5.2 Fermat's Little Theorem

Theorem 5.2.1. *Fermat's Little Theorem: Let p be a prime and $p \nmid a$ then,* $a^{p-1} \equiv 1(\text{mod } p)$.

Proof. Let us begin with the first $p-1$ positive multiples of a which are

$$a, 2a, 3a, \cdots, (p-1)a.$$

None of them are congruent modulo p to any other. Then $ra \equiv sa(\text{mod } p)$ with $1 \leq r < s \leq p-1$ implies $r \equiv s(\text{mod } p)$, which is not possible. Multiplying we get,

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)(\text{ mod } p) \Rightarrow a^{p-1} \equiv 1(\text{ mod } p).$$

□

This is not the only way to prove the theorem. There are a lot more other interesting ways to prove this theorem. Mathematical induction is one among them. To begin with, we fix a prime p. For this prime p it is obvious that $1^p \equiv 1($ mod $p)$ *i.e.* $1^{p-1} \equiv 1(\text{mod } p)$, when $a = 1$. Suppose the statement prevails for $a = k$. Then $k^{p-1} \equiv 1(\text{mod } p)$. Now we have to prove $(k+1)^{p-1} \equiv 1(\text{mod } p)$ for some base $k+1 \in \mathbb{Z}$ and $p \nmid (k+1)$. Taking aid of binomial theorem we have,

$$(k+1)^p = k^p + \binom{p}{1}k^{p-1} + \cdots + \binom{p}{l-1}k + 1.$$

Because $\binom{p}{l} = \dfrac{p!}{l!(p-l)!}$ for $1 \leq l \leq p-1$, it follows that p divides every coefficients of the terms of right hand side of the foregoing equation except k^p and 1. Now taking modulo p we have $(k+1)^p \equiv k^p + 1(\text{mod } p)$. So by induction hypothesis we get $(k+1)^p \equiv k+1(\text{mod } p)$. Therefore the result holds for $k+1$. Hence the principle of mathematical induction yields $a^p \equiv a(\text{mod } p)$ *i.e.*$a^{p-1} \equiv 1($ mod $p)$ for all $a \in \mathbb{Z}$ such that $p \nmid a$.

The above two proofs of Fermat's Little theorem are mostly theoretic. Instead, we can provide some experimental ways by means of combinatorics to make the theorem more lively and natural. Choose $p = 3, a = 2$ where $3 \nmid 2$. Consider the following diagrams,

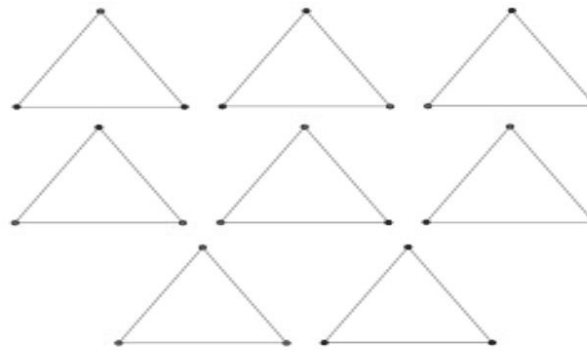

Figure 5.1: Fermat's Little Theorem

Here every angle of the triangles are associated with red and blue coloured balls. There are $2^3 = 8$ ways to pick the colour of the balls. Also we see that $2^3 - 2 = 6$ is divisible by 3. Therefore $2^3 \equiv 2 (\mathrm{mod}\ 3)$. Thus in general $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$ holds, where $p \nmid a$.

Our next corollary investigates the question: Can we drop the condition $\gcd(a, p) = 1$?

Corollary 5.2.1. *If p is prime, then $a^p \equiv a (\mathrm{mod}\ p)$ for any integer a.*

Proof. When $p \mid a$ then $a^p \equiv 0 \equiv a (\mathrm{mod}\ p)$ and if $p \nmid a$ then by above theorem $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$ implies $a^p \equiv a (\mathrm{mod}\ p)$. □

A simple but interesting question to ask: if $a^n \equiv a (\mathrm{mod}\ n)$ holds, then does it imply n is prime? The answer is in a negative sense. For instance, pick out $n = 117$. Then taking $a = 2$ we see that $2^{117} = (2^7)^{16} \cdot 2^5$ where $2^7 = 128 \equiv 11 (\mathrm{mod}\ 117)$. Thus we find $2^{117} \equiv 11^{16} \cdot 2^5 (\mathrm{mod}\ 117) \equiv 4^8 \cdot 2^5 (\mathrm{mod}\ 117) \equiv 2^{21} (\mathrm{mod}\ 117)$. But $2^{21} = (2^7)^3$. Hence $2^{21} \equiv 11^3 (\mathrm{mod}\ 117) \equiv 121 \cdot 11 (\mathrm{mod}\ 117) \equiv 4 \cdot 11 (\mathrm{mod}\ 117) \equiv 44 (\mathrm{mod}\ 117) \not\equiv 2 (\mathrm{mod}\ 117)$. Here we note $117 = 13 \cdot 9$. Hence, if $a^n \equiv a (\mathrm{mod}\ n)$ holds then n must be composite.

Our future discussions will be based on some instances where those types of composite numbers even satisfy this congruence relation under some special

circumstances.

Lemma 5.2.1. *If p and q are distinct primes with $a^p \equiv a(\text{mod } q)$ and $a^q \equiv a($ mod $p)$ then, $a^{pq} \equiv a(\text{mod } pq)$.*

Proof. It is very clear that $(a^p)^q \equiv a^q(\text{mod } p) \equiv a(\text{mod } p)$ and $(a^q)^p \equiv a^p($ mod $q) \equiv a(\text{mod } q)$. So we have $p|a^{pq}$ and $q|a^{pq}$. As $\gcd(p,q) = 1$ then we can directly say that $pq|a^{pq}$. Since $\gcd(a,b) = 1$ and $a|c, b|c$ together imply $ab|c$, therefore $a^{pq} \equiv a(\text{mod } pq)$. □

So the above lemma highlights the fact that the converse of Fermat's theorem satisfies for some special type of composite numbers which can be expressed as the product of two distinct primes. These types of numbers are said to be pseudo-prime to the base a. Now we are in a position to define pseudoprime viz

Definition 5.2.1. *A composite integer n for which $a^n \equiv a(\text{mod } n)$ is called a pseudoprime to the base a.*

If $a = 2$ then, it is called pseudo prime to the base 2 or simply pseudoprime.

Let us take $341 = 11 \cdot 31$. So by Fermat's Little Theorem we have $2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1024(\text{mod } 31) \equiv 2 \cdot 1(\text{mod } 31) \equiv 2(\text{mod } 31)$ and $2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1^3($ mod $11) \equiv 2(\text{mod } 11)$. Furthermore, $\gcd(11, 31) = 1$. In view of Lemma(5.2.1) we can say that $2^{11 \cdot 31} = 2^{341} \equiv 2(\text{mod } 341)$ which further yields 341 as a pseudoprime. In fact, the first five pseudoprimes are $341, 561, 645, 1105, 161038$ and the first four are odd. Finding pseudoprimes are difficult as those are rarer than primes. There are only 245 pseudoprimes and 78498 primes less than 10^6. We now try to construct an increasing sequence of pseudoprimes from the following theorem.

Theorem 5.2.2. *There are infinitely many psuedo-primes to the base 2.*

Proof. Let n be a composite number. Then $\exists\ r, s \in \mathbb{Z}$ such that $n = rs$ where $1 < r \leq s < n$. Let $K_n = 2^n - 1$ be any integer where $(2^r - 1)|(2^n - 1)$[refer to Problem(2.6.4)] or $(2^r - 1)|K_n$, making K_n a composite quantity.

As n is pseudo-prime then $2^n \equiv 2(\text{mod } n)$. Hence $2^n - 2 = kn$ for some $k \in \mathbb{Z}$. Therefore

$$\begin{aligned} 2^{K_n - 1} = 2^{kn} - 1 &= (2^n - 1)[2^{n(k-1)} + \cdots + 2^n + 1] \\ &= K_n[2^{n(k-1)} + \cdots + 2^n + 1] \\ &\equiv 0(\text{ mod } K_n). \end{aligned}$$

Hence $2^{K_n} \equiv 2(\text{mod } K_n)$. Therefore K_n is a pseudoprime. □

Remark 5.2.1. *The number $K_n = 2^n - 1$ shown in the above theorem is said to be Mersenne number, which is named after Father Marin Mersenne* (1588 – 1648)*[for further studies refer to Chapter 10 Section 10.4 of this book].*

The above discussion generates the fact that the pseudoprimes are the special type of composite numbers which satisfies the conditions of Fermat's Little theorem. But in pseudoprime, we have a barrier of base element a *i.e.* for these types of numbers the condition of Fermat's theorem does not satisfy for all base elements a. If we consider $561(= 3 \times 11 \times 17)$ with $\gcd(a, 561) = 1$ for any $a \in \mathbb{Z}^+$, we have $\gcd(a, 3) = 1 = \gcd(a, 11) = \gcd(a, 17)$. By virtue of Fermat's theorem, we get $a^2 \equiv 1(\text{mod } 3), a^{10} \equiv 1(\text{mod } 11), a^{16} \equiv 1(\text{mod } 17)$ which imply

$$a^{560} = (a^2)^{280} \equiv 1(\text{ mod } 3)$$
$$a^{560} = (a^{10})^{56} \equiv 1(\text{ mod } 11)$$
$$a^{560} = (a^{16})^{35} \equiv 1(\text{ mod } 17).$$

Since $3, 11, 17$ are primes, the last three congruences together conclude $a^{560} \equiv 1($ mod $561)$. Therefore $a^{561} \equiv a(\text{mod } 561)$ for all $a \in \mathbb{Z}^+$ with $\gcd(a, 561) = 1$.

The last example spotlights the fact that 561 is a special type of composite number which satisfies the condition of Fermat's theorem for any integer. R.D.Carmichael first noticed the existence of these types of numbers in the year 1910. Those numbers are called Carmichael numbers named after American Mathematician Carmichael. There are six Carmichael numbers $561, 1105, 1729, 2465, 2821, 6601$ less than $10,000$. There are just 43 Carmichael numbers less than 10^6 and 1547 less than 10^{10}. Thus we are in a position to define the Carmichael number.

Definition 5.2.2. *The composite numbers n which satisfy the property $a^n \equiv a($* mod $n)$ *for all integers a are said to be absolute pseudoprime or Carmichael numbers.*

Next our aim is to establish the criterion for the existence of Carmichael numbers.

Theorem 5.2.3 (Korselt's Criterion)**.** *Let n be a composite square free integers; $n = p_1 p_2 \cdots p_n$ where p_i are distinct primes. If $(p_i - 1)\big|(n-1)$ for $i = 1, 2, \cdots, r$ then n is Carmichael number.*

Proof. Suppose that a is an integer satisfying $\gcd(a, p_i) = 1$ for each i. Then, by Fermat's theorem we have $p_i|(a^{p_i - 1} - 1)$. As $(p_i - 1)|(n-1)$ so $p_i|(a^{n-1} - 1)$, as $p_i|(a^n - a)$, for all a and $i = 1, 2, 3, \cdots, r$. This implies $n\big|(a^n - a)$ for all a. Therefore n is Carmichael number. □

The next theorem supplies the pertinent information about the prime factorizations of Carmichael numbers.

Theorem 5.2.4. *A Carmichael number must have at least three different odd prime factors.*

Proof. Let n be a Carmichael number. Since n is composite and is the product of distinct primes so, it cannot have just one prime factor. Then assume, $n = pq$ for some odd primes p, q with $p > q$. So

$$n - 1 = pq - 1 = (p - 1)q + (q - 1) \equiv (q - 1) \not\equiv 0(\mod p - 1),$$

which render $(p-1) \nmid (n-1)$. Since it has just two different prime factors hence, n cannot be a Carmichael number. □

The development of primality of testing can be done further with the following:

Definition 5.2.3. *Let n be a positive integer with $n-1 = 2^k t$ where k is a non–negative integer and t is an odd positive integer. We can say n passes Miller's test for the base a if either $a^t \equiv 1(\mod n)$ or $a^{2^i t} \equiv -1(\mod n)$ for some i with $0 \leq i \leq k-1$.*

The next theorem shows the idea of primality testing by means of Miller's test.

