. $2^{15} \not\equiv 2(\text{mod } 15)]$

Lemma 6.1.1 (Primality Test). *[58] If $n \in \mathbb{N}$ and a, b are integers such that $a^n \equiv a(mod\ n)$ and $b^n \not\equiv b(mod\ n)$, then n is a composite number.*

Moreover n is a pseudoprime to the base a but not a pseudoprime to the base b.
For example, $2^{341} \equiv 2(\text{mod } 341)$ and $7^{341} \not\equiv 7(\text{mod } 341)$.
$[7^3 = 343 \equiv 2(\text{mod } 341) \Rightarrow 7^{30} \equiv 2^{10} \equiv 1024 \equiv 1(\text{mod } 341)$ and
$7^{341} = (7^3)^{133} \times 7^2 \equiv 2^{113} \times 49 \equiv (2^{10})^{11} \times 2^3 \times 49 \equiv 1^{11} \times 392 \equiv 51(\text{mod } 341)$,
in particular $7^{341} \not\equiv 7(\text{mod } 341)]$.
So 341 is a pseudoprime to the base 2 but not a pseudoprime to the base 7.

Result 6.1.3. If n is a pseudoprime to the base a and not a pseudoprime to the base b where both nonzero integers a and b are relatively prime with n, then $(ab)^n \not\equiv ab(\text{mod n})$.

Proof. As $gcd(a, n) = gcd(b, n) = 1$ and n is a pseudoprime to the base a and not a pseudoprime to base b, we have $a^{n-1} \equiv 1(\text{mod n}), b^{n-1} \not\equiv 1(\text{mod n})$ and $gcd(ab, n) = 1$ $\Rightarrow (ab)^{n-1} = a^{n-1}.b^{n-1} \equiv b^{n-1}(\text{mod n})$ and so $(ab)^{n-1} \not\equiv 1(\text{mod n})$.
Hence n is not a pseudoprime to the base ab. □

Here restrictions $gcd(a, n) = gcd(b, n) = 1$ are essential.
For example, 15 is a pseudoprime to the base 5, not pseudoprime to the base 2 but 15 is a pseudoprime to the base $10(= 5 \times 2)$.
$5^3 \equiv 5(\text{mod } 15) \Rightarrow 5^5 = 5^3 \times 5^2 \equiv 5 \times 5^2 \equiv 5(\text{mod } 15)$ and so
$5^{15} = (5^5)^3 \equiv 5^3 \equiv 5(\text{mod } 15)$ and $2^{15} = (32)^3 \equiv 8(\text{mod } 15)$. And $10 = 5 \times 2$ with
$10^{15} \equiv (-5)^{15} \equiv -5^{15} \equiv -5 \equiv 10(\text{mod } 15)$.

Result 6.1.4. If $gcd(a, n) = 1$ and n is a pseudoprime to the base a, then n is a pseudoprime to the base $\bar{a}$, where $a\bar{a} \equiv 1(\text{mod n})$.

Here $a^{n-1}(\bar{a})^{n-1} = (a\bar{a})^{n-1} \equiv 1(\text{mod n})$ and $a^{n-1} \equiv 1(\text{mod n})$.
Therefore $(\bar{a})^{n-1} \equiv 1(\text{mod n})$ and result follows.

Example 6.1.2. 91 is a pseudoprime to the base 3 but not to the base 2.
Solution: $n = 91 = 7 \times 13$ is a composite number and by FLT, $3^6 \equiv 1(\text{mod } 7)$ and so $3^{12} \equiv 1(\text{mod } 7)$ and $3^{12} \equiv 1(\text{mod } 13)$

$\Rightarrow 3^{12} \equiv 1(\text{mod } 7 \times 13)$ i.e $3^{12} \equiv 1(\text{mod } 91)$ by result 1.2.1(vi).

Now $3^{91} = (3^{12})^7 \times 3^7 \equiv 1^7 \times 2187 \equiv 3(\text{mod } 91)$.

$\Rightarrow 91$ is a pseudoprime to the base 3.

Similarly we have $2^{12} \equiv 1(\text{mod } 91)$ and hence $2^{91} = (2^{12})^7 \times 2^7 \equiv 1^7 \times 128 \equiv 37(\text{mod } 91)$ and so $2^{91} \not\equiv 2(\text{mod } 91)$.

$\Rightarrow 91$ is not a pseudoprime to the base 2.

In general a number pseudoprime to an integer may not be a pseudoprime to some other integer.

Example 6.1.3. 45 is a pseudoprime to both the bases 17 and 19.

Note: For a pseudoprime n to the base a, if we consider $gcd(a, n) = 1$ then

(i) 341 is the smallest pseudoprime to the base 2;

(ii) 91 is the smallest pseudoprime to the base 3;

(iii) 217 is the smallest pseudoprime to the base 5.

It has been proved in 1903 [31] that there are infinitely many pseudoprimes to any given base.

Definition 6.1.2. *A pseudoprime to the base 2 is simply said to be a pseudoprime. Thus a composite number n is a pseudoprime if $n|(2^n - 2)$ i.e. $2^n \equiv 2(mod\ n)$.*

The first five pseudoprimes are 341, 561, 645, 1105, 161038 and first four are odd.

Verification: As $561 = 3 \times 11 \times 17$, so by FLT we have,

$2^2 \equiv 1(\text{mod } 3) \Rightarrow 2^{561} = (2^2)^{280} \times 2 = 1^{280} \times 2 \equiv 2(\text{mod } 3)$,

$2^{10} \equiv 1(\text{mod } 11) \Rightarrow 2^{561} = (2^{10})^{56} \times 2 \equiv 2(\text{mod } 11)$,

$2^{16} \equiv 1(\text{mod } 17) \Rightarrow 2^{561} = (2^{16})^{35} \times 2 \equiv 2(\text{mod } 17)$.

By result 1.2.1(vi), $2^{561} \equiv 2(\text{mod } 3 \times 11 \times 15)$ i.e. $2^{561} \equiv 2(\text{mod } 561)$.

Therefore 561 is a pseudoprime.

As $645 = 3 \times 5 \times 43$, so by FLT we have,

$2^2 \equiv 1(\text{mod } 3) \Rightarrow 2^{645} = (2^2)^{320} \times 2 \equiv 2(\text{mod } 3)$,

$2^4 \equiv 1(\text{mod } 5) \Rightarrow 2^{645} = (2^4)^{161} \times 2 \equiv 2(\text{mod } 5)$,

$2^{42} \equiv 1(\text{mod } 43) \Rightarrow 2^{645} = (2^{42})^{15} \times 2^{15} \equiv 2^{15} \equiv 32768 \equiv 2(\text{mod } 17)$.

$[32768 = 43 \times 762 + 2 \equiv 2(\text{mod } 43)]$

By result 1.2.1(vi), $2^{645} \equiv 2 \text{ mod } (3 \times 5 \times 43)$ i.e. $2^{645} \equiv 2(\text{mod } 645)$, showing 645 is a pseudoprime.

As $1105 = 5 \times 13 \times 17$, so by FLT we have,

$2^4 \equiv 1(\text{mod } 5) \Rightarrow 2^{1105} = (2^4)^{276} \times 2 \equiv 2(\text{mod } 5)$,

$2^{12} \equiv 1(\text{mod } 13) \Rightarrow 2^{1105} = (2^{12})^{92} \times 2 \equiv 2(\text{mod } 13)$,

$2^{16} \equiv 1(\text{mod } 17) \Rightarrow 2^{1105} = (2^{16})^{69} \times 2 \equiv 2(\text{mod } 17)$.

By result 1.2.1(vi), $2^{1105} \equiv 2(\text{mod } 1105)$ and hence 1105 is a pseudoprime.

As $161038 = 2 \times 73 \times 1103$, so by FLT we have,

$2^{72} \equiv 1(\text{mod } 73) \Rightarrow 2^{161038} = (2^{72})^{2236} \times 2^{46} \equiv 2^{46}(\text{mod } 73)$, and

$2^{1102} \equiv 1(\text{mod } 1103) \Rightarrow 2^{161038} = (2^{1102})^{146} \times 2^{146} \equiv 2^{146}(\text{mod } 1103)$,

Now $2^6 = 64 \equiv -9(\text{mod } 73) \Rightarrow 2^9 \equiv (-9) \times 8 \equiv -72 \equiv 1(\text{mod } 73)$ and hence

$2^{46} = (2^9)^5 \times 2 \equiv 1^5 \times 2 \equiv 2(\text{mod } 73)$. And $2^{16} = 65536 \equiv 459(\text{mod } 1103)$

$\Rightarrow 2^{48} = (2^{16})^3 \equiv 96702579 \equiv 363(\text{mod } 1103)$ and

$2^{144} = (2^{48})^3 \equiv (363)^3 \equiv 47832147 \equiv 552(\text{mod } 1103)$,

$2^{146} \equiv 2^{144} \times 2^2 \equiv 552 \times 4 \equiv 2208 \equiv 2(\text{mod } 1103)$.

Thus we have $2^{161038} \equiv 2^{46} \equiv 2(\text{mod} 73), 2^{161038} \equiv 2^{146} \equiv 2(\text{mod } 1103)$

and also we have $2^{161038} \equiv 2(\text{mod } 2)$.

Using result 1.2.1(vi), $2^{161038} \equiv 2(\text{mod } 2 \times 73 \times 1103)$ i.e. $2^{161038} \equiv 2(\text{mod } 161038)$.

Hence 161038 is a pseudoprime.

Note: [52] The smallest (first) even pseudoprime is 161038 was found in 1956 .

Pseudoprimes are much rarer than the primes. There are only 245 pseudoprimes and 78498 primes smaller than 10^6. There are only 14884 pseudoprimes and 455052512 primes less than 10^{10} . $561|(2^{561} - 2)$ and $561|(3^{561} - 3)$ i.e. 561 is a pseudoprime to the base 2 and 3. It is an unanswered question whether there exist infinitely many composite numbers n with the property that $n|(2^n - 2)$ and $n|(3^n - 3)$.

Lemma 6.1.2. *For distinct primes p and q with $a^p \equiv a(mod\ q)$ and $a^q \equiv a(mod\ p)$, pq is a pseudoprime to the base a .*

Proof. By FLT, $a^p \equiv a(\text{mod p})$ and as $a^q \equiv a(\text{mod p})$, we have

$a^{pq} \equiv (a^p)^q \equiv a^q \equiv a(\text{mod p})$. Similarly $a^{pq} \equiv a(\text{mod q})$. By result 1.2.1(vi),
$a^{pq} \equiv a(\text{mod pq})$, i.e. pq is a pseudoprime to the base a . □

If p, q, r are distinct primes with $a^{pq} \equiv a(\text{mod r}), a^{qr} \equiv a(\text{mod p})$ and $a^{pr} \equiv a(\text{mod q})$, then
$a^{pqr} \equiv a(\text{mod } pqr)$. Here $(a^{pq})^r \equiv a^r(\text{mod r}) \equiv a(\text{mod r})$ by FLT. Similarly
$a^{pqr} \equiv a(\text{mod } p)$ and $a^{pqr} \equiv a(\text{mod } q)$. As p, q, r are distinct primes, $a^{pqr} \equiv a(\text{mod } pqr)$ and so pqr is a pseudoprime to the base a.
Generalisation: If $p_1, p_2, \cdots, p_k$ are distinct primes ($k \geq 2$) and $a \in \mathbb{Z}$ with $a^{q_i} \equiv a(\text{mod } p_i)$ where $q_i = \dfrac{p_1 p_2 \cdots p_k}{p_i} \quad \forall i$, then $p_1 p_2 \cdots p_k$ is a pseudoprime to the base a.

Lemma 6.1.3. *Every composite (Fermat) number $F_m = 2^{2^m} + 1$ is a pseudoprime.*

Proof. $F_m = 2^{2^m} + 1$ is an odd composite number and $2^{2^m} \equiv -1(\text{mod } F_m)$.
Raising power $2^{2^m - m}$, we get $(2^{2^m})^{2^{2^m \times 2^{-m}}} \equiv 1(\text{mod } F_m)$ i.e. $2^{2^{2^m}} \equiv 1(\text{mod } F_m)$
$2^{F_m - 1} \equiv 1(\text{mod } F_m)$ i.e. $2^{F_m} \equiv 2(\text{mod } F_m)$
Hence F_m is a pseudoprime. □

Thus every Fermat number is a prime or pseudoprime [9].

Lemma 6.1.4. *Let $m|n$ where m and n be positive integers. Then $(2^m - 1)|(2^n - 1)$. In general for an integer $a > 1, (a^m - 1)|(a^n - 1)$.*

Proof. As $m|n$, we have $n = km$ for some $k \in \mathbb{N}$ and
$2^n - 1 = 2^{km} - 1 = (2^m - 1)(2^{m(k-1)} + 2^{m(k-2)} + \cdots + 2^m + 1)$
Therefore $(2^m - 1)|(2^n - 1)$. □

Lemma 6.1.5. *Let n be an odd pseudoprime. Then Mersenne number $M = 2^n - 1$ is also an odd pseudoprime.*

Proof. Let n be an odd pseudoprime. Then $n = cd$ is a composite number where $c, d \in \mathbb{N}$ with $1 < c, d < n$ and $2^{n-1} \equiv 1(\text{mod n})$ i.e. $2^n \equiv 2(\text{mod n})$.
By lemma 6.1.4, $c|n \Rightarrow (2^c - 1)|(2^n - 1)$ with $1 < 2^c - 1 < 2^n - 1$,
so $M = 2^n - 1$ is a composite number.

Now $n|(2^n-2)$, so $2^n-2=kn$ for some $k\in\mathbb{N}$,

i.e. $M-1=kn$. Then $2^{M-1}-1=2^{kn}-1$.

Again by lemma 6.1.4, $M=(2^n-1)|(2^{kn}-1)$

i.e. $M|(2^{M-1}-1)\Rightarrow 2^{M-1}\equiv 1(\text{mod M})$,

i.e. $2^M\equiv 2(\text{mod M})$.