Theorem 5.2.5. *If n is prime and a is a positive integer with $n \nmid a$, then n passes Miller's test for the base a.*

Proof. Let $n - 1 = 2^k t$ where k is non–negative integer and t is an odd positive integer. Let $z_\omega = a^{\frac{(n-1)}{2^\omega}} = a^{2^{k-\omega} \cdot t}$ for $\omega = 0, 1, 2, \ldots, k$. Since n is prime, by Fermat's little theorem we have $z_0 = a^{n-1} \equiv 1(\mod n)$. Furthermore $z_1^2 = \left(a^{\frac{n-1}{2}}\right)^2 = a^{n-1} = z_0 \equiv 1(\mod n)$ implies either $z_1 \equiv -1(\mod n)$ or $z_1 \equiv 1(\mod n)$. If $z_1 \equiv 1(\mod n)$ then $z_2^2 = \left(a^{\frac{n-1}{2^2}}\right)^2 = a^{\frac{n-1}{2}} = z_1 \equiv 1(\mod n)$. Thus either $z_2 \equiv 1(\mod n)$ or $z_2 \equiv -1(\mod n)$. Proceeding as above, $z_0 \equiv z_1 \equiv z_2 \cdots z_\omega \equiv 1(\mod n)$ for $\omega < k$. Also, $z_{\omega+1}^2 = z_\omega \equiv 1(\mod n)$ or $z_{\omega+1} \equiv 1(\mod n)$. Thus continuing for $\omega = 1, 2, 3, \ldots, k$ we find that either $z_k \equiv 1(\mod n)$ or $z_\omega \equiv -1(\mod n)$ for some integer ω with $0 \leq \omega \leq (k-1)$. Hence n passes Miller's test for the base a. □

Let us illustrate the above theorem by the following example. Choose $n = 25 = 5 \cdot 5$. Then $7^{24} = (7^4)^6 \equiv 1(\mod 5)$ such that 25 is a pseudoprime to the

base 7. Also $24 = 2^3 \cdot 3$ then $7^{2^1 \cdot 3} \equiv -1 (\mathrm{mod}\ 25)$. Therefore 25 passes Miller's test for base 7 as well as it is a pseudoprime. So getting motivated from the example we are going to define:

Definition 5.2.4. *If n is composite and passes Miller's test to the base a, then n is called strong pseudoprime to the base a.*

Let us illustrate the ideas behind the definition(5.2.4) with an example of strong pseudoprime which has passed Miller's test. Consider $n = 25326001$. Then $n-1 = 2^4 \times 1582875$. Here we can check that $2^{1582875} \equiv -1 (\mathrm{mod}\ 25326001)$. This shows that 25326001 is a strong pseudoprime as it passes Miller's test.

Strong pseudoprimes are rare but there are still infinitely many of them. We conclude this section with a theorem that reflects the existence of an infinite number of strong pseudoprimes to the base 2.

Theorem 5.2.6. *There are infinitely many strong pseudoprimes to the base 2.*

Proof. To begin with, suppose n to be an odd pseudoprime base 2. We claim that the composite number $N = 2^n - 1$ is a strong pseudoprime to the base 2. Referring to Problem 2.6.4 we see that if n is composite then $2^n - 1$ is also so. Furthermore, if n is pseudoprime then we have $2^{n-1} \equiv 1 (\mathrm{mod}\ n)$. This implies that $2^{n-1} - 1 = nk$ for some odd integer $k(> 0)$. We note that

$$N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2nk.$$

As $2^n = (2^n - 1) + 1 = N + 1 \equiv 1 (\mathrm{mod}\ N)$ then we can write $2^{\frac{(N-1)}{2}} = 2^{nk} \equiv 1 (\mathrm{mod}\ N)$. The argument shows that N passes Miller's test for base 2. Thus N becomes a strong pseudoprime base 2. An appeal to Theorem 5.2.2 concludes that there are infinitely many strong pseudoprime to the base 2. This finishes the proof. □

5.3 Worked out Exercises

Problem 5.3.1. *If* $\gcd(a, 35) = 1$, *show that* $a^{12} \equiv 1 (\mathrm{mod}\ 35)$.

Solution 5.3.1. *As* $\gcd(a, 35) = 1$, *therefore* $\gcd(a, 7) = 1 = \gcd(a, 5)$. *An appeal to Fermat's theorem indicates* $a^6 \equiv 1 (\mathrm{mod}\ 7) \Rightarrow a^{12} = (a^6) \cdot (a^6) \equiv 1 (\mathrm{mod}\ 7)$ *and* $a^4 \equiv 1 (\mathrm{mod}\ 5) \Rightarrow (a^4)^3 \equiv 1 (\mathrm{mod}\ 5)$. *Since* $\gcd(5, 7) = 1$, *it follows that* $35 \big| (a^{12} - 1)$. *Therefore* $a^{12} \equiv 1 (\mathrm{mod}\ 35)$.

Problem 5.3.2. *If* $\gcd(a, 42) = 1$ *then* $168 = 3 \cdot 7 \cdot 8$ *divides* $a^6 - 1$.

Solution 5.3.2. *Because* $\gcd(a, 42) = 1$, *therefore* $\gcd(a, 7) = \gcd(a, 3) = \gcd(a, 2) = 1$. *By virtue of Fermat's theorem, we find* $a^6 \equiv 1 (\mod 7)$, $a^2 \equiv 1 (\mod 3)$ *and* $a \equiv 1 (\mod 2)$. *Therefore* $a^6 = (a^2)^3 \equiv 1 (\mod 3)$. *Moreover,* $a^6 - 1 = (a^3 - 1)(a^3 + 1) = (a - 1)(a + 1)(a^2 + a + 1)(a^2 - a + 1)$. *Because* a *is odd therefore,* $a > 0 \Rightarrow a \geq 3$. *This yields* $2 \big| (a - 1)$, $4 \big| (a + 1)$. *Since* $7, 3, 8$ *are relatively prime to each other, therefore we get* $168 \big| (a^6 - 1)$. *Hence* $8 \big| (a^6 - 1)$.

Problem 5.3.3. *If* $\gcd(a, 133) = \gcd(b, 133) = 1$ *then, show that* $133 | (a^{18} - b^{18})$.

Solution 5.3.3. *We know that* $133 = 7 \cdot 19$ *and* $\gcd(a, 19) = \gcd(b, 19) = 1$. *Therefore in view of Fermat's theorem we obtain* $a^{18} \equiv 1 (\mod 19)$ *and* $b^{18} \equiv 1 (\mod 19)$. *Hence* $a^{18} - b^{18} \equiv (1 - 1) (\mod 19) \equiv 0 (\mod 19)$. *Hence* $19 | (a^{18} - b^{18})$. *By similar reasoning,* $7 | (a^6 - b^6)$. *Since* $a^{18} - b^{18} = (a^6 - b^6) \left((a^6)^2 + a^6 b^6 + (b^6)^2 \right)$, *therefore we have* $7 | (a^{18} - b^{18})$. *Thus* $7 \cdot 19 = 133 | (a^{18} - b^{18})$.

Problem 5.3.4. *Derive the following congruences:*
(a) $a^{21} \equiv a (\mod 15)$, $\forall a$. *(b)* $a^7 \equiv a (\mod 42)$ $\forall a$. *(c)* $a^9 \equiv a (\mod 30)$ $\forall a$.

Solution 5.3.4. **(a)** *Taking into consideration the corollary of Fermat's theorem, we find* $a^{21} \equiv a (\mod 5) \Rightarrow (a^5)^4 \equiv a^4 (\mod 5) \Rightarrow a^{21} \equiv a^5 \equiv a (\mod 15)$. *Furthermore,* $a^3 \equiv a (\mod 3) \Rightarrow a^{21} \equiv a^7 (\mod 3)$. *Again,* $(a^3)^2 \equiv a^2 (\mod 3) \Rightarrow a^7 \equiv a^3 (\mod 3) \equiv a (\mod 3)$. *Hence* $a^{21} \equiv a (\mod 3)$. *Thus,* $a^{21} \equiv a (\mod 15)$.

(b) *As* $42 = 7 \cdot 3 \cdot 2$ *by Fermat's theorem we have* $a^7 \equiv a (\mod 7)$ *and* $a^3 \equiv a (\mod 3)$. *Therefore* $a^6 \equiv a^2 (\mod 3) \Rightarrow a^7 \equiv a^3 (\mod 3) \equiv a (\mod 3)$. *Also,* $a^2 \equiv a (\mod 2) \Rightarrow a^6 \equiv a^3 (\mod 2) \equiv a (\mod 2) \Rightarrow a^7 \equiv a^2 (\mod 2) \equiv a (\mod 2)$. *Since* $7, 3, 2$ *are prime to each other therefore,* $a^7 \equiv a (\mod (7 \cdot 3 \cdot 2)) \Rightarrow a^7 \equiv a (\mod 42)$.

(c) *Left to the reader.*

Problem 5.3.5. *If* $\gcd(a, 30) = 1$, *show that* $60 \big| (a^4 + 59)$.

Solution 5.3.5. *Note that* $\gcd(a, 30) = 1$ *implies* $\gcd(a, 2) = \gcd(a, 3) = \gcd(a, 5) = 1$. *So* $\gcd(a, 4) = \gcd(a, 2^2) = 1$. *Now* $60 = 2^2 \cdot 3 \cdot 5$ *and* $60 | (a^4 + 59)$ *together implies* $a^4 \equiv 1 (\mod 60)$. *Here* $a^2 \equiv 1 (\mod 3)$ *implies* $a^4 \equiv 1 (\mod 3)$ *and* $a^4 \equiv 1 (\mod 5)$. *Further,* $a \equiv 1 (\mod 2) \Rightarrow a^2 \equiv 1 (\mod 2)$ *which leads to* $2 \big| (a^2 - 1)$. *Hence*

$$\begin{aligned} a^2 &\equiv (1 - 2)(\mod 2) \\ &\equiv -1(\mod 2). \end{aligned}$$

Thus, combining the foregoing equation with $2\big|(a^2+1)$ *yields* $2\big|(a^4-1)$. *Since* $3,4,5$ *relatively prime to each other, therefore we can conclude* $60|(a^4-1)$. *Hence*

$$\begin{aligned} a^4 &\equiv 1(\mod 60) \\ &\equiv (1-60)(\mod 60) \\ &\equiv -59(\mod 60). \end{aligned}$$

This completes the solution.

Problem 5.3.6. *(a) Find the unit digit of* 3^{100} *using Fermat's theorem.*
(b) For any integer verify that a^5 *and* a *have same unit digit.*

Solution 5.3.6. *(a) Its suffices to consider modulo 10. Now we plan to use Fermat's theorem to get* $3^4 \equiv 1(\mod 5)$. *Therefore* $3^{100} \equiv 1(\mod 5)$. *Moreover* $3 \equiv 1(\mod 2)$. *Hence* $3^{100} \equiv 1(\mod 2)$. *Further* $\gcd(2,5) = 1 \Rightarrow 10\big|3^{100} \equiv 1(\mod 10)$. *Hence the unit digit is* 1.

(b) By virtue of Fermat's theorem, $a^5 \equiv a(\mod 5)$ *and* $a^2 \equiv a(\mod 2)$. *Hence* $a^4 \equiv a^2(\mod 2) \equiv a(\mod 2)$ *implies* $a^5 \equiv a^2(\mod 2) \equiv a(\mod 2)$. *Thus* $a^5 \equiv a(\mod 10)$. *Let* $0 \le r < 10$ *holds. Then* $a^5 - r \equiv a - r(\mod 10)$. *Therefore* $a^5 - r \equiv 0(\mod 10) \iff a - r \equiv 0(\mod 10)$. *Therefore unit digit's are same.*

Problem 5.3.7. *If* $7 \nmid a$, *then prove that either* $7|(a^3+1)$ *or* $7|(a^3-1)$.

Solution 5.3.7. *By Fermat's theorem,* $a^6 \equiv 1(\mod 7)$. *Therefore* $7|(a^6-1)$ *but* $a^6 - 1 = (a^3-1)(a^3+1)$. *Therefore* $7 \nmid (a^3+1)$ *implies* $7|(a^3-1)$ *and vice–versa.*

Problem 5.3.8. *If* p, q *are distinct odd primes such that* $(p-1)|(q-1)$ *and* $\gcd(a, pq) = 1$, *show that* $a^{q-1} \equiv 1(\mod pq)$.

Solution 5.3.8. *Here* $\gcd(a, pq) = 1$ *implies* $\gcd(a,p) = 1 = \gcd(a,q)$. *Therefore with the help of Fermat's Theorem we get* $a^{p-1} \equiv 1(\mod p)$ *and* $a^{q-1} \equiv 1(\mod q)$. *Since* $(p-1)\big|(q-1)$, *therefore* $q - 1 = k(p-1)(k \in \mathbb{Z})$. *Hence* $(a^{p-1})^k \equiv 1^k(\mod p) \equiv 1(\mod p) \Rightarrow a^{q-1} \equiv 1(\mod p)$. *Thus* $pq|(a^{q-1}-1) \Rightarrow a^{q-1} \equiv 1(\mod pq)$.

Problem 5.3.9. *If* p, q *are distinct primes then prove that* $p^{q-1} + p^{q-1} \equiv 1(\mod pq)$.

Solution 5.3.9. *By virtue of Fermat's theorem,* $p^{q-1} \equiv 1(\mod q)$ *implies* $q^{p-1} \equiv 0(\mod q)$. *Therefore* $p^{q-1} + p^{q-1} \equiv 1(\mod q)$. *Similarly,* $q^{p-1} + p^{q-1} \equiv 1(\mod p)$. *Further,* $\gcd(p,q) = 1$ *yields* $p^{q-1} + p^{q-1} \equiv 1(\mod pq)$.

Problem 5.3.10. *Establish the statement: If* p *is an odd prime, then* $1^{p-1} + 2^{p-1} \cdots (p-1)^{p-1} \equiv (p-1) \equiv -1(\mod p)$.

Solution 5.3.10. *Since p is odd prime, so $p \geq 3$ and $p \nmid a$. if $a < p$ then by Fermat's theorem we have, $a^{p-1} \equiv 1(\text{mod } p)$. For $p-1$ terms we have,*

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

   $\vdots$
3. $(p-1)^{p-1} \equiv 1(\text{mod } p)$.

Therefore $1^{p-1} + 2^{p-1} \cdots (p-1)^{p-1} \equiv (p-1) \equiv -1(\text{mod } p)$.

Problem 5.3.11. *Confirm* $1105 = 5 \cdot 13 \cdot 17$ *is absolute pseudoprime.*

Solution 5.3.11. *For any integer a, if $1105 \nmid a$ then $5 \nmid a$, $13 \nmid a$ & $17 \nmid a$. So by Fermat's theorem, we have $a^4 \equiv 1(\text{mod } 5) \Rightarrow a^{1104} = (a^4)^{276} \equiv 1(\text{mod } 5)$. Also $a^{12} \equiv 1(\text{mod } 13) \Rightarrow a^{1104} = (a^{12})^{92} \equiv 1(\text{mod } 13)$. Moreover, $a^{16} \equiv 1(\text{mod } 17) \Rightarrow a^{1104} = (a^{16})^{69} \equiv 1(\text{mod } 17)$. As $5, 13, 17$ are relatively prime to each other, therefore $a^{1104} \equiv 1(\text{mod } 1105)$. Thus $a^{1105} \equiv a(\text{mod } 1105)$ provided $1105 \nmid a$. Clearly, $a^{1105} \equiv a(\text{mod } 1105)$ prevails provided $1105 \mid a$. Hence 1105 is an absolute pseudo prime as it satisfies $a^{1105} \equiv a(\text{mod } 1105)$ for any integer a.*

Problem 5.3.12. *Prove that any integer of the form $n = (6k+1)(12k+1)(18k+1)$ is an absolute pseudoprime if all three factors are prime; hence $1729 = 7 \cdot 13 \cdot 19$ is also absolute pseudo–prime.*

Solution 5.3.12. *Let $p_1 = 6k+1, p_2 = 12k+1, p_3 = 18k+1$, be all primes. Now $n = 36 \cdot 36k^3 + 36 \cdot 2k^2 + 36 \cdot 9k^2 + 36k + 1$. Therefore $n-1 = 36k[36 \cdot k^2 + 11k + 1]$ gives $p_1 - 1 \big| n-1, p_2 - 1 \big| n-1$ and $p_3 - 1 \big| n-1$. Since p_1, p_2, p_3 are distinct primes and n is square free, therefore n is absolute pseudoprime.*

Problem 5.3.13. *Show that* 561 *is the only Carmichael number of the form* $3pq$ *where p and q are primes.*

Solution 5.3.13. *Let $n = 3pq$, with $q > p$ odd primes, be a carmichael number. Then using Korselt's criterion, we obtain $(p-1) \big| (3pq-1) = 3(p-1)q + 3q - 1$. So $(p-1) \big| (3q-1) \Rightarrow (p-1)a = 3q - 1$ for some $a \in \mathbb{Z}$. Since $q > p$, we must have $a \geq 4$. Similarly, $\exists\ b \in \mathbb{Z}$ satisfying $(q-1)a = 3p - 1$. Solving these two equations for p, q yields*

$$p = \frac{2b + ab - 3}{ab - 9} = 1 + \frac{2b + 6}{ab - 9}, \tag{5.3.1}$$

$$q = \frac{2a + ab - 3}{ab - 9}. \tag{5.3.2}$$

Since $p > 3$ being odd prime, therefore $4(ab-9) \leq 2b+6$ reduces to $b(2a-1) \leq 21$. Now $a \geq 4 \Rightarrow b \leq 3$. Then,

$$4(ab-9) \leq 2b+6 \leq 12 \Rightarrow ab \leq \frac{21}{4} \Rightarrow a \leq 5.$$

Hence $a = 4$ or 5. If $b = 3$, then the denominator of (5.3.2) is multiple of 3. So the numerator must be multiple of 3, which is impossible as there $\nexists$ any 'a' divisible by 3. Thus $b = 1$ or 2.The denominator of equation (5.3.2) must be positive, so $ab > 9$. Thus the only possible values for a and b is 5 and 2 respectively, which gives $p = 11, q = 17$. So $561 = 3 \cdot 11 \cdot 17$ is the only Carmichael number of the form $3pq$, where p and q are primes.

Problem 5.3.14. *Show that there are only a finite number of Carmichael numbers of the form $n = pqr$ where p is a fixed prime, and q and r are also primes.*

Solution 5.3.14. *Assume $r > q$. Applying Korselt's Criterion, we get $(q-1)\big|(pqr-1) = (q-1)pr + pr - 1$. Therefore $(q-1)\big|(pr-1) \Rightarrow pr - 1 = a(q-1)$ for some $a \in \mathbb{Z}$. Similarly, $pq - 1 = b(r-1)$ for some $b \in \mathbb{Z}$. Since, $r > q$ so $a > b$. Solving last two equations for q and r yields*

$$r = \frac{p(a-1) + a(b-1)}{ab - p^2},$$
$$q = \frac{p(b-1) + b(a-1)}{ab - p^2}.$$

Because this last fraction must be an integer, we have

$$ab - p^2 \leq p^2 + pb - p - b,$$

which further reduces to

$$a(b-1) \leq 2p^2 + p(b-1),$$
$$\Rightarrow a - 1 \leq \frac{2p^2}{b} + \frac{p(b-1)}{b} \leq 2p^2 + p.$$

So $\exists$ only finite values for a. Likewise, the same inequality gives

$$b(a-1) \leq 2p^2 + p(b-1),$$
$$\Rightarrow b(a-1-p) \leq 2p^2 - p.$$

Since $a > b$ and the denominator of the expression for q must be positive, we have $a \geq p+1$. Now, $a = p+1$ gives

$$(p+1)(q-1) = pq - p + q - 1 = pr - 1 \Rightarrow p|q, \text{ a contradiction.}$$

Therefore $a > p+1 \Rightarrow a-p-1 > 0$. *The last inequality gives us*

$$b \leq b(a-p-1) \leq 2p^2 - p,$$

which shows $\exists$ *finitely many values of* b. *Because* a, b *determine* q, r *respectively, therefore there are only a finite number of Carmichael numbers of the form* $n = pqr$.

Problem 5.3.15. *Show that* 2047 *is a strong pseudoprime base* 2.

Solution 5.3.15. *Here* $n = 2047$ *yields* $n-1 = 2046 = 2 \times 1023$. *Now* $2^{1023} = (2^{11})^{93} = 2048^{93} \equiv 1 (\mathrm{mod}\ 2047)$. *So* 2047 *passes Miller's test for base* 2. *Thus* 2047 *is a strong pseudoprime base* 2.

5.4 Wilson's Theorem

Wilson's theorem, in number theory, signifies that any prime p divides $(p-1)!+1$, where $n!$ is the factorial notation for $1 \times 2 \times 3 \times 4 \times \cdots \times n$. For example, 7 divides $(7-1)! + 1 = 6! + 1 = 721$. The conjecture was first published by the English mathematician Edward Waring in Meditationes Algebraicae (1770 'Thoughts on Algebra'), where he described it to the English mathematician John Wilson.

After that it was proved by the French mathematician Joseph-Louis Lagrange in 1771. The converse of the theorem is also true; that is, $(n-1)! + 1$ is not divisible by a composite number n. In theory, these theorems provide a test for primes; in practice, the calculations are impractical for large numbers.

Theorem 5.4.1. *Wilson's Theorem: If* p *is a prime then* $(p-1)! \equiv -1 (\mathrm{mod}\ p)$.

Proof. Let us choose $p > 3$ and consider the linear congruence $ax \equiv 1 (\mathrm{mod}\ p)$ where a is any one of $1, 2, 3, \cdots, p-1$. Therefore $\gcd(a, p) = 1$. Hence, it has an unique solution viz $a\tilde{a} \equiv (\mathrm{mod}\ p)$ with $1 \leq \tilde{a} \leq p-1$. Because p is prime, $a = \tilde{a} \Leftrightarrow a = 1$ or $a = p-1$ provided $a^2 \equiv 1 (\mathrm{mod}\ p) \Rightarrow (a-1)(a+1) \equiv 0 (\mathrm{mod}\ p)$. Therefore $(a-1) \equiv 0 (\mathrm{mod}\ p)$ or $(a+1) \equiv 0 (\mathrm{mod}\ p)$. Now if we delete 1 and $p-1$, then the remaining $2, 3, \ldots, p-2$ are set into pairs a and $\tilde{a}$, where $a \neq \tilde{a}$. So if these $\frac{p-3}{2}$ congruences are multiplied, we obtain $2 \cdot 3 \cdots (p-2) \equiv 1 (\mathrm{mod}\ p) \Rightarrow (p-2)! \equiv 1 (\mathrm{mod}\ p) \Rightarrow (p-1)! \equiv (p-1) \equiv -1 (\mathrm{mod}\ p)$. □

Let us illustrate the use of the theorem by means of an example. Let us take

$p = 11$. Divide the integers $2, 3, 4, 5, 6, 7, 8, 9$ into $\frac{p-3}{2}$ pairs such as

$$2 \cdot 6 \equiv 1(\mod 11)$$
$$3 \cdot 4 \equiv 1(\mod 11)$$
$$7 \cdot 8 \equiv 1(\mod 11)$$
$$5 \cdot 9 \equiv 1(\mod 11)$$

Multiplying each pair together we obtain, $9! \equiv 1(\mod 11)$. Hence $10! \equiv 1(\mod 11)$, shows the result is true for $p = 11$. An interesting observation is that the converse is also true. Let n be a non–prime required integer. Then n must have a divisor d where $1 < d < n$. As $d \leq n - 1$, we have $d|(n-1)!$. Now from the condition we have, $n|((n-1)!+1)$. Hence combining the conditions, we have $d|((n-1)!+1)$. Thus $d|1$ leads to contradiction, showing n is prime. Taking Wilson's theorem and its converse together we can say that the condition is necessary and sufficient for an integer to be prime. Thus it gives us a condition of testing primality.

Now we are at the end of this discussion with an application of Wilson's theorem on quadratic congruences, where quadratic congruences assume the form $Ax^2 + Bx + C \equiv 0(\mod m)$, where $A \not\equiv 0(\mod m)$ (otherwise the congruence would be a linear congruence). We will learn methods to evaluate these quadratic congruences. However, we will first restrict our modulus m to being only an odd prime $(3, 5, 7, 11, 13, \ldots)$, or rather, any prime except 2. Now we are in a position to state the following theorem:

Theorem 5.4.2. *The quadratic congruence $x^2 + 1 \equiv 0(\mod p)$ where p is an odd prime, has a solution if and only if $p \equiv 1(\mod 4)$.*

Proof. Let a be a solution of $x^2+1 \equiv 0(\mod p)$ then $a^2 \equiv -1(\mod p)$. Since $p \nmid a$ by Fermat's theorem, we have $1 \equiv a^{p-1}(\mod p) \equiv (a^2)^{\frac{p-1}{2}}(\mod p) \equiv (-1)^{\frac{p-1}{2}}(\mod p)$. The possibility that $p = 4k + 3$ for any integer k does not arise as $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$. Therefore $1 \equiv (-1)(\mod p)$ implies $p|2$ which is a contradiction. So p is of the form $4k + 1$. Now, $(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1)$ and

$$p - 1 \equiv -1(\mod p)$$
$$p - 2 \equiv -2(\mod p)$$
$$\vdots$$
$$\frac{p+1}{2} \equiv \left(\frac{p-1}{2}\right)(\mod p).$$

Therefore $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 (\text{mod } p)$. If we assume $p = 4k+1$, then $(-1)^{\frac{p-1}{2}} = 1$. Therefore $-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 (\text{mod } p)$, by Wilson's theorem. Therefore $\left(\frac{p-1}{2}\right)!$ satisfies $x^2 + 1 \equiv 0(\text{mod } p)$. □

5.5 Worked out Exercises

Problem 5.5.1. *Find the remainder when* 15! *is divided by* 17.

Solution 5.5.1. *Since* $(17-1)! = 16!$, *we have by virtue of Wilson's theorem* $(17-1)! \equiv -1(\text{mod } 17)$. *Therefore* $16! \equiv -1(\text{mod } 17) \equiv 16(\text{mod } 17) \Rightarrow 15! \equiv 1($ mod 17). *Hence the remainder is* 1.

Problem 5.5.2. *Find the remainder when* 2(26)! *is divided by* 29.

Solution 5.5.2. *From Wilson's theorem, we find* $28! \equiv -1(\text{mod } 29) \Rightarrow 28! \equiv 28($ mod 29) $\Rightarrow 27! \equiv 1(\text{mod } 29)$. *Here we note that* $\gcd(28, 29) = 1 \Rightarrow 27(26)! \equiv (1 + 29) = 30(\text{mod } 29) \Rightarrow 9(26)! \equiv 10(\text{mod } 29) \Rightarrow 9(26)! \equiv (10 + 29) = 9($ mod 29) $\Rightarrow 3(26)! \equiv 13(\text{mod } 29) \Rightarrow 3(26)! \equiv (13 + 29) = 42(\text{mod } 29) \Rightarrow (26)! \equiv$ 14(mod 29). *Therefore* $2(26)! \equiv 28(\text{mod } 29)$. *Thus,* 28 *is the remainder.*

Problem 5.5.3. *Show that* $18! \equiv -1(\text{mod } 437)$.