Thus, if n is an odd pseudoprime, then $M=2^n-1$ is an odd pseudoprime (larger than n). □

Note: If we take n as even pseudoprime in lemma 6.1.5, then we get $M=2^n-1$ as an odd pseudoprime.

Theorem 6.1.1. *[58] There are infinitely many pseudoprimes.*

Proof. $n_0=341$ is an odd pseudoprime. By lemma 6.1.5, $n_1=2^{n_0}-1$ is also an odd pseudoprime and $n_0<n_1$. [$n_1=2^{341}-1$ is an integer with more than 100 decimal digits !]

Define $n_{i+1}=2^{n_i}-1$ for $i=0,1,2,3,\cdots$. Then we have infinitely many odd pseudoprimes $n_0,n_1,n_2,n_3,\cdots$ with $n_0<n_1<n_2<n_3<\cdots$.

Thus there is an infinite number of (odd) pseudoprimes. □

Remark 6.1.1. The following two questions about pseudoprimes remain unsolved:

(A) Are there infinitely many square pseudoprimes ?

(B) Are there infinitely many primes p such that $2^{p-1}\equiv 1(\text{mod } p^2)$?

Note that $2^{p-1}\equiv 1(\text{mod } p^2)$ is equivalent to $2^{p^2}\equiv 2(\text{mod } p^2)$.

$2^{p^2}\equiv 2(\text{mod } p^2)$ and p is odd prime , hence we have

$$2^{p^2-1}\equiv 1(\text{mod } p^2) \tag{6.1.1}$$

Let $\bar{2}\in U(p^2)$ is inverse of $2\in U(p^2)$ i.e.

$$2(\bar{2})\equiv 1(\text{mod } p^2) \tag{6.1.2}$$

$$(\bar{2})^{p^2-p}\equiv 1(\text{mod } p^2)\quad \text{since } |U(p^2)|=p^2-p \tag{6.1.3}$$

By equations (6.1.1) and (6.1.3), we have
$2^{p-1}(2 \times \bar{2})^{p^2-p} \equiv 1(\text{mod } p^2)$ i.e. $2^{p-1} \equiv 1(\text{mod } p^2)$.
The smallest pseudoprimes that are not square free are $1194649 = 1093^2$;
$12327121 = 3511^2$ and $3914864773 = 29 \times 113 \times 1093^2$.

Theorem 6.1.2. *[31] There is an infinity of pseudoprimes with respect to every base* $a > 1$.

Proof. Let p be any odd prime which does not divide $a(a^2-1)$ where integer $a > 1$.
Then $p \nmid a$ and $p \nmid (a^2-1)$.
Take $n = \dfrac{a^{2p}-1}{a^2-1} = (\dfrac{a^p-1}{a-1})(\dfrac{a^p+1}{a+1})$.
Then n is a composite number and by FLT, $a^{p-1} \equiv 1(\text{mod p})$ i.e. $p|(a^{p-1}-1)$.
Now $n-1 = \dfrac{a^{2p}-a^2}{a^2-1} \Rightarrow (n-1)(a^2-1) = a(a^{p-1}-1)(a^p+a)$ is divisible by p.
As $p \nmid (a^2-1)$, by Euclid's lemma , $p|(n-1)$.
Also $n = \underbrace{a^{2(p-1)} + a^{2(p-2)} + \cdots + a^2}_{\text{(p - 1 (even) terms)}} + 1$ is odd, i.e. $2|(n-1)$.
Hence $2p|(n-1)$ i.e. $n = 1 + 2kp$ for some $k \in \mathbb{N}$ and $a^{2p} = 1 + (a^2-1)n \equiv 1(\text{mod n})$ (by definition of n.)
$\Rightarrow (a^{2p})^k \equiv 1(\text{mod n})$ i.e. $a^{n-1} \equiv 1(\text{mod n}) \quad [\because n = 1 + 2kp]$.
Therefore n is a pseudoprime to the base a . As n has different values for different odd prime p, with $p \nmid a(a^2-1)$, we have infinitely many pseudoprimes to the base a . □

6.2 Absolute Pseudoprimes (Carmichael Numbers).

If n is a positive integer and $a, b \in \mathbb{Z}$ with $\gcd(a,n) = \gcd(b,n) = 1$ such that $a^{n-1} \equiv 1(\text{mod n}), b^{n-1} \not\equiv 1(\text{mod n})$ then n is a composite number. There are numbers n that cannot be shown composite using above approach, that is there are pseudoprimes n to every base: $b^{n-1} \equiv 1(\text{mod n})$ for all $b \in \mathbb{Z}$ with $\gcd(b,n) = 1$. This leads to the following definition.

Definition 6.2.1. *A composite integer n that satisfies* $a^{n-1} \equiv 1(mod\ n)$ *for all positive integers a with* $gcd(a,n) = 1$ *is called an absolute pseudoprime or a Carmichael*

number [23], [36] (Robert D. Camichael (1907-1912), studied them) .

Example 6.2.1. Consider $561 = 3 \times 11 \times 17$. For any $a \in \mathbb{Z}$ with $\gcd(a, 561) = 1$, we have $\gcd(a, 3) = 1 = \gcd(a, 11)$ =$\gcd(a, 17)$ and by FLT, So that
$a^2 \equiv 1(\text{mod } 3), a^{10} \equiv 1(\text{mod } 11), a^{16} \equiv 1(\text{mod } 17)$
$\Rightarrow a^{560} = (a^2)^{280} \equiv 1(\text{mod } 3), a^{560=(a^{10})^{56}} \equiv 1(\text{mod } 11), a^{560=(a^16)^{35}} \equiv 1(\text{mod } 17)$
$\Rightarrow a^{560} \equiv 1(\text{mod } 3 \times 11 \times 17)$
i.e. $a^{560} \equiv 1(\text{mod } 561)$ by result 1.2.1(vi) for all $a \in \mathbb{N}$ with $\gcd(a, 561) = 1$.

Note:[58] 561 is the smallest Carmichael number. The next two are $1105 = 5 \times 13 \times 17$ and $1729 = 7 \times 13 \times 19$. R. D. Carmichael was the first to notice existence of absolute pseudoprimes. In his first paper on the subject published in 1910, Camichael indicated four absolute pseudoprimes including the well known $561 = 3 \times 11 \times 17$, others are $1105 = 5 \times 13 \times 17, 2821 = 7 \times 13 \times 31$ and $15841 = 7 \times 31 \times 73$.
Two years later he published 11 more having three prime factors and discovered one absolute pseudoprime with four factors specifically $16046641 = 13 \times 37 \times 73 \times 457$. The largest number of this kind known to date is the product of 1101518 distinct odd primes. It has 16142049 digits. There are six Carmichael numbers 561, 1105, 1729, 2465, 2821, 6601 less than 10000. There are just 43 Carmichael numbers less than 10^6 and 1547 less than 10^{10}. There are 2163 Carmichael numbers below 25×10^9.In 1992, using high powered computers, Richard G. E. Pinch at Cambridge University found that there are 105212 absolute pseudoprimes less than 10^{15}. And search continues.
In 1912, Carmichael made a conjecture that Carmichael numbers are infinte in numbers. After 80 years i.e. in 1992 [1], Andrew Granville, Carl Pomerance and Red Alford of the University of Georgia established the existence of infinitely many Carmichael numbers [1]. In particular, they showed that C(x), the number of Carmichael not exceeding x, satisfies the inequality $C(x) > x^{\frac{2}{7}}$ for sufficiently large numbers x. Erdos has made the stronger conjecture that for any $\epsilon > 0$, there exists a number $x_0(\epsilon)$ such that $C(x) > x^{1-\epsilon}$ for all $x \geq x_0(\epsilon)$.