Solution 5.5.3. *Note that* $437 = 19 \cdot 23$, *where both* 19 *and* 23 *are prime numbers. By Wilson's theorem, we have* $18! \equiv -1(\text{mod } 19)$ *therefore* $19|(18! +$ 1) *holds. So here the only thing we need to show is* $23|(18! + 1)$, *because* $\gcd(19, 23) = 1$. *Further by Wilson's theorem, we obtain* $22! \equiv -1(\text{mod } 23) \equiv 22($ mod 23) $\Rightarrow 21! \equiv 1(\text{mod } 23) \equiv 1 + 23 = 24(\text{mod } 23) \Rightarrow 7(20)! \equiv 8(\text{mod } 23) \Rightarrow$ $7 \cdot 5 \cdot 19! \equiv 2 \equiv 2 + 23 \equiv 25(\text{mod } 23) \Rightarrow 7 \cdot 19 \cdot 18! \equiv 5(\text{mod } 23) \equiv 5 + 23 = 28($ mod 23) $\Rightarrow 19 \cdot 18! \equiv 4(\text{mod } 23) \Rightarrow 19 \cdot 18! \equiv (4 - 23) = -19(\text{mod } 23) \Rightarrow 18! \equiv$ $-1(\text{mod } 23)$. *Therefore* $23\big|(18! + 1) \Rightarrow 437\big|(18! + 1)$.

Problem 5.5.4. *Prove that for* $n(> 1)$ *is prime if and only if* $(n-2)! \equiv 1($ mod $n)$.

Solution 5.5.4. *By Wilson's theorem and it's converse we have,* n *is prime if and only if* $(n-1)! \equiv -1(\text{mod } n)$. *Hence* $(n-1)! \equiv -1 + n = n - 1(\text{mod } n)$. *Therefore* $(n-2)! \equiv 1(\text{mod } n)$, *as* $\gcd(n, n-1) = 1$.

Problem 5.5.5. *If* n *is composite then show that* $(n-1)! \equiv 0(\text{mod } n)$ *except* $n = 4$.

Solution 5.5.5. *If* $n = 4$, *then* $(4-1)! = 3! = 6 \equiv 2(\text{mod } 4)$. *Thus this equivalence is not true for* $n = 4$. *If* $n > 4$ *is a composite number, then* $n = r \cdot s$ *for some integers* r *and* s. *Since* $\gcd(n, n-1) = 1$, *therefore* $1 < r < n-1$. *So* r *must be the one of the factor of* $(n-1)!$. *Similarly, for* $1 < s < n-1$ *the above argument is also true.*

If $r \neq s$, *then* r *and* s *are different factors of* $(n-1)!$. *So* $n = r \cdot s | (n-1)!$. *Therefore* $(n-1)! \equiv 0(\text{mod } n)$.

If $r = s$, *then* $n = r^2$. *Our claim is* $r < \frac{n}{2}$. *If not then,* $r \geq \frac{n}{2}$. *Therefore* $n = r^2 \geq \frac{n^2}{4} \Rightarrow 4 \geq n$. *But this is not true because* $n > 4$. *Hence* $r < \frac{n}{2} \Rightarrow 2r < n \Rightarrow 2r \leq n-1$. *Both* r *and* $2r$ *are factors of* $(n-1)!$, *therefore* $r(2r) \big| (n-1)! \Rightarrow r^2 \big| (n-1)!$. *Hence* $(n-1)! \equiv 0(\text{mod } n)$.

Problem 5.5.6. *Given a prime* p, *establish* $(p-1)! \equiv (p-1)(\text{mod } 1+2+3+\cdots+(p-1))$.

Solution 5.5.6. *An appeal to Wilson's theorem generates,* $(p-1)! \equiv -1 = p-1(\text{mod } p)$. *Therefore* $p|\{(p-1)! - (p-1)\}$. *We know that,* $1+2+3+\cdots+(p-1) = \frac{p(p-1)}{2}$. *Since* $p-1$ *is even, therefore* $\frac{(p-1)}{2}$ *is an integer and* $\frac{(p-1)}{2} < (p-1)$. *Furthermore,* $(p-1) \big| \{(p-1)! - (p-1)\} \Rightarrow \frac{(p-1)}{2} \big| \{(p-1)! - (p-1)\}$. *Because* $\gcd\left(\frac{(p-1)}{2}, p\right) = 1$, *therefore both* p *and* $\frac{(p-1)}{2}$ *divide* $\{(p-1)! - (p-1)\}$. *Thus* $\frac{p(p-1)}{2} \big| \{(p-1)! - (p-1)\} \Rightarrow (p-1)! \equiv (p-1)(\text{mod } 1+2+3\cdots+(p-1))$.

Problem 5.5.7. *If* p *is a prime prove that* $p \big| (a^p + (p-1)! \cdot a)$, *for any integer* a.

Solution 5.5.7. *Taking into consideration Euler's generalisation theorem and Wilson's theorem, we find* $a^p \equiv a(\text{mod } p)$ *and* $-1 \equiv (p-1)!(\text{mod } p)$ *hold respectively. Multiplying last two congruences, we have* $-a^p \equiv (p-1)! \cdot a(\text{mod } p)$. *This proves,* $p \big| (a^p + (p-1)! \cdot a)$.

Problem 5.5.8. *If* p *is a prime prove that* $p|((p-1)! \cdot a^p + a)$, *for any integer* a.

Solution 5.5.8. *Hint: Same as Problem(5.5.7)*

Problem 5.5.9. *Verify* $4(29!) + 5!$ *is divided by* 31.

Solution 5.5.9. *An appeal to Wilson's theorem gives,* $30! \equiv -1(\text{mod } 31)$. *Therefore* $30 \cdot 29! \equiv 31 - 1 = 30(\text{mod } 31) \Rightarrow 29! \equiv 1(\text{mod } 31)$. *Hence* $4(29)! \equiv 4(\text{mod } 31)$. *Thus, we have* $4(29!) + 5! \equiv 4 + 120 = 124(\text{mod } 31) \equiv 0(\text{mod } 31)$.

Problem 5.5.10. *Obtain the solution of* $x^2 \equiv -1(\text{mod } 29)$.

Solution 5.5.10. *As* $29 \equiv 1(\text{mod } 4)$ *so,* $\exists$ *a solution given by* $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1(\text{mod } p)$*[refer to Theorem 5.4.2]. Therefore* $\pm\left(\frac{29-1}{2}\right)! = \pm 14!$.

Problem 5.5.11. *Prove that the odd prime divisor of* n^2+1 *is of the form* $4k+1$.

Solution 5.5.11. *Let* p *be an odd prime divisor of* n^2+1. *Therefore* $n^2+1 \equiv 0(\text{mod } p)$. *So* n *satisfies the quadratic congruence equation* $x^2 \equiv -1(\text{mod } p)$. *Hence* p *is of the form* $4k+1$. *Because* p *is of the form* $4k+3$ *it follows that,* $n^2 \equiv -1(\text{mod } p) \Rightarrow 1 \equiv n^{p-1}(\text{mod } p) \equiv (n^2)^{\frac{p-1}{2}}(\text{mod } p) \equiv (-1)^{\frac{p-1}{2}}(\text{mod } p) \Rightarrow 1 \equiv (-1)^{\frac{4k+3-1}{2}}(\text{mod } p) \equiv (-1)^{2k+1}(\text{mod } p) \equiv -1(\text{mod } p)$. *This proves* $p \mid 2$, *a contradiction.*

5.6 Exercises:

1. Verify using Fermat's theorem: $17 \mid (11^{104}+1)$.
2. Find the remainder of 97! when divided by 101.
3. Derive the congruence: $a^{13} \equiv a(\text{mod } 3 \cdot 7 \cdot 13)$ for all integer a.
4. Find the remainder of 53! when divided by 61.
5. Prove $1835^{1910} + 1986^{2061} \equiv 0(\text{mod } 7)$.
6. Assume $p \nmid a, p \nmid b$, p is prime;
   - **(i)** If $a^p \equiv b^p(\text{mod } p)$ then, $a \equiv b(\text{mod } p)$.
   - **(ii)** If $a^p \equiv b^p(\text{mod } p)$ then, $a^p \equiv b^p(\text{mod } p^2)$.
7. Using Fermat's theorem, prove that for a odd prime p;
   - **(i)** $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1(\text{mod } p)$.
   - **(ii)** $1^p + 2^p + \cdots + (p-1)^p \equiv 0(\text{mod } p)$
8. Confirm that the followings are absolute prime: (a) $2821 = 7 \cdot 13 \cdot 31$ (b) $2465 = 5 \cdot 17 \cdot 29$.
9. Use Korselt's criterion to determine which of them are Charmichael numbers: (a) 8911 (b) 10659 (c) 162401 (d) 126217.
10. Find the remainder when 3^{456} is divided by 7.
11. Find all positive integers n such that 2^{2^n+1} is divided by 17.

12. Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 17$.

13. Determine whether 17 is a prime or not using Wilson's theorem.

14. If p and $p+2$ are a pair of primes then prove that $4((p-1)! + 1) + p \equiv 0($ mod $p(p+2))$.

15. What is the remainder of 149! when divided by 139.

16. Find all Carmichael numbers of the form $5pq$ where p and q are primes.

17. Find a Carmichael number of the form $7 \cdot 23 \cdot q$ where q is an odd prime.

18. Show that 1373653 is a strong pseudoprime to base 2, 3.

19. Obtain the solution of $x^2 \equiv -1 (\text{mod } 37)$.

We give an account of the most important results obtained by Euler in number theory.

7.2 Euler's ϕ–function

The chapter, Fermat's little theorem addresses the congruence relation with a prime number. Now the question arises: Can we change the prime number by an arbitrary positive integer? The answer is in an affirmative sense and Euler's generalization is the important result which leads to that answer. Before going to this significant result we need to introduce an important arithmetic function called Euler's ϕ–function or Euler's totient function. To meet the purpose, first let us define this special type of function.

Definition 7.2.1. *For any positive integer n with $n \geq 1$, Euler's phi functionor Euler's totient function denoted as $\phi(n)$ and defined as the number of positive integers not exceeding n and relatively prime to n.*

Let us illustrate the above definition by some example, for which we displayed below a table of positive integers n and corresponding $\phi(n)$.

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

From the above table, it is clear that $\phi(1) = 1$ and $\phi(p) = p - 1$ for any prime p. Also, the converse with respect to second equality is true, *i.e.* if for any positive integer n, $\phi(n) = n-1$ holds then n is prime. Our next proposition directs us to ensure the proof of this statement.

Proposition 7.2.1. *If p is a prime then $\phi(p) = p - 1$ holds and vice versa.*

Proof. If p is a prime, from the definition of ϕ-function, the number of integers which are less than p and prime to p is $p-1$. Thus, $\phi(p) = p-1$ for every prime p.

Conversely, let p be composite. Then it has a divisor q with $1 < q < p$ and $\gcd(p, q) \neq 1$. Now q belongs to the set $\{1, 2, 3, \cdots p - 1\}$ and q not relatively prime to p implies $\phi(p) \leq p-2$. Hence if $\phi(p) = p-1$ then p must be prime. □

The first important agenda of this section is, for any arbitrary positive integer n what should be $\phi(n)$ when the prime factorisation of n is known. The next few results of this section helps us to reach that platform from where we can find $\phi(n)$ for any arbitrary positive integer n.

Theorem 7.2.1. *If p is prime and $\alpha > 0$, then $\phi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right)$.*

Proof. Here we need to find those positive integers for which $\gcd(n, p^\alpha) = 1$ that is $p \nmid n$. Now given below the arrangement of those positive integers not greater than p^α. The arrangement is a rectangular array containing p columns and $p^{\alpha-1}$ rows:

$$\begin{array}{cccc} 1 & 2 & \cdots & p \\ p+1 & p+2 & \cdots & 2p \\ \vdots & \vdots & \vdots & \vdots \\ p^\alpha - p + 1 & p^\alpha - p + 2 & \cdots & p^\alpha \end{array}$$

and there are $p^{\alpha-1}$ integers between 1 and p^α which are divisible by p, namely

$$p, 2p, 3p, \ldots, p^{\alpha-1}.$$

p lies in rightmost column of the above array. Thus there are exactly $p^\alpha - p^{\alpha-1}$ integers which are relatively prime to p^α and so by definition of the ϕ–function, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$. □

To understand the above theorem lucidly by means of an example, let us choose $p = 2$ and $\alpha = 3$. Now using the table we have:

$$\begin{array}{cc} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{array}$$

Only the elements of the right sided column divides 2^3. Thus $\phi(2^3) = \phi(8)$ is the number of elements of the set $\{1, 3, 5, 7\}$ which is $4 = 2^{3-1}(2-1)$. We are now in the stage to find the phi function for prime powers. But still a question arises, whether it is possible to find the phi function of any positive integer directly whose prime factorization is given using the above theorem. The answer of this statement is in the affirmative sense but for that we have to check the multiplicative property of this arithmetic function ϕ. The next part of the present section deals with this fact.

Now we are in the position to state and prove the following theorem.

Theorem 7.2.2. *The function ϕ is a multiplicative function.*

Proof. It suffices to show that $\phi(mn) = \phi(m)\phi(n)$, where $\gcd(m, n) = 1$. If any one of m, n is 1, the result is true(Why!). Thus we may assume $m > 1, n > 1$. We arrange the integers from 1 to mn into $m \times n$ order array as follows:

$$\begin{array}{ccccccc} 1 & 2 & \cdots & r & \cdots & m \\ m+1 & m+2 & \cdots & m+r & \cdots & 2m \\ 2m+1 & 2m+2 & \cdots & 2m+r & \cdots & 3m \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & mn \end{array}$$

We know that there are $\phi(mn)$ entries of the above array which are prime to mn(Why!) and this is same as the number of integers relatively prime to both m and n(refer to problem(2.6.1)). Now $\gcd(qm+r, m) = \gcd(r, m)$, so the numbers in $r-$th column are relatively prime to m if and only if $\gcd(r, m) = 1$. Thus there are only $\phi(m)$ columns containing integers relatively prime to m. Here every entry of that $\phi(m)$ columns are relatively prime to m. Now to show each of these $\phi(m)$ columns there are $\phi(n)$ integers which are relatively prime to n. In the entries of r-th column there are n integers $r, m+r, \ldots, (n-1)m+r$ no two of which are congruent modulo n. If it happens, let $(im+r) \equiv (jm+r)(\mod n)(0 \leq i < j < n)$. Therefore $im \equiv jm(\mod n)$ implies $i \equiv j(\mod n)$ as $\gcd(m, n) = 1$, which leads to a contradiction. Thus the numbers in the r-th column are congruent modulo n to $0, 1, 2, \cdots, n-1$, in some order. If $s \equiv t(\mod n)$ for some integer s and t then $\gcd(s, n) = 1$ if and only if $\gcd(t, n) = 1$. Thus r-th column contains as many integers, which are relatively prime to n, as does the set $\{0, 1, 2, \ldots, n-1\}$, namely $\phi(n)$. Therefore the total number of entries in the array that are relatively prime to both m, n is $\phi(m)\phi(n)$. □

Finally, we are in the position to find the phi-function for any arbitrary positive integer.

Theorem 7.2.3. *If the integer $n > 1$ has a prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then $\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.*

Proof. Since ϕ is multiplicative(Why!) and n has a prime factorization, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ then we have

$$\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_r^{\alpha_r}).$$

Again from the Theorem 7.2.1, we have $\phi(p_j^{\alpha_j}) = (p_j^{\alpha_j} - p_j^{\alpha_j - 1})$ for each

$j = 1, 2, 3, \cdots, r$. Hence

$$\begin{aligned}\phi(n) &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

□

The exemplification of the above theorem has been done from the following example:

Example 7.2.1. *Choose $n = 720$. Then the prime factorization of 720 is $2^4 \cdot 3^2 \cdot 5$. Thus applying above theorem, we have*

$$\begin{aligned}\phi(360) &= 720 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right), \\ &= 720 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}, \\ &= 192.\end{aligned}$$

At the outset of this section, a table of positive integers and their corresponding phi-function, was displayed. There, $\phi(1) = \phi(2) = 1$ and the values of phi function for other integers are even. This is not a coincidence, as evident from our next theorem:

Theorem 7.2.4. *For $n > 2$, $\phi(n)$ is an even integer.*

Proof. Let us consider $n = 2^j$ with $j \geq 2$. Then from Theorem 7.2.1, $\phi(n) = \phi(2^j) = 2^{j-1}$, an even integer. If n is not a power of 2 then it is divisible by some odd prime. Then $n = p^j m$, where p being an odd integer and $\gcd(p, m) = 1$. Therefore $\phi(n) = \phi(p^j)\phi(m)(Why!) = p^{j-1}\phi(m)(p-1)$, which is also even(Why!). □

7.3 Worked out Exercises

Problem 7.3.1. *Verify that the equality $\phi(z) = \phi(z+1) = \phi(z+2)$ holds, when $z = 5186$.*

Solution 7.3.1. *Note that*

$$5186 = 2 \cdot 2593,\ \phi(5186) = 5186\left(\frac{1}{2}\right)\left(\frac{2592}{2593}\right) = 2592.$$

$$5187 = 3 \cdot 7 \cdot 13 \cdot 19,\ \phi(5187) = 5187\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)\left(\frac{12}{13}\right)\left(\frac{18}{19}\right) = 2592.$$

$$5188 = 2^2 \cdot 1297,\ \phi(5188) = 5188\left(\frac{1}{2}\right)\left(\frac{1296}{1297}\right) = 2592.$$

Problem 7.3.2. *Prove: For some $k \geq 1$, $\phi(z) = \dfrac{z}{2}$ if and only if $z = 2^k$.*

Solution 7.3.2. *Let us consider $z = 2^k$. Then $\phi(z) = \phi(2^k) = 2^k\left(1 - \dfrac{1}{2}\right) = 2^{k-1} = \dfrac{z}{2}$.*

Conversely, suppose $\phi(z) = \dfrac{z}{2}$. Then for $\dfrac{z}{2}$ to be an integer, z must be even. Let $z = 2^k p_2^{k_2} \cdots p_r^{k_r}$ and assume $k_i \neq 0$. Let $q = p_2^{k_2} \cdots p_r^{k_r}$. So $q > 1$ and $\gcd(2^k, q) = 1$.

$$\begin{aligned}
\therefore\ \phi(z) &= \phi(2^k q) = \phi(2^k)\phi(q), \\
&= 2^k\left(1 - \frac{1}{2}\right)\phi(q) = 2^{k-1}\phi(q). \\
\textit{Further } \frac{z}{2} &= \phi(z) = 2^{k-1}\phi(q) \Rightarrow z = 2^k\phi(q). \\
\therefore\ p_2^{k_2} \cdots p_r^{k_r} &= \phi(q) = \phi(p_2^{k_2} \cdots p_r^{k_r}) \\
&= p_2^{k_2} \cdots p_r^{k_r}\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right). \\
\therefore\ p_2 \cdots p_r &= (p_2 - 1) \cdots (p_r - 1).
\end{aligned}$$

Therefore for each $p_i, p_i = (p_j - 1)$ for some j. This is impossible if $k_i \neq 0$. Hence $k_i = 0$. Thus the converse part follows.

Problem 7.3.3. *Prove that the equation $\phi(z) = \phi(z + 2)$ is satisfied by $z = 2(2p - 1)$ whenever p and $2p - 1$ are both odd primes.*

Solution 7.3.3. *Here $2p - 1$ is an odd prime implies* $\gcd(2, 2p - 1) = 1$.

$$\therefore\ \phi(z) = \phi(2)\phi(2p - 1) = (2p - 1)\left(1 - \frac{1}{2p - 1}\right) = 2p - 2.$$

Now $z + 2 = 2(2p - 1) + 2 = 4p$, p being an odd prime, yields $\gcd(4, p) = 1$.

$$\therefore\ \phi(z + 2) = \phi(4)\phi(p) = 2p\left(1 - \frac{1}{p}\right) = 2p - 2.$$

$$\therefore\ \phi(z) = \phi(z + 2).$$

Problem 7.3.4. *Show that there are infinitely many integers n for which $\phi(n)$ is a perfect square.*

Solution 7.3.4. *For $k \geq 1$, $\phi(2^k) = 2^k\left(1-\frac{1}{2}\right) = 2^{k-1}$. If k is odd, then $k-1$ is even. Let $k = 2m+1$, for some $m \in \mathbb{Z}$.*

$$\therefore\ \phi(2^k) = \phi(2^{2m+1}) = (2^m)^2 = \text{a perfect square.}$$

Thus there are infinitely many $n = 2^k$, k being odd, and $\phi(n)$ is a perfect square.

Problem 7.3.5. *Prove that if the integer n has s distinct odd prime factors, then $2^s \big| \phi(n)$.*

Solution 7.3.5. *Let $n = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$, $p_i > 2$.*

$$\therefore\ \phi(n) = p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\cdots p_s^{k_s-1}(p_s-1).$$

As each p_i is odd, so let $p_i = 2r_i + 1$ for some r_i.

$$\begin{aligned}\therefore\ \phi(n) &= p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\cdots p_s^{k_s-1}(p_s-1)(2r_1)(2r_2)\cdots(2r_s),\\ &= 2^s p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\cdots p_s^{k_s-1}(p_s-1)r_1r_2\cdots r_s.\\ \therefore\ 2^s &\big| \phi(n).\end{aligned}$$

Problem 7.3.6. *If every prime that divides n also divides m, prove that $\phi(nm) = n\phi(m)$.*

Solution 7.3.6. *Let $p_1, p_2, \ldots, p_s$ be all those primes which divide both n and m. Suppose*

$n = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$, $m = p_1^{j_1}p_2^{j_2}\cdots p_s^{j_s}q_1^{m_1}q_2^{m_2}\cdots q_r^{m_r}$, q_i being prime be such that $q_i \neq p_j$.

$$\begin{aligned}\therefore\ nm &= p_1^{k_1+j_1}p_2^{k_2+j_2}\cdots p_s^{k_s+j_s}q_1^{m_1}q_2^{m_2}\cdots q_r^{m_r}.\\ \therefore\ \phi(nm) &= p_1^{k_1+j_1}p_2^{k_2+j_2}\cdots p_s^{k_s+j_s}q_1^{m_1}q_2^{m_2}\cdots q_r^{m_r}\\ &\qquad\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_r}\right),\\ &= p_1^{j_1}p_2^{j_2}\cdots p_s^{j_s}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_r}\right)p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s},\\ &= \phi(m)p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s},\\ &= n\cdot\phi(m).\end{aligned}$$

Problem 7.3.7. *If $\phi(n)|(n-1)$, prove that n is a square-free integer.*

Solution 7.3.7. *Let* $n = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$ *and suppose* n *is not square-free such that* $k_i \geq 2$ *for some* i. *Now*

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})\cdots(p_i^{k_i} - p_i^{k_i-1})\cdots(p_s^{k_s} - p_s^{k_s-1}).$$

Since $k_i \geq 2,\ k_i - 1 \geq 1$, *so* $p_i \big| (p_i^{k_i} - p_i^{k_i-1}) \Rightarrow p_i \big| \phi(n)$. *By hypothesis* $\phi(n) \big| (n-1)$ *implies* $p_i \big| (n-1)$. *Again* $p_i \big| n$ *yields* $p_i \big| n - (n-1) \Rightarrow p_i \big| 1$, *which is a contradiction. Therefore for all* i, $k_i = 1$ *implies* n *is square-free.*

Problem 7.3.8. *Prove that there are no integers* n *for which* $\phi(n) = \dfrac{n}{4}$.

Solution 7.3.8. *Here* $\phi(1) = 1 = \phi(2), \phi(3) = 2 = \phi(4)$. *So the statement holds true for* $n = 1, 2, 3, 4$. *Let* $n > 4$. *On the contrary, suppose* $\phi(n) = \dfrac{n}{4}$. *Let* $n = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}, k_i \geq 1$.

$$\begin{aligned}
\therefore\ \phi(n) &= n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_s}\right) = \frac{n}{4}, \\
&\Rightarrow \frac{(p_1 - 1)(p_2 - 1)\cdots(p_s - 1)}{p_1p_2\cdots p_s} = \frac{1}{4}, \\
&\Rightarrow 4(p_1 - 1)(p_2 - 1)\cdots(p_s - 1) = p_1p_2\cdots p_s, \\
&\Rightarrow 2(p_2 - 1)\cdots(p_s - 1) = p_2\cdots p_s,\ \textit{as}\ p_1 = 2.
\end{aligned}$$

Since $p_2, \ldots, p_s$ *are all odd, therefore* $p_2\cdots p_s$ *is odd. But* $2(p_2 - 1)\cdots(p_s - 1)$ *is even. So* $p_1 = 2$ *fails to work. Now if all* $p_1, p_2, \ldots, p_s$ *are odd, then* $p_1p_2\cdots p_s$ *is also so. Furthermore* $4(p_1 - 1)(p_2 - 1)\cdots(p_s - 1)$ *is even, which implies no such* n *exists.*

Problem 7.3.9. *If* p *is a prime and* $k \geq 2$, *show that* $\phi(\phi(p^k)) = p^{k-2}\phi((p-1)^2)$.

Solution 7.3.9. *Here* $\phi(p^k) = p^{k-1}(p-1)$. *Since* $\gcd(p, p-1) = 1$, *therefore* $\gcd(p^{k-1}, p-1) = 1$. *Using the multiplicative property of* ϕ, *we obtain*

$$\phi(\phi(p^k)) = \phi(p^{k-1}(p-1)) = \phi(p^{k-1})\phi(p-1) = p^{k-2}(p-1)\phi(p-1).$$

Now for every positive integer n, $\phi(n^2) = n\phi(n)$. *Therefore* $(p-1)\phi(p-1) = \phi((p-1)^2)$. *Hence* $\phi(\phi(p^k)) = p^{k-2}(p-1)\phi(p-1) = p^{k-2}\phi((p-1)^2)$.