Remark 6.2.1. It can happen that one Carmichael number is a factor of another, for example, $1729, 63973 = 7 \times 13 \times 19 \times 37$ are Carmichael numers with $1729|63973$.

It is established in 1948 that the product of two Carmichael numbers can also be a Carmichael number, for example, $1729,294409 = 37 \times 73 \times 109$ and $509003161 = 1729 \times 294409$ are Carmichael numbers [22].

In 1990, H. Duhner and H. Nelson discovered two Carmichael numbers that are products of three Carmichael numbers; one contains 97 digits and other contains 124 digits.

Example 6.2.2. Each of the following is a Carmichael number

(a) $1105 = 5 \times 13 \times 17$ (b) $1729 = 7 \times 13 \times 19$

(c) $2465 = 5 \times 17 \times 29$ (d) $2821 = 7 \times 13 \times 31$

Solution: (a) Consider any $a \in \mathbb{Z}$ with $\gcd(a, 1105) = 1$.

Then $\gcd(a, 5) = 1 = \gcd(a, 13) = \gcd(a, 17)$ and by FLT,

$a^4 = 1 (\text{mod } 5)$, $a^{12} = 1 (\text{mod } 13)$, $a^{16} = 1 (\text{mod } 17)$

$\Rightarrow a^{1104} = (a^4)^{276} \equiv 1 (\text{mod } 5)$, $a^{1104} = (a^{12})^{92} \equiv 1 (\text{mod } 13)$, and

$a^{1104} = (a^{16})^{69} \equiv 1 (\text{mod } 17)$,

result 1.2.1(vi) $\Rightarrow a^{1104} \equiv 1 (\text{mod } 5 \times 13 \times 17)$ i.e. $a^{1104} \equiv 1 (\text{mod } 1105)$

Hence 1105 is a Carmichael number.

(b) Consider any $a \in \mathbb{Z}$ with $\gcd(a, 1729) = 1$.

Then $\gcd(a, 7) = 1 = \gcd(a, 13) = \gcd(a, 19)$ and by FLT,

$a^6 = 1 (\text{mod } 7)$, $a^{12} = 1 (\text{mod } 13)$, $a^{18} = 1 (\text{mod } 19)$

$\Rightarrow a^{1728} = (a^6)^{288} \equiv 1 (\text{mod } 7)$, $a^{1728} = (a^{12})^{144} \equiv 1 (\text{mod } 13)$, and

$a^{1728} = (a^{18})^{96} \equiv 1 (\text{mod } 19)$,

result 1.2.1(vi) $\Rightarrow a^{1728} \equiv 1 (\text{mod } 7 \times 13 \times 19)$ i.e. $a^{1728} \equiv 1 (\text{mod } 1729)$

Hence 1729 is a Carmichael number.

(c) Consider any $a \in \mathbb{Z}$ with $\gcd(a, 2465) = 1$.

Then $\gcd(a, 5) = 1 = \gcd(a, 17) = \gcd(a, 29)$ and by FLT,

$a^4 = 1 (\text{mod } 5)$, $a^{16} = 1 (\text{mod } 17)$, $a^{28} = 1 (\text{mod } 29)$

$\Rightarrow a^{2464} = (a^4)^{616} \equiv 1 (\text{mod } 5)$, $a^{2464} = (a^{16})^{154} \equiv 1 (\text{mod } 17)$, and

$a^{2464} = (a^{28})^{88} \equiv 1 (\text{mod } 29)$,

result 1.2.1(vi) $\Rightarrow a^{2464} \equiv 1 (\text{mod } 5 \times 17 \times 29)$ i.e. $a^{2464} \equiv 1 (\text{mod } 2465)$

Hence 2465 is a Carmichael number.

Theorem 6.2.1. *[58] Any absolute pseudoprime is squarefree.*

Proof. Let n be an absolute pseudoprime.
Suppose n is not square free. Then there is an integer $k > 1$ such that $k^2|n$. As n is an absolute pseudoprime, so $k^n \equiv k(\text{mod n})$ and hence $k^n \equiv k(\text{mod } k^2)$ since $k^2|n$. Then $k \equiv 0(\text{mod } k^2)$, since $k^2|k^n$ i.e. $k^2|k$, a contradiction. So the supposition 'n is not square free' is wrong. □

Converse of theorem 6.2.1 is not true, for example $341 = 11 \times 31$ is a squrefree, it is pseudoprime to the base 2 but not to the base 7, i.e. 341 is not absolutely pseudoprime . $91 = 7 \times 13$ is not absolute pseudoprime since it is not pseudoprime to the base 2.

Theorem 6.2.2 (Theorem to find Carmichael Numbers)**.** *[58] Let $n = p_1p_2 \cdots, p_r$ be a square free composite integer with distinct primes p_i . If $(p_i - 1)$ divies $(n - 1)$ for $i = 1, 2, \cdots, r$, then n is an absolute pseudoprime.*

Proof. Let $n = p_1p_2 \cdots p_r$ be a composite square free integer where $p_1, p_2, \cdots, p_r$ are distinct primes and $(p_i - 1)\big|(n - 1)$ for $i = 1, 2, \cdots, r$.
Consider any $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then $\gcd(a, p_i) = 1$ for $i = 1, 2, \cdots, r$ and by FLT, $a^{p_i-1} \equiv 1(\text{mod } p_i)$ i.e. $p_i|(a^{p_i-1} - 1.)$ Now

$$(p_i - 1)|(n - 1) \Rightarrow (a^{p_i-1} - 1)|(a^{n-1} - 1) \tag{6.2.1}$$

Since $\gcd(a, n) = 1$ and by equation (6.2.1), we have $p_i|(a^{n-1} - 1)$ and hence
$p_i|(a^n - a)$ for $i = 1, 2, \cdots, r$.
As $\gcd(p_i, p_j) = 1$ for $i \neq j$, so by result 1.2.1 (vi), $p_1p_2 \cdots p_r|(a^n - a)$ i.e.

$$n|(a^n - a) \quad \forall a \in \mathbb{Z} \tag{6.2.2}$$

$\Rightarrow n$ is an absolute pseudoprime. □

Note: (a) The converse of theorem 6.2.2 is also true, that is all Carmichael numbers are of the form $p_1p_2 \cdots p_r$ where the p_j are distinct primes and $(p_j - 1)|(n - 1)$ for all j.

(b) **Justification of equation** (6.2.2)**:** If $n|a$ or $\gcd(a,n)=1$, then equation (6.2.2) is clear.

Let us consider $a \in \mathbb{Z}, n = p_1p_2\cdots p_r$, with $n \nmid a$ and $\gcd(a,n) > 1$ and $\gcd(a,n) = p_1p_2\cdots p_j$ and $\gcd(a, p_{j+1}p_{j+2}\cdots p_r) = 1$. Now

$$p_1p_2\cdots p_j|a \Rightarrow p_1p_2\cdots p_j|(a^n - a) \tag{6.2.3}$$

As $\gcd(a, p_{j+1}p_{j+2}\cdots p_n) = 1$ and $(p_i - 1)|(n-1)$ we have $p_i|(a^{p_i-1} - 1)$ and $(a^{p_i-1} - 1)|(a^{n-1} - 1)$ since p_i are primes for $i = j+1, j+2, \cdots, r$

$\Rightarrow p_i|(a^{n-1} - 1)$ for all $i = j+1, j+2, \cdots, r$

$p_{j+1}p_{j+2}\cdots p_r|(a^{n-1} - 1)$ by result 1.2.1(vi) and hence

$$p_{j+1}p_{j+2}\cdots p_r|(a^n - a) \tag{6.2.4}$$

By equations (6.2.3) and (6.2.4), $n = p_1p_2\cdots p_r|(a^n - a)$ for all $a \in \mathbb{Z}$ and equation (6.2.2) holds for all $a \in \mathbb{Z}$

(c) Examples of integers that satify the conditions of theorem are $1729 = 7\times13\times19$, $6601 = 7\times23\times41, 10585 = 5\times28\times73$.

$n = 6601 = 7\times23\times41$ is product of three distinct primes and $n-1 = 6600$. Here $6 = (7-1)|6600, 22 = (23-1)|6600, 40 = (41-1)|6600$. Hence 6601 is absolute pseudoprime.

Example 6.2.3. Following integers are Carmichael numbers.

(a) $2821 = 7\times13\times31$ (b) $10585 = 5\times29\times73$ (c) $29341 = 13\times37\times61$

(d) $314821 = 13\times61\times397$ (e) $278545 = 5\times17\times29\times113$

(f) $172081 = 7\times13\times31\times61$ (g) $564651361 = 43\times3361\times3907$

Using theorem 6.2.2 results follows.

Example 6.2.4. Carmichael number of the form $7\times23\times q$ where q is an odd prime.

Solution: Assume $c = 7\times23\times q$ with q an odd prime, is a Carmichael number. Then by theorem 6.2.2, $(7-1)|(c-1), (23-1)|(c-1)$ and $(q-1)|(c-1)$.

$6|(c-1) \Rightarrow c = 7 \times 23 \times q \equiv 1(\text{mod } 6) \Rightarrow 1 \times (-1) \times q \equiv 1(\text{mod } 6)$, since

$$7 \equiv 1(\text{mod } 6), 23 \equiv -1(\text{mod } 6) \Rightarrow q \equiv 5(\text{mod } 6) \tag{6.2.5}$$

Now $22|(c-1)$ gives $c = 7 \times 23 \times q \equiv 1(\text{mod } 22)$
$\Rightarrow 7 \times 1 \times q \equiv 1(\text{mod } 22)$ since $23 \equiv 1(\text{mod } 23)$
$(19 \times 7)q \equiv 19(\text{mod } 22)$ i.e. $133q \equiv 19(\text{mod } 22)$

$$\Rightarrow q \equiv 19(\text{mod } 22) \text{ since } \quad 133 \equiv 1(\text{mod } 22) \tag{6.2.6}$$

Applying Chinese remainder theorem to equations (6.2.5) and (6.2.6), we obtain $q \equiv 41(\text{mod } 66)$, i.e.

$$q = 41 + 66k \quad \text{for some integer } k \geq 0 \tag{6.2.7}$$

Now $(q-1)|(c-1)$ gives $(40+66k)|(7 \times 23 \times [41+66k]-1)$

$$\begin{aligned} \Rightarrow m(40+66k) &= 6600 + 10626k \quad \text{for some } m \in \mathbb{N} \\ &= 160 + 6440 + 10626k \\ &= 160 + 161(40+66k) \end{aligned}$$

$\Rightarrow 160$ must be multiple of $40+66k \quad \Rightarrow k = 0$ only.
Then $q = 41$ only (by equation (6.2.7)) prime and the Carmichael number is $7 \times 23 \times 41 = 6601$.

Example 6.2.5. (a) Every integer of the form $(6t+1)(12t+1)(18t+1)$ where t is a positive integer with $6t+1, 12t+1, 18t+1$ are all primes, is a Carmichael number.
(b) Each of the numbers $1729 = 7 \times 13 \times 19; 294409 = 37 \times 78 \times 109;$
$56052361 = 211 \times 421 \times 631; 118901521 = 271 \times 541 \times 811$ and $172947529 = 307 \times 613 \times 919$ are Carmichael numbers (using part (a)).
Solution: (a) $n = (6t+1)(12t+1)(18t+1)$, product of three primes ($t \in \mathbb{N}$ etc.)
$\Rightarrow n - 1 = 6 \times 12 \times 18t^3 + (6 \times 12 + 6 \times 18 + 12 \times 18)t^2 + (6+12+18)t$ is divisible by all $6t, 12t, 18t$. Hence n is a Carmichael number.

(b) For $t = 1, 6t + 1 = 7, 12t + 1 = 13, 18t + 1 = 19$ are primes. Hence by part (a), $(6t + 1)(12t + 1)(18t + 1) = 7 \times 13 \times 19 = 1729$ is a Carmichael number.
For $t = 35; (6t + 1)(12t + 1)(18t + 1) = 321197185$ is a Carmichael number etc.

Example 6.2.6. The smallest Carmichael number with six prime factors is
$5 \times 19 \times 23 \times 29 \times 37 \times 137 = 321197185$.
We will verify that this number is a Carmichael number.
Solution: We have $321197185-1 = 321197184 = 4\times80\times299\times296 = 18\times17844288 = 22 \times 14599872 = 28 \times 11471328 = 36 \times 8922144 = 136 \times 2361744$.
So $(p - 1)|(321197185 - 1)$ for every prime p which divides 321197185.
Therefore, by theorem 6.2.2, 321197185 is a Carmichael number.