Problem 7.3.10. *If* $n = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$, *then prove that*

$$\sigma(n)\phi(n) \geq n^2\left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right)\cdots\left(1 - \frac{1}{p_s^2}\right).$$

Solution 7.3.10. *Note that* $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdots \frac{p_s^{k_s+1}-1}{p_s-1}$ *and* $\phi(n) = p_1^{k_1-1}(p_1 - 1)\cdots p_s^{k_s-1}(p_s-1)$. *Therefore* $\sigma(n)\phi(n) = (p_1^{2k_1} - p_1^{k_1-1})\cdots(p_s^{2k_s} - p_s^{k_s-1})$. *But* $(p_j^{2k_j} - p_j^{k_j-1}) = p_j^{2k_j}\left(1 - \frac{p_j^{k_j-1}}{p_j^{2k_j}}\right) = (p_j^{k_j})^2\left(1 - \frac{1}{p_j^{k_j+1}}\right)$. *For* $p_j \geq 1$ *we find*

$$p_j^{k_j+1} \geq p_j^2 \Rightarrow \frac{1}{p_j^2} \geq \frac{1}{p_j^{k_j+1}} \Rightarrow -\frac{1}{p_j^2} \leq -\frac{1}{p_j^{k_j+1}} \Rightarrow 1 - \frac{1}{p_j^2} \leq 1 - \frac{1}{p_j^{k_j+1}}.$$

$$\therefore\ p_j^{2k_j} - p_j^{k_j-1} \geq (p_j^{k_j})^2\left(1 - \frac{1}{p_j^2}\right).$$

$$\therefore\ \sigma(n)\phi(n) \geq \prod_s (p_s^{k_s})^2\left(1 - \frac{1}{p_s^2}\right),$$

$$= \prod_s (p_s^{k_s})^2 \prod_s \left(1 - \frac{1}{p_s^2}\right),$$

$$= n^2\left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right)\cdots\left(1 - \frac{1}{p_s^2}\right).$$

7.4 Euler's Theorem

The first published proof of Fermat's little theorem(stated in chapter 5 of this book) was given by Euler in 1736, where he had taken a prime p and an integer a. But later in the year, 1760 he succeeded in generalizing the result from prime p to an arbitrary integer n. This generalization is known as Euler's generalization of Fermat's theorem. The present section deals with the proof and related ideas associated with this remarkable theorem.

Now, as a precursor to launch the proof of Euler's generalization of Fermat's theorem, we need the following lemma:

Lemma 7.4.1. *Let* $n > 1$ *and* $\gcd(a, n) = 1$. *If* $k_1, k_2, \cdots, k_{\phi(n)}$ *are the positive integers less than and prime to* n, *then* $ak_1, ak_2, \cdots, ak_{\phi(n)}$ *are congruent modulo* n *to* $k_1, k_2, \cdots, k_{\phi(n)}$ *in some order.*

Proof. Here we are going to show that no two of the integers $ak_1, ak_2, \cdots, ak_{\phi(n)}$ are congruent modulo n. For if, $ak_i \equiv ak_j \pmod{n}$ holds with $1 \leq i < j \leq \phi(n)$ then $k_i \equiv k_j \pmod{n}$, which is a contradiction since this two integers are less than n. Since, $\gcd(k_i, n) = 1\ \forall i$ and $\gcd(a, n) = 1$ then from the worked out Problem 2.6.1) $\gcd(ak_i, n) = 1\ \forall i$. Let us fix ak_j for some integer j, there exists unique integer b where $0 \leq b < n$ for which $ak_j \equiv b \pmod{n}$. Since, $\gcd(b, n) = \gcd(ak_j, n) = 1$, so b must be one of the integers $k_1, k_2, \cdots, k_{\phi(n)}$.

This is true for all j. This proves that the numbers $ak_1, ak_2, \cdots, ak_{\phi(n)}$ and the numbers $k_1, k_2, \cdots, k_{\phi(n)}$ are identical with respect to modulo n in a certain order. □

We now represent an example to make a lucid understanding of this lemma. For that let us take $n = 9$ and the set $\{1, 2, 4, 5, 7, 8\}$ is a reduce system modulo 9. Since $\gcd(2, 9) = 1$ then we have, $2 \cdot 1 = 2, 2 \cdot 2 = 4, 2 \cdot 4 = 8, 2 \cdot 5 = 10, 2 \cdot 7 = 14, 2 \cdot 8 = 16$ is also a reduce system modulo 9.

Theorem 7.4.1. *(Euler): If n is a positive integer and $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 (\mod n)$.*

Now before going to the proof, we illustrate the idea of it by an example.

Example 7.4.1. *From the last example, it is clear that both the sets $\{1, 2, 4, 5, 7, 8\}$ and $\{2\cdot1, 2\cdot2, 2\cdot4, 2\cdot5, 2\cdot7, 2\cdot8\}$ are reduced residue system of modulo 9. Therefore*

$$(2 \cdot 1)(2 \cdot 2)(2 \cdot 4)(2 \cdot 5)(2 \cdot 7)(2 \cdot 8) \equiv 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 (\mod 9),$$
$$2^6 \cdot 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \equiv 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 (\mod 9).$$

Since we have $\gcd(1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8, 9) = 1$, we conclude that $2^6 = 2^{\phi(9)} \equiv 1 (\mod 9)$.

We now use the idea of this example to the following proof.

Proof. Let us take $n > 1$ and $k_1, k_2, \cdots, k_{\phi(n)}$ be the positive integers less than n which are relatively prime to n. Since $\gcd(a, n) = 1$, $ak_1, ak_2, \cdots, ak_{\phi(n)}$ are congruent to $k_1, k_2, \cdots, k_{\phi(n)}$ (Why!). Then the least positive residue of $ak_1, ak_2, \cdots, ak_{\phi(n)}$ are the integers $k_1, k_2, \cdots, k_{\phi(n)}$ in some order. Therefore

$$(ak_1)(ak_2)\cdots(ak_{\phi(n)}) \equiv k_1 k_2 \cdots k_{\phi(n)} (\mod n)$$
$$\text{and so } a^{\phi(n)} k_1 k_2 \cdots k_{\phi(n)} \equiv k_1 k_2 \cdots k_{\phi(n)} (\mod n).$$

Since $\gcd(k_i, n) = 1$ for each i so $\gcd(k_1 k_2 \cdots k_{\phi(n)}, n) = 1$[see Problem 2.6.1]. Thus the congruence becomes $a^{\phi(n)} \equiv 1 (\mod n)$. □

Remark 7.4.1. *If $n = p$ is prime, then $\phi(p) = p - 1$. Further if $p \nmid a$, then we have $a^{p-1} \equiv 1 (\mod p)$, which is equivalent to Fermat's Little theorem.*

Euler's theorem has vast application in finding the modulo of a large number with respect to a positive integer. Applying Euler's theorem, we can find congruent modulo of 4^{301} with respect to 99. Since $\gcd(4, 99) = 1$ and $\phi(99) = \phi(3^2 \cdot 11) = 99\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right) = 99 \times \frac{2}{3} \times \frac{10}{11} = 60$, from Euler's theorem we have $4^{60} \equiv 1 (\mod 99)$. Now $301 = 5 \cdot 60 + 1$, therefore $4^{301} \equiv (4^{60})^5 \cdot 4^1 \equiv 4 (\mod 99)$.

7.5 Worked out Exercises

Problem 7.5.1. *Use Euler's theorem to evaluate* 2^{100000} *modulo* 77.

Solution 7.5.1. *Here* $\gcd(2,77)=1$, *therefore* $2^{\phi(77)} \equiv 1 (\mathrm{mod}\ 77)$. *Now*

$$\phi(77) = 6 \cdot 10 = 60 \Rightarrow 2^{60} \equiv 1(\ \mathrm{mod}\ 77).$$

Hence

$$2^{60000} \equiv 1(\ \mathrm{mod}\ 77),\ (2^{60})^{300} = 2^{18000} \equiv 1(\ \mathrm{mod}\ 77) \Rightarrow 2^{36000} \equiv 1(\ \mathrm{mod}\ 77).$$
$$\therefore\ 2^{96000} \equiv 1(\ \mathrm{mod}\ 77),\ (2^{60})^{300} = 2^{1800} \equiv 1(\ \mathrm{mod}\ 77) \Rightarrow 2^{3600} \equiv 1(\ \mathrm{mod}\ 77).$$
$$\therefore\ 2^{99600} \equiv 1(\ \mathrm{mod}\ 77),\ (2^{60})^{3} = 2^{180} \equiv 1(\ \mathrm{mod}\ 77) \Rightarrow 2^{360} \equiv 1(\ \mathrm{mod}\ 77).$$
$$\therefore\ 2^{99960} \equiv 1(\ \mathrm{mod}\ 77).$$

But $2^{10} = 1024,\ 13 \cdot 77 = 1001 \Rightarrow 2^{10} \equiv 23(\mathrm{mod}\ 77)$. *Therefore* $2^{40} \equiv 23^4(\ \mathrm{mod}\ 77) \Rightarrow 2^{100000} \equiv 23^4(\mathrm{mod}\ 77)$. *Now* $23^2 = 529 = 6 \cdot 77 + 67 \Rightarrow 23^2 \equiv -10(\ \mathrm{mod}\ 77) \Rightarrow 23^4 \equiv 100 \equiv 23(\mathrm{mod}\ 77)$. *Hence*

$$2^{100000} \equiv 23(\ \mathrm{mod}\ 77).$$

Problem 7.5.2. *For any prime* p, *prove that:*

$$\tau(p!) = 2\tau((p-1)!).$$

Solution 7.5.2. *Let* $p! = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \cdot p = 1 \cdot 2 \cdot 3 \cdots (p-1) \cdot p$ *and* $p_1, p_2, \cdots p_s$ *be distinct primes. Here* $k_i \geq 0$ *are the integers for each* $i(= 1, 2, \cdots s)$. *Therefore* $(p-1)! = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. *Since* $\gcd(p, p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) = 1$, *therefore*

$$\begin{aligned}\tau(p!) &= \tau(p \cdot p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) \\ &= \tau(p)\tau(p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) \\ &= \tau(p)\tau((p-1)!) \\ &= 2 \cdot \tau((p-1)!),\ \because\ \tau(p) = 2.\end{aligned}$$

Problem 7.5.3. *If* $\gcd(a,n) = 1$, *show that the linear congruence* $ax \equiv b(\ \mathrm{mod}\ n)$ *has the solution* $x \equiv ba^{\phi(n)-1}(\mathrm{mod}\ n)$.

Solution 7.5.3. *If* $x \equiv ba^{\phi(n)-1}(\mathrm{mod}\ n)$, *then* $ax = a(ba^{\phi(n)-1}) = ba^{\phi(n)}$. *Since* $\gcd(a,n) = 1$, *by Euler's theorem we have* $a^{\phi(n)} \equiv 1(\mathrm{mod}\ n)$.

$$\therefore\ ax = ba^{\phi(n)} \equiv b \cdot 1 \equiv b(\ \mathrm{mod}\ n).$$

Problem 7.5.4. *Show that if* $\gcd(a,n) = gcd(a-1,n) = 1$, *then*

$$1 + a + a^2 + \ldots + a^{\phi(n)-1} \equiv 0(\ \mathrm{mod}\ n).$$

Solution 7.5.4. *By Euler's theorem, we have*

$$\gcd(a,n)=1 \Rightarrow a^{\phi(n)} \equiv 1(\mod n) \Rightarrow a^{\phi(n)}-1 \equiv 0(\mod n).$$

But $a^{\phi(n)}-1=(a-1)(a^{\phi(n)-1}+\ldots+a^2+a+1)$. *Therefore* $(a-1)(a^{\phi(n)-1}+\ldots+a^2+a+1)\equiv 0(\mod n)$. *Since* $\gcd(a-1,n)=1$, *therefore* $1+a+a^2+\ldots+a^{\phi(n)-1}\equiv 0(\mod n)$.

Problem 7.5.5. *If m and n are relatively prime positive integers, prove that* $m^{\phi(n)}+n^{\phi(m)}\equiv 1(\mod mn)$.

Solution 7.5.5. *Since* $\gcd(m,n)=1$, *therefore an appeal to Euler's theorem produces*

$$m^{\phi(n)} \equiv 1(\mod n) \ \& \ n^{\phi(m)} \equiv 1(\mod m).$$

But $n^{\phi(m)} \equiv 0(\mod n)$ & $m^{\phi(n)} \equiv 0(\mod m)$.

$$\begin{aligned} \therefore\ m^{\phi(n)}+n^{\phi(m)} &\equiv 1+0=1(\mod n),\\ n^{\phi(m)}+m^{\phi(n)} &\equiv 1+0=1(\mod m). \end{aligned}$$

Since $\gcd(m,n)=1$, *therefore combining we obtain* $m^{\phi(n)}+n^{\phi(m)}\equiv 1(\mod mn)$.