Remark 6.2.2. (i) Any Carmichael number n must be odd, since it has odd prime factor p such that $(p - 1)|(n - 1)$ i.e. $n - 1$ is even.
(ii) A Carmichael number must have more than two prime factors.
Suppose n is a Carmichael number, which is a product of two primes p, q, that is $n = pq$ with $1 < p < q < n$ and $(q - 1)|(n - 1)$.
Now $0 \equiv n - 1 \equiv pq - 1 \equiv (p - 1)(\text{mod q} - 1) \Rightarrow (q - 1)|(p - 1)$
$\Rightarrow q \leq p$, a contradiction. Hence a Carmichael number (composite number etc) is a product of two primes is wrong. Hence a Carmichael number is a product of more than two odd primes.
(iii) The taxicab number $1729 = 7 \times 13 \times 19 [= 10^3 + 9^3 = 12^3 + 1^3]$ which Hardy told to Ramanujan was uninteresting is also a Carmichael number.
(iv) If $p, 2p-1$ and $3p-2$ are all primes, with $p > 3$, then their product is a Carmichael number.
Let $n = p(2p - 1)(3p - 2)$, product of three primes where $p > 3$. Then
$n - 1 = 6p^3 - 7p^2 + 2p - 1 = (p - 1)(6p^2 - p + 1)$ is even and divisible by $p - 1$, here p is odd, so $6p^2 - p + 1$ is even and hence $2(p - 1)|(n - 1)$. As prime $p > 3$, so $p = 3q + 1 (p = 3q - 1$ is deleted since $3p - 2 = 3(3q - 1)$ is composite) for some $q \in \mathbb{N}$ and $6p^2 - p + 1 = 6(3q + 1)^2 - 3q$ is divisible by 3, i.e. $3(p - 1)|(n - 1)$.
Hence $p(2p - 1)(3p - 2)$ is a Carmichael number.

Using above remarks one can easily show that the numbers $7 \times 13 \times 19, 37 \times 73 \times 109$, $271 \times 541 \times 811, 307 \times 613 \times 919, 331 \times 661 \times 991$ are Carmichael numbers.
(v) Carmichael number of the form $3pq$ where p and q are primes with $3 < p < q$ is the only one, which is $3 \times 11 \times 17$. Carmichael numbers of the form 5pq where p and q are primes with $5 < p < q$ are only two, which are $5 \times 13 \times 17$ and $5 \times 29 \times 73$.
(vi) It is not known whether there exist infinitely many Carmichael numbers with a fixed number of prime factors.

6.3 Strong Pseudoprime to a base.

Let m be an odd pseudoprime to the base a and $\gcd(a, m) = 1$. Let $m - 1 = 2^r \times s$, where s is odd, $r \in \mathbb{N}$. Then

$$a^{m-1} - 1 = (a^s - 1)(a^s + 1)(a^{2s} + 1)(a^{4s} + 1) \cdots (a^{2^{r-1}s} + 1) \tag{6.3.1}$$

If m is a prime, then it divides exactly one of thses factors.

Definition 6.3.1. *An odd integer m is said to be a strong pseudoprime for the base a if it is composite, relatively prime to a, and divides one of the factors on the right hand side of equation* (6.3.1).

Remark 6.3.1. (Primality Test):[58] Let $n > 1$ be an odd positive integer and $a \in \mathbb{Z}$ such that $a^{n-1} \equiv 1(\text{mod n.})$ Consider the least positive residue of $a^{\frac{n-1}{2}}$modulo n
i.e. $a^{\frac{n-1}{2}}(\text{mod n}) \in U(n)$. For $x = a^{\frac{n-1}{2}}$, we have $x^2 = a^{n-1} \equiv 1(\text{mod n})$. For n prime we have by result 1.2.1(vii) [or by result 1.2.2] either $x \equiv 1(\text{mod n})$ or $x \equiv -1(\text{mod n})$. If $x \not\equiv \pm 1(\text{mod n})$, then n is composite.

Example 6.3.1. Let $a = 5$ and $n = 561$, the smallest Carmichael number. We have $5^{561-1} \equiv 1(\text{mod } 561)$ and $5^{\frac{561-1}{2}} = 5^{280} \equiv 67(\text{mod } 561)$. Hence 561 is composite.

To continue developing primality tests, we need the following definition.

Definition 6.3.2. [Miller's Test] [58]. *Let $m > 2$ be an integer and $m - 1 = 2^r s$, where r is a nonnegative integer and s is an odd positive integer. We say that m satisfies Miller's test for the base b if either $b^s \equiv 1 (mod\ m)$ or $b^{2^i s} \equiv -1 (mod\ m)$ for some i with $0 \leq i \leq t - 1$.*

Example 6.3.2. 2047 satisfies Miller's test for the base 2.
For $m = 2047 = 23 \times 89$, we have $2^{2046} = (2^{11})^{186} = (2048)^{186} \equiv 1(\text{mod } 2047)$,
so that 2047 is a pseudoprime to the base 2.
Now $m - 1 = 2046 = 2^1 \times 1023 = 2^r.s$ where $r = 1, s = 1023$ (odd) and
$2^s = 2^{1023} = (2^{11})^{93} = (2048)^{93} \equiv 1(\text{mod } 2047)$.
Therefore 2047 satisfies Miller's test for the base 2.

Theorem 6.3.1. *If m is prime and a is a positive integer with $m \nmid a$, then m satisfies Miller's test for the base a [58].*

Note: If the positive integer $m > 1$ satisfies Miller's test for the base a, then either $a^s \equiv 1(\text{mod m})$ or $a^{2^i s} \equiv -1(\text{mod m})$ for some i with $0 \leq i \leq r-1$, where $m-1 = 2^r s$ and s is an odd number.
In either case, we have $a^{m-1} \equiv 1(\text{mod m})$, because $a^{m-1} = (a^{2^i} s)2^{r-i}$ for $i = 0, 1, 2, \cdots, r$, so that a composite integer that satisfies Miller's test for the base b is automatically a pseudoprime to the base b. This observation give following definition.

Definition 6.3.3. *If a composite number m satisfies Miller's test for the base a, then we say m is a strong pseudoprime to the base a.*

By example (6.3.2) $2047 = 23 \times 89$ is a strong pseudoprime to the base 2.
Strong pseudoprimes are rare but infinitely many. We prove this for the base 2 with the following theorem.

Theorem 6.3.2. *[58] There are infinitely many strong pseudoprimes to the base 2.*

Proof. Let n be an odd pseudoprime to the base 2 (for example n= 341 etc.)
We will show the odd composite number $N = 2^n - 1$ is a strong pseudoprime to the

base 2. Now n is composite and $2^{n-1} \equiv 1(\text{mod n})$, then $2^{n-1} - 1 = nk$ for some $k \in \mathbb{N}$ and k must be odd. We have

$N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2^1 nk$; a factorization into a power of 2 and an odd integer.

As $2^n = (2^n - 1) + 1 = N + 1 \equiv 1(\text{mod N})$, so $2^{nk} \equiv 1(\text{mod N})$

$2^{\frac{(N-1)}{2}} \equiv 1(\text{mod N})$.

This proves that N satisfies Miller's test for base 2.

$\Rightarrow N = 2^n - 1$ is a strong pseudoprime to the base 2.

Every pseudoprime n to the base 2 yields a strong pseudoprime $2^n - 1$ to the base 2 and because there are infinitely many pseudoprimes to the base 2, so there are infinitely many strong pseudoprimes to the base 2.

□

Note: (Primality Test):[58] The smallest odd strong pseudoprime to the base 2 is 2047.

So if a positive odd integer $n < 2047$ satisfies Miller's test to the base 2, then n is prime.

The smallest odd strong pseudoprime to both the bases 2 and 3 is 1373653, giving us a primality test for an odd positive integer $n < 1373653$, i.e. if n satisfies Miller's test to both the bases 2 and 3, then n is prime.

The smallest odd strong pseudoprime to the bases 2, 3 and 5 is 25326001. The smallest odd strong pseudoprime to the base 2, 3, 5 and 7 is 3215031751 and there are no other strong pseudoprime to all these bases that are les than 25×10^9. This leads us to a primality test for integers less than 25×10^9. An odd integer n is prime if $n < 25 \times 10^9$, n satisfies Miller's test for the bases 2, 3, 5 and 7, and $n \not\equiv 3125031751$. Computations show that there are only 101 integers less than 10^{12} that are strong pseudoprimes to the bases 2, 3 and 5 simultaneously. Only 9 of these are also strong pseudoprimes to the base 7 and none of these is a strong pseudoprime to the base 11. The smallest strong pseudoprime to the bases 2, 3, 5, 7 and 11 simultaneously is 2152302898747. Therefore an odd positive integer $n < 2152302898747$ is prime if it satisfies Miller's test for bases 2, 3, 5, 7 and 11.

If we want to test a bigger odd integer for primality in this way, we observe that no positive integer < 3415500717228321 is a strong pseudoprime to the bases 2, 3, 5, 7, 11, 13 and 17.

A positive odd integer not exceeding 341550071728321 is prime if it satisfies Miller's test for the seven primes 2, 3, 5, 7, 11, 13 and 17.

From above observations we can say that there is no positive integer which is strong pseudoprime to the all primes. Thus there is no analogue to the Carmichael number for strong pseudoprimes.

Example 6.3.3. 25 is a strong pseudoprime to the base 7.

Solution: 25 is composite and $\gcd(7, 25) = 1, 7^2 \equiv -1 (\text{mod } 25)$

$\Rightarrow 7^{24} \equiv 1(\text{mod } 25)$ and $24 = 2^3 \times 3 = 2^r s$ where $r = 3, s = 3(\text{odd})$.

Now we determine k in $7^{2^j t} \equiv k(\text{mod } 25)$ whether $k = -1$ for some j, $0 \leq j \leq 2$.

$[7^t = 7^3 \equiv -7 \equiv 18(\text{mod } 25), 7^t \not\equiv 1(\text{mod } 25)]$.

For $i = 0, 7^3 \equiv 7(\text{mod } 25)$ and for $i = 1, 7^6 \equiv -1(\text{mod } 25)$.

Thus Miller's test satisfies 25 to the base 7.

Hence 25 is a strong pseudoprime to the base 7.

Example 6.3.4. (a) 1387 is a pseudoprime, but not a strong pseudoprime to the base 2.

(b) 1373653 is a strong pseudoprime to the bases 2 and 3.

(c) 25326001 is a strong pseudoprime to the bases 2, 3 and 5.

Solution: (a) A computation shows $2^{1387} \equiv 2(\text{mod } 1387)$, so 1387 is a pseudoprime. But $1387 - 1 = 2 \times 693$ and $2^{693} \equiv 512(\text{mod } 1387)$ [i.e. $2^s \not\equiv \pm 1(\text{mod } 1387)$ where $s = 693$ (odd)]. So 1387 fails Miller's test and hence it is not a strong pseudoprime to the base 2.

(c) Note that $25326001 - 1 = 2^4 \times 1582875 = 2^r \times s$ and with this value of s,

$2^s \equiv -1(\text{mod } 25326001), 3^s \equiv -1(\text{mod } 25326001)$ and $5^s \equiv 1(\text{mod } 25326001)$

$\Rightarrow$ Result.

Theorem 6.3.3. *(***Lucas's Converse of FLT)** *If n is a positive integer and if an integer x exists such that $x^{n-1} \equiv 1(mod\ n)$ and $x^{\frac{(n-1)}{q}} \not\equiv 1(mod\ n)$ for all prime*

divisors q of n - 1, then n is prime.

Proof. As $x^{n-1} \equiv 1(\text{mod n})$, i.e. $x^{n-1} = 1$ in $U(n)$, we have $o(x)|(n-1)$ and hence $o(x) \leq n-1$.

Suppose $o(x) \not\equiv n-1$. Then $n-1 = k \cdot o(x)$ for some integer $k > 1$. Now k has a prime divisor q, so $q|(n-1)$ and $x^{\frac{(n-1)}{q}} = x^{\frac{k \cdot o(x)}{q}} = (x^{o(x)})^{\frac{k}{q}} \equiv 1(\text{mod n})$ (since $x^{o(x)} = 1$ in $U(n)$ and $\frac{k}{q} \in \mathbb{N}$). This is a contradiction. So the supposition '$o(x) \not\equiv n-1$' is wrong.

Thus $o(x) = n-1 = o(U(n))$, i.e. $\phi(n) = n-1$

$\Rightarrow n$ is a prime. □

Corollary 6.3.4. *If n is an odd positive integer and if x is a positive integer such that* $x^{\frac{(n-1)}{2}} \equiv -1(mod\ n)$ *and* $x^{\frac{(n-1)}{q}} \not\equiv 1(mod\ n)$ *for all odd prime divisors q of n-1, then n is prime.*

Proof. $x^{\frac{(n-1)}{2}} \equiv -1(\text{mod n}) \Rightarrow x^{n-1} \equiv 1(\text{mod n})$ (by squaring).

Also given $x^{\frac{(n-1)}{q}} \not\equiv 1(\text{mod n})$ for all prime divisors q of $(n-1)$.

By theorem 6.3.3, n is prime. □

Example 6.3.5. (a) Let n= 1009. Then $11^{1008} \equiv 1(\text{mod } 1009)$. The prime divisors of 1008 are 2, 3 and 7 [$1008 = 2^4 \times 3^2 \times 7$].

As $11^{\frac{1008}{2}} = 11^{504} \equiv -1(\text{mod } 1009), 11^{\frac{1008}{3}} = 11^{336} \equiv 374(\text{mod } 1009)$,

$11^{\frac{1008}{7}} = 11^{144} \equiv 935(\text{mod } 1009)$; by theorem 6.3.3, 1009 is prime.

(b) Let $n = 2003$. The odd prime divisors of $n-1 = 2002$ are 7,11 and 13. As

$5^{\frac{2002}{11}} = 5^{183} \equiv 88(\text{mod } 2003)$ and $2^{\frac{2002}{13}} = 2^{154} \equiv 633(\text{mod } 2003)$,

by corollary 6.3.4, 2003 is prime.

(c) Let n= 997. Then $n-1 = 996 = 2^2 \times 3 \times 83$ has prime divisors 2,3,83.

Now $7^{\frac{996}{3}} \equiv 1(\text{mod } 997), 7^{\frac{996}{2}} = 7^{498} \equiv -1(\text{mod } 997)$,

$7^{\frac{996}{3}} = 7^{332} \equiv 304(\text{mod } 997)$ and $7^{\frac{996}{83}} = 7^{12} \equiv 9(\text{mod } 997)$.

Then by theorem 6.3.3, 997 must be prime.