Problem 7.5.6. *Find the units digit of* 3^{100} *by means of Euler's theorem.*

Solution 7.5.6. *Here* $\gcd(10,3)=1$. *By Euler's theorem,* $3^{\phi(10)}\equiv 1(\mod 10)$. *Now,* $\phi(10)=4$, *therefore* $3^4\equiv 1(\mod 10)$. *Hence* $(3^4)^{25}\equiv 1(\mod 10)$. *Therefore* $3^{100}\equiv 1(\mod 10)$. *Thus, unit digit of* 3^{100} *is* 1.

Problem 7.5.7. *Prove that* $a^{15}\equiv a^3(\mod (2^{15}-2^3))$ *for any integer* a.

Solution 7.5.7. *Here,*

$$\begin{aligned} a^{15}-a^3 &= a^3(a^{12}-1)=a^3(a^6+1)(a^6-1)\\ &= a^3(a^6+1)((a^3+1))(a^3-1)\\ &= a^3(a^6+1)((a^3+1))(a^2+a+1)(a-1).\\ 2^{15}-2^3 &= 2^3(2^6+1)((2^3+1))(2^2+2+1)(2-1)\\ &= 2^3\cdot 3^2\cdot 5\cdot 7\cdot 13. \end{aligned}$$

Applying the definition of Euler's phi function we get,

$$\phi(8)=4,\phi(5)=4,\phi(13)=12,\phi(9)=6,\phi(7)=6.$$

Case(i) *If* $\gcd(a,2^{15}-2^3)=1$, *then this implies,*

$$\gcd(a,8)=1, \qquad \gcd(a,13)=1, \qquad \gcd(a,2)=1,$$

$$\gcd(a,5)=1, \qquad \gcd(a,9)=1.$$

Now applying Euler's theorem in all those above cases we can write,

$$a^4 \equiv 1(\mod 8), \qquad a^{12} \equiv 1(\mod 13), \qquad a^6 \equiv 1(\mod 7),$$

$$a^4 \equiv 1(\mod 5), \qquad a^6 \equiv 1(\mod 9).$$

Considering all the congruences together, we have

$$a^{12} \equiv 1(\mod 8\cdot 5\cdot 13\cdot 9\cdot 7).$$

$$\therefore\ a^{15} \equiv a^3(\mod (2^{15}-2^3)).$$

Case(ii) *If* $\gcd(a, 2^{15}-2^3) \neq 1$, *then for some integer* k,

$$a = k(2^{15}-2^3),\ \textit{and}$$

$a^{15}-a^3 = (a^{14}-a^2)a = (a^{14}-a^2)k(2^{15}-2^3) \Rightarrow a^{15} \equiv a^3(\mod (2^{15}-2^3))$.

Hence combining both the cases for any integer a, *we get* $a^{15} \equiv a^3(\mod (2^{15}-2^3))$.

Problem 7.5.8. *Use Euler's theorem to confirm that, for any integer* $z \geq 0,\ 51|10^{32z+9}-7$.

Solution 7.5.8. *Here,* $51 = 17\cdot 3$. *Therefore* $\phi(51) = 16\cdot 2 = 32$. *Also,* $\gcd(10,51)=1$ *gives* $10^{\phi(51)} = 10^{32} \equiv 1(\mod 51)$. *Thus,*

$$10^{32z} \equiv 1(\mod 51). \tag{7.5.1}$$

Next, we are going to show $10^9 \equiv 7(\mod 51)$. *Now,*

$$10 \equiv 7(\mod 3),$$

$$10 \equiv 1(\mod 3) \Rightarrow 10^{18} \equiv 1(\mod 3).$$

$$\therefore\ 10^9 = 10^8\cdot 10 \equiv 7\cdot 1(\mod 3),$$

$$\textit{or, } 10^9 \equiv 7(\mod 3). \tag{7.5.2}$$

$$-10 \equiv 7(\mod 17),$$

$$\therefore\ (-10)^2 \equiv 7^2 = 49 \equiv -2(\mod 17).$$

$$\therefore\ (-10)^8 = 10^8 \equiv (-2)^4 = 16 \equiv -1(\mod 17).$$

$$\therefore\ (-10)^9 \equiv -10 \equiv 7(\mod 17). \tag{7.5.3}$$

$$(7.5.2)+(7.5.3) \Rightarrow 10^9 \equiv 7(\mod 51). \tag{7.5.4}$$

$$(7.5.1)+(7.5.4) \Rightarrow 10^{32z}\cdot 10^9 \equiv 1\cdot 7(\mod 51),$$

$$10^{32z+9} \equiv 7(\mod 51). \tag{7.5.5}$$

Thus, for any integer $z \geq 0,\ 51|10^{32z+9}-7$.

Problem 7.5.9. *Prove that if a is an integer, then $a^7 \equiv a(\mathrm{mod}\ 63)$.*

Solution 7.5.9. *From Fermat's little theorem we see that, $a^7 \equiv a(\mathrm{mod}\ 7)$. So to prove this assertion we need to check $a^7 \equiv a(\mathrm{mod}\ 9)$. If $9|a$ then it is trivial. If $3 \nmid a$ then $\gcd(a, 9) = 1$, so from Euler's theorem it follows that $a^{\phi(9)} = a^6 \equiv 1(\mathrm{mod}\ 9)$ or $a^7 \equiv a(\mathrm{mod}\ 9)$. Thus together we have $a^7 \equiv a(\mathrm{mod}\ 63)$.*

Problem 7.5.10. *Solve the linear congruence $5x \equiv 3(\mathrm{mod}\ 14)$ by Euler's theorem.*

Solution 7.5.10. *Here we multiply both sides of the congruence by $5^{\phi(14)-1} = 5^5$. This gives $5^6 \cdot x \equiv 3 \cdot 5^5(\mathrm{mod}\ 14)$. Now by Euler's theorem we have $5^{\phi(14)} = 5^6 \equiv 1(\mathrm{mod}\ 14)$. This implies, $x \equiv 3 \cdot 5^5 \equiv 15 \cdot 11^{11} \equiv 15 \cdot 9 \equiv 9(\mathrm{mod}\ 14)$.*

7.6 Properties of ϕ–function

Present section deals with some curious properties of Euler's phi function related with some arithmetic functions. Discussion of this chapter commence with an important property of totient(ϕ) function, where the sum of values of $\phi(d)$ where d is the divisor of any positive integer n is always equal to n itself. Famous German mathematician Carl Friedrich Gauss was the first person to notice that.

Theorem 7.6.1. *For each positive integer $n \geq 1, n = \sum_{d|n} \phi(d)$ where d is positive divisor of n.*

Proof. Let us choose $n = 1$ then, $\sum_{d|1} \phi(d) = \phi(1) = 1 = n$. Thus the equality is true in this case. Now we are only to prove the result for any positive integer $n > 1$. Let us choose a set $S_n = \{1, 2, 3, \cdots, n\}$ and $|S_n|$ be the number of elements in S_n, then clearly $|S_n| = n$. For each divisor d of n we denote S_d be the set of all integers not exceeding n and $\gcd(m, n) = d$ for each $m \in S_d$. Now from the proposition (2.4.2) we have $\gcd(m, n) = d$ if and only if $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. We now have to show that each S_d has $\phi\left(\frac{n}{d}\right)$ number of elements. Here for a particular d all the elements of S_d are multiples of d and less than or equal to n. Thus the elements of S_d are $d, 2d, 3d, \cdots, \left(\frac{n}{d}\right)d$. Now, let $ad \in S_d$ be any element where $\gcd\left(a, \frac{n}{d}\right) = e$. Then clearly $\gcd(ad, n) = ed$. Here $ed = d$ if and only if $e = 1$ imply that only ad in S_d are those whose $\gcd\left(a, \frac{n}{d}\right) = 1$ that is the

number $\phi\left(\frac{n}{d}\right)$. Since each integers of the set $\{1, 2, 3, \cdots, n\}$ lies in exactly one class S_d, we have the formula $n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$. But d runs through all positive divisors of n so does $\frac{n}{d}$. Thus finally we have, $n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$. □

Here we have illustrated the above theorem by means of an example:

Example 7.6.1. *Let us choose a number* $n = 12$ *and the divisors of* 12 *are* $1, 2, 3, 4, 6, 12$. *Thus the classes* S_d *are,*

$$S_1 = \{1, 5, 7, 11\}, S_2 = \{2, 10\}, S_3 = \{3, 9\}, S_4 = \{4, 8\}, S_6 = \{6\} S_{12} = \{12\}.$$

Now, $\phi(12) = 4, \phi(6) = 2, \phi(4) = 2, \phi(3) = 2, \phi(2) = 1, \phi(1) = 1$.

Therefore $\sum_{d|12} \phi(12) = \phi(12) + \phi(6) + \phi(4) + \phi(3) + \phi(2) + \phi(1) = 12 = n$.

This shows the clarification of our above theorem.

Also, the next part of our discussion is based on the last theorem. Here we illustrate the theorem with a suitable example, which totally depends on the multiplicative property of ϕ[for further details refer to theorem (7.2.2)]. Now for $n = 1$, the case is trivial. Let us choose $n = 24$ and apply the formula $F(n) = \sum_{d|n} \phi(d)$ where F and ϕ are both number theoretic functions. Since ϕ is multiplicative, F is also so(Why!). Again $n = 24 = 2^3 \cdot 3$ be the prime factorization of 24, which implies $F(24) = F(2^3)F(3)$. Now

$$\begin{aligned} F(2^3) &= \sum_{d|2^3} \phi(d) \\ &= \phi(1) + \phi(2) + \phi(4) + \phi(8) \\ &= 1 + (2-1) + (2^2 - 2) + (2^3 - 2^2) [\because \phi(p^k) = p^k - p^{k-1}] \\ &= 1 + 1 + 2 + 4 = 2^3 \\ \text{and } F(3) &= \sum_{d|3} \phi(d) \\ &= \phi(1) + \phi(3) = 1 + 2 = 3. \end{aligned}$$

Therefore $F(24) = 2^3 \cdot 3 = 24$ and thus we have $n = 24 = F(24) = \sum_{d|24} \phi(d)$ which is our desired result.

Based on the last example, we are going to give the alternative proof of Theorem 7.6.1 as follows:

Proof. If $n = 1$, the case is trivial(Verify!). So we assume $n > 1$. Let us consider the number-theoretic function $F(n) = \sum_{d|n} \phi(d)$. Since ϕ is multiplicative, F is also so. Let the prime factorization of n be given by $n = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s}$. Then $F(n) = F(p_1^{d_1})F(p_2^{d_2}) \cdots F(p_s^{d_s})$. For each value of j, we obtain

$$\begin{aligned} F(p_j^{d_j}) &= \sum_{d|p_j^{d_j}} \phi(d) \\ &= \phi(1) + \phi(p_j) + \phi(p_j^2) + \phi(p_j^3) + \ldots + \phi(p_j^{d_j}) \\ &= 1 + (p_j - 1) + (p_j^2 - p_j) + (p_j^3 - p_j^2) + \ldots + (p_j^{d_j} - p_j^{d_j - 1}) \\ &= p_j^{d_j}. \end{aligned}$$

Hence $F(n) = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s} = n \Rightarrow \sum_{d|n} \phi(d) = n.$ □

Now for the next part of discussion , let us choose a positive integer 20 and $\phi(20) = 8$. Here the set of positive integers less than 20 and prime to 20 are $\{1, 3, 7, 9, 11, 13, 17, 19\}$ and their sum is $1+3+7+9+11+13+17+19 = 80 = \frac{1}{2} \times 20 \times 8$. This is not a coincidence, in fact our next theorem deals with it.

Theorem 7.6.2. *For $n > 1$, the sum of the positive integers less than n and prime to n is $\frac{1}{2} n\phi(n)$.*

Proof. Let $k_1, k_2, \cdots, k_{\phi(n)}$ be the positive integers less than n and prime to n. Now using Proposition (2.4.3), we have from congruence relation,

$$\begin{aligned} k_1 + k_2 + \cdots + k_{\phi(n)} &= (n - k_1) + (n - k_2) + \cdots + (n - k_{\phi(n)}) \\ &= n\phi(n) - (k_1 + k_2 + \cdots + k_{\phi(n)}) \\ \text{Therefore, } \quad 2(k_1 + k_2 + \cdots + a_{\phi(n)}) &= n\phi(n) \\ \Rightarrow k_1 + k_2 + \cdots + k_{\phi(n)} &= \frac{1}{2} n\phi(n), \end{aligned}$$

which proves the theorem. □

Finally at this point we can give an application of Mobiöus Inversion formula, which leads us to the following theorem:

Theorem 7.6.3. *For any positive integer n, $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.*

Before going to the proof, let us illustrate the theorem by means of an example: taking $n = 14$ we see that,

$$
\begin{aligned}
14\sum_{d|14}\left(\frac{\mu(d)}{d}\right) &= 14\left[\mu(1)+\frac{\mu(2)}{2}+\frac{\mu(7)}{7}+\frac{\mu(14)}{14}\right] \\
&= 14\left[1+\frac{-1}{2}+\frac{(-1)}{7}+\frac{(-1)^2}{14}\right] \\
&= 14\left[1-\frac{1}{2}-\frac{1}{7}+\frac{1}{14}\right] \\
&= 14\times\frac{6}{14}=6=\phi(14).
\end{aligned}
$$

Proof. From the Theorem (7.6.1) we know, $F(n)=\sum_{d|n}\phi(d)=n$ and from Mobiöus inversion formulae we have, $\phi(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)$. Therefore we get,

$$\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}=n\sum_{d|n}\frac{\mu(d)}{d}.$$ □

7.7 Worked out Exercises

Problem 7.7.1. *For a square-free integer $n>1$, show that $\tau(n^2)=n$ if and only if $n=3$.*

Solution 7.7.1. *If $n=3$, then $\tau(n^2)=\tau(3^2)=2+1=3$[refer to Theorem 6.2.2]. Next, suppose n is square-free with $n>1$ and $\tau(n^2)=n$. Let $n=p_1p_2\cdots p_s$ with $p_i\neq p_j$. Moreover, applying Theorem 6.2.2 we get*

$$
\begin{aligned}
\tau(n^2) &= \tau(p_1^2p_2^2\cdots p_s^2) \\
&= (2+1)(2+1)\cdots(2+1)=3^s. \\
\therefore\ \tau(n^2) &= n=p_1p_2\cdots p_s=3^s,
\end{aligned}
$$

which implies all $p_i=3$. Hence $n=3$ and $s=1$.