Theorem 6.3.5. *If for each prime* p_i *dividing* $n-1$ *there exists an integer* a_i *such that*

$a_i^{n-1} \equiv 1(mod\ n)$ *but* $a_i^{\frac{(n-1)}{p_i}} \not\equiv 1(mod\ n)$, *then n is prime.*

Proof. Assume that $n-1 = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, with the p_i distinct primes. Also let h_i be the order of a_i modulo n. The combination of $h_i|(n-1)$ and $h_i \nmid \frac{(n-1)}{p_i}$ implies that $p_i^{k_i}|h_i$. but for each i, we have $h_i|\phi(n)$ and therefore $p_i^{k_i}|\phi(n)$. This gives $(n-1)|\phi(n)$, [but $(n-1) \geq \phi(n)$], i.e. $\phi(n) = n-1$ and hence n is prime. □

Example 6.3.6. For n= 997, $n-1 = 996 = 2^2 \times 3 \times 83$ has prime divisors 2, 3 and 83. For different bases 3, 5 and 7 we have $3^{\frac{996}{83}} = 3^{12} \equiv 40(\text{mod } 997)$,
$5^{\frac{996}{2}} = 5^{498} \equiv -1(\text{mod } 997), 7^{\frac{996}{3}} = 7^{332} \equiv 304(\text{mod } 997)$
Using theorem 6.3.5, 997 is a prime number.

6.4 Euler Pseudoprime.

Lemma 6.4.1. (Primality Test): *Consider an odd prime p such that $p \nmid b$ where b is an integer, then $b^{\frac{(p-1)}{2}} \equiv (\frac{b}{p})(mod\ p)$.*

Converse may not be true and it gives definition of Euler's pseudoprime.
Thus if n is an odd number, $b \in \mathbb{N}$ with $\gcd(b,n) = 1$ and $b^{\frac{(n-1)}{2}} \not\equiv (\frac{b}{n})(\text{mod n})$, then n is a composite number. Here $(\frac{b}{n})$ is the Jacobi symbol.

Example 6.4.1. For $n = 341$ and $b = 2$, we have
$\gcd(b,n) = 1, 2^{170} \equiv 1(\text{mod } 341), [\frac{n-1}{2} = 170]$. As $341 \equiv -3(\text{mod } 8)$, we have by definition 1.2.2, $(\frac{2}{341}) = -1$ and so $2^{270} \not\equiv (\frac{2}{341})(\text{mod } 341)$. This shows that 341 is not prime.

Pseudoprime based on Euler's criterion is defined below:

Definition 6.4.1. *If n is a composite, odd and positive integer that satisfies $b^{\frac{(n-1)}{2}} \equiv (\frac{b}{n})(mod\ n)$, where $b \in \mathbb{N}$ with $gcd(b,n) = 1$, then n is called an Euler pseudoprime to the base b.*

Example 6.4.2. Consider $n = 1105$ and b=2. As $1105 \equiv 1(\text{mod } 8)$, we have $(\frac{2}{1105}) = 1$. Now $2^{552} \equiv 1(\text{mod } 1105)$ (here $\frac{n-1}{2} = 552$ etc) gives $2^{552} \equiv (\frac{2}{1105})(\text{mod } 1105)$, because 1105 is composite, it is an Euler pseudoprime to the base 2.

Example 6.4.3. (a) 561 is an Euler pseudoprime to the base 2.
$[2^{\frac{(561-1)}{2}} = (2^{10})^{28} \equiv (-98)^{28} \equiv (-98^2)^{14} \equiv 67^{14} \equiv (67^2)^7 \equiv 1^7 \equiv 1(\text{mod } 561)$ and $(\frac{2}{561}) = 1$ because $561 \equiv 1(\text{mod } 8)$ etc]
(b) 15841 is a Carmichael number, a strong pseudoprime to the base 2 and an Euler pseudoprime to the base 2.

Result 6.4.1. *n* is Euler pseudoprime to the base $n - b$, where n is an Euler pseudoprime to the base b.

Result 6.4.2. If m is an Euler pseudoprime to the bases c and d, then m is also an Euler pseudoprime to the base cd.
Hint: $c^{\frac{(m-1)}{2}} \equiv (\frac{c}{m})(\text{mod m})$ and $d^{\frac{(m-1)}{2}} \equiv (\frac{d}{m})(\text{mod m})$
$\Rightarrow (cd)^{\frac{(m-1)}{2}} = c^{\frac{(m-1)}{2}} d^{\frac{(m-1)}{2}} \equiv (\frac{c}{m})(\frac{d}{m}) \equiv (\frac{cd}{m})(\text{mod m})$.

Theorem 6.4.1. *[58] If n is an Euler pseudoprime to the base b, then n is a pseudoprime to the base b.*

Proof. Let n be an Euler pseudoprime to the base b , so $b^{\frac{n-1}{2}} \equiv (\frac{b}{n})(\text{mod n})$ and $(\frac{b}{n}) = \pm 1$. On squaring , we get $b^{n-1} \equiv 1(\text{mod n})$, which gives n is a pseudoprime to the base b. □

Converse of above theorem is not true, as 341 is a pseudoprime to the base 2, it is not an Euler pseudoprime to the base 2.

Theorem 6.4.2. *[58] If n is a strong pseudoprime to the base b , then n is an Euler pseudoprime to the base b.*

Remark 6.4.1. Converse of theorem 6.4.2 is not true, for example 1105 is an Euler pseudoprime to the base 2 but it is not a strong pseudoprime to the base 2, since $2^{\frac{1105-1}{2}} = 2^{552} \equiv 1(\text{mod } 1105)$ whereas $2^{\frac{(1105-1)}{2^2}} = 2^{276} \equiv 781(\text{mod } 1105)$.

Under certain condition converse of theorem 6.4.2 is true, given in following two theorems:

Theorem 6.4.3. *[58] If $n \equiv 3(mod\ 4)$ and n is an Euler pseudoprime to the base b, then n is a strong pseudoprime to the base b.*

Proof. Since $n \equiv 3(\text{mod } 4)$, we have $n-1 = 2k$ where $k = \frac{n-1}{2}$ is odd. As n is an Euler pseudoprime to the base b, it follows that $b^k = b^{\frac{n-1}{2}} \equiv (\frac{b}{n})(\text{mod n})$. As $(\frac{b}{n}) = \pm 1$, so we have $b^k \equiv 1(\text{mod n})$ or $b^k \equiv \pm 1(\text{mod n})$
$\Rightarrow n$ is a strong pseudoprime to the base b. □

Theorem 6.4.4. *[58] If n is an Euler pseudoprime to the base b and* $(\frac{b}{n}) = -1$, *then n is a strong pseudoprime to the base b.*

Example 6.4.4. If $n = 5(\text{mod } 8)$ and n is an Euler pseudoprime to the base 2, then prove that n is a strong pseudoprime to the base 2.

Solution: $n \equiv 5(\text{mod } 8)$ i.e. $n \equiv -3(\text{mod } 8)$ gives $(\frac{2}{n}) = -1$. As n is an Euler pseudoprime to the base 2, we have
$2^{\frac{n-1}{2}} \equiv (\frac{2}{n}) \equiv -1(\text{mod n})$ and $n-1 = 2^2 t$ where t is odd.
Now $2^{\frac{n-1}{2}} = 2^{2t} \equiv -1(\text{mod n}) \Rightarrow$n is a strong pseudoprime to the base 2.