Problem 7.7.2. *For $n>2$, prove the inequality $\phi(n^2)+\phi((n+1)^2)\leq 2n^2$.*

Solution 7.7.2. *If k is composite, then $\phi(k)\leq k-\sqrt{k}$. As n^2 is composite, so is $(n+1)^2$. Therefore $\phi(n^2)\leq n^2-\sqrt{n^2}=n^2-n$. Again $\phi((n+1)^2)\leq (n+1)^2-\sqrt{(n+1)^2}=n^2+n$. Thus $\phi(n^2)+\phi((n+1)^2)\leq 2n^2$.*

Problem 7.7.3. *Given an integer z, prove that there exists at least one k for which $z|\phi(k)$.*

Solution 7.7.3. *Let* $k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *be such that*

$$\phi(k) = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1).$$

Our claim is $z = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}$. *So let* $z = q_1^{\beta_1} \cdots q_s^{\beta_s}$. *Choose* $k = q_1^{\beta_1 + 1} \cdots q_s^{\beta_s + 1}$.

$$\therefore\ \phi(k) = q_1^{\beta_1} \cdots q_s^{\beta_s}(q_1 - 1) \cdots (q_s - 1),$$

which implies $z|\phi(k)$.

Problem 7.7.4. *Show that if* z *is a product of twin primes, say* $z = p(p+2)$, *then*

$$\phi(z)\sigma(z) = (z+1)(z+3).$$

Solution 7.7.4. *Here* $\gcd(p, p+2) = 1$, *so* $\phi(z) = \phi(p)\phi(p+2) = (p-1)(p+1)$. *But* $\sigma(z) = \sigma(p)\sigma(p+2) = (p+1)(p+3)$. *Therefore* $\phi(z)\sigma(z) = (p-1)(p+1)^2(p+3)$. *Now* $(z+1)(z-3) = (p^2+2p+1)(p^2+2p-3) = (p+1)^2(p+3)(p-1)$. *Hence* $\phi(z)\sigma(z) = (z+1)(z+3)$.

Problem 7.7.5. *Assuming* $d|n$, *prove that* $\phi(d)|\phi(n)$.

Solution 7.7.5. *Since* $d|n$, *so assume* $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ *and* $d = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ *where* $0 \le a_i \le k_i$. *Then* $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_r})$ *and* $\phi(d) = d(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_r})$. *Since* $d|n$, *then it follows that* $\phi(d)|\phi(n)$.

Problem 7.7.6. *If* z *is a square-free integer, prove that for all integers* $k \ge 2$

$$\sum_{d|z} \sigma(d^{k-1})\phi(d) = z^k.$$

Solution 7.7.6. *Since* ϕ *and* σ *are multiplicative,*

$$F(z) = \sum_{d|z} \sigma(d^{k-1})\phi(d) = \sum_{d|z} \underbrace{\sigma(d)\sigma(d)\cdots\sigma(d)}_{(k-1)times}\phi(d),$$

is also so.

Case(i) *Let* z *be square-free and* $z = p$. *Then*

$$\begin{aligned} F(p) &= \sum_{d|z} \sigma(d^{k-1})\phi(d) \\ &= \sigma(1)\phi(1) + \sigma(p^{k-1})\phi(p) \\ &= 1 + \frac{p^{k-1+1} - 1}{p - 1} \cdot (p - 1) = p^k = z^k. \end{aligned}$$

Case(ii) *If* $z = p_1 p_2 \cdots p_r$, *then*

$$\sum_{d|z} \sigma(d^{k-1})\phi(d) = F(z) = F(p_1)F(p_2)\cdots F(p_r)$$
$$= p_1^k p_2^k \cdots p_r^k = (p_1 p_2 \cdots p_r)^k = z^k.$$

Problem 7.7.7. *For any integer* n, *prove that* $3|\sigma(3n+2)$.

Solution 7.7.7. *Let* $3n+2 = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. *Since* $3 \equiv 0(\text{mod } 3)$ *and* $3n+2 \equiv 2(\text{mod } 3)$, *therefore* $p_i^{k_i} \not\equiv 0(\text{mod } 3)$ *for* $i = 1, 2, \ldots, s$. *If all* $p_i^{k_i} \equiv 1(\text{mod } 3)$, *then* $p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \equiv 1(\text{mod } 3)$. *Since* $p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \equiv 2(\text{mod } 3)$, *therefore* $\exists$ *one* p_i *satisfying* $p_i^{k_i} \equiv 2(\text{mod } 3)$. *This implies* $p_i \equiv 2(\text{mod } 3)$. *Because if* $p_i \equiv 0(\text{mod } 3)$ *and* $p_i \equiv 1(\text{mod } 3)$, *then this yields* $p_i^{k_i} \equiv 0(\text{mod } 3)$ *and* $p_i^{k_i} \equiv 1(\text{mod } 3)$ *respectively. But this is not the case. Since* $p_i \equiv 2(\text{mod } 3)$, *then* $p_i^2 \equiv 4 \equiv 1(\text{mod } 3)$ *and* $p_i^3 \equiv 2(\text{mod } 3)$. *Therefore if* $p_i^r \equiv 2(\text{mod } 3)$, *then* r *is odd. Hence* $p_i^{k_i} \equiv 2(\text{mod } 3)$, k_i *is odd.*

$$\therefore\ \sigma(p_i^{k_i}) = \frac{p_i^{k_{i+1}} - 1}{p_i - 1} = \frac{(p_i - 1)(p_i^{k_i} + p_i^{k_i - 1} + \ldots + p_i + 1)}{p_i - 1},$$
$$= p_i^{k_i} + p_i^{k_i - 1} + \ldots + p_i + 1, \text{ and } k_i \text{ is odd.}$$

Since $2 \equiv (-1)(\text{mod } 3)$, *therefore if* r *is odd then* $p_i^r \equiv (-1)(\text{mod } 3)$ *and if* r *is even then* $p_i^r \equiv 1(\text{mod } 3)$.

$$\therefore\ \sigma(p_i^{k_i}) = p_i^{k_i} + p_i^{k_i - 1} + \ldots + p_i + 1$$
$$\equiv (-1) + 1 + \ldots + (-1) + 1(\ \text{mod } 3)$$
$$\equiv 0(\ \text{mod } 3.).$$
$$\therefore\ 3|\sigma(p_i^{k_i}) \Rightarrow 3|(\sigma(p_1^{k_1}))\cdots\sigma(p_i^{k_i})\cdots\sigma(p_s^{k_s})$$
$$\Rightarrow \sigma(p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}),\ \because,\ \sigma \text{ is multiplicative}$$
$$3|\sigma(3n+2).$$

Problem 7.7.8. *For any integer* $n > 1$ *has the form* $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, *then show that* $\sum_{d|n} \mu(d)\phi(d) = (2 - p_1)(2 - p_2)\ldots(2 - p_r)$.

Solution 7.7.8. *Since* μ *and* ϕ *are multiplicative then* $\mu \cdot \phi$ *is also multiplicative. Therefore* $F(n) = \sum_{d|n} \mu(d)\phi(d)$ *is also multiplicative. Note that* $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ *is the prime factorization of* n. *Then*

$$F(p^k) = \sum_{d|p^k} \mu(d)\phi(d)$$
$$= \mu(1)\phi(1) + \mu(p)\phi(p) + \ldots + \mu(p^k)\phi(p^k)$$
$$= 1 + (-1)(p-1) = 2 - p\ [\because \mu(p^k) = 0 \text{ for } k \geq 2].$$

$\therefore\ F(n) = (2-p_1)(2-p_2)\ldots(2-p_r).$

Problem 7.7.9. *If the integer $z>1$ has the prime factorization $z = q_1^{k_1}q_2^{k_2}\cdots q_s^{k_s}$, prove*

$$\sum_{d|z} d\phi(d) = \left(\frac{q_1^{2k_1+1}+1}{q_1+1}\right)\left(\frac{q_2^{2k_2+1}+1}{q_2+1}\right)\cdots\left(\frac{q_s^{2k_s+1}+1}{q_s+1}\right).$$

Solution 7.7.9. *Since $f(x)=x$ is multiplicative, therefore $f\cdot\phi$ is also so. Hence*

$$F(z) = \sum_{d|z} d\phi(d),\ \textit{is multiplicative.}$$

Consider,

$$\begin{aligned}
F(q^k) &= \sum_{d|q^k} d\phi(d)\\
&= 1\cdot\phi(1) + q\cdot\phi(q) + q^2\cdot\phi(q^2) + \ldots + q^k\cdot\phi(q^k),\\
&= 1 + q(q-q^0) + q^2(q^2-q) + \ldots + q^k(q^k-q^{k-1}),\\
&= 1 + q^2 - q + q^4 - q^3 + q^6 - q^5 + \ldots + q^{2k} - q^{2k-1},\\
&= 1 + (-1)^1 q + (-1)^2 q^2 + (-1)^3 q^3 + \ldots + (-1)^{2k} q^{2k}.
\end{aligned}$$

$$\begin{aligned}
&\therefore\ q^{2k+1}+1 = (q+1)(q^{2k}-q^{2k-1}+\ldots+q^2-q+1)(Why!).\\
&\Rightarrow\ \frac{q^{2k+1}+1}{q+1} = q^{2k}-q^{2k-1}+\ldots+q^2-q+1,\\
&\quad\Rightarrow\ F(q^k) = \frac{q^{2k+1}+1}{q+1}.\\
&\therefore\ \sum_{d|z} d\phi(d) = F(z) = F(q_1^{k_1}q_2^{k_2}\cdots q_s^{k_s}),\\
&\qquad\qquad = F(q_1^{k_1})F(q_2^{k_2})\cdots F(q_s^{k_s}),\\
&\qquad\qquad = \left(\frac{q_1^{2k_1+1}+1}{q_1+1}\right)\left(\frac{q_2^{2k_2+1}+1}{q_2+1}\right)\cdots\left(\frac{q_s^{2k_s+1}+1}{q_s+1}\right).
\end{aligned}$$

Problem 7.7.10. *Given $k>0$, establish that there exists a sequence of k consecutive integers $n+1, n+2, ..., n+k$ satisfying*

$$\mu(n+1) = \mu(n+2) = \cdots = \mu(n+k) = 0.$$

Solution 7.7.10. *Let p_k be the kth prime. Then for $i\neq j$. $\gcd(p_i^2, p_j^2) = 1$. By*

virtue of Chinese Remainder theorem, ∃ a solution to:

$$\begin{aligned} X &\equiv -1(\mod p_1^2),\\ X &\equiv -2(\mod p_2^2),\\ &\vdots\\ X &\equiv -k(\mod p_k^2), \end{aligned}$$

where $p_1 = 2, p_2 = 3, \ldots, p_k = kth$ *prime. If* $n = p_1 p_2 \cdots p_k$ *and* $N_i = \frac{n}{p_i}$, *then a simultaneous solution is*

$$\begin{aligned} & X = (-1)N_1^{\phi(p_1^2)} + (-2)N_2^{\phi(p_2^2)} + \ldots + N_k^{\phi(p_k^2)}.\\ \Rightarrow\ & X = -N_1^{\phi(2^2)} - 2N_2^{\phi(3^2)} - \ldots - kN_k^{\phi(k^2)}.\\ \Rightarrow\ & X + i \equiv 0(\mod p_i^2),\ \textit{for}\ \ i = 1, 2, 3, \ldots, k.\\ \Rightarrow\ & X + i = ap_i^2,\ \textit{for some integer}\ \ a. \end{aligned}$$

Hence $\mu(X + i) = 0,\ i = 1, 2, 3, \ldots, k.$

7.8 Exercises:

1. Calculate $\phi(5040),\ \phi(36000)$.

2. Prove the following assertions:
   (a) $\phi(3n) = 3\phi(n)$ if and only if $3|n$.
   (b) $\phi(3n) = 2\phi(n)$ if and only if $3 \nmid n$.

3. If the integer $n > 1$ has r distinct prime factors, then show that $\phi(n) \geq \frac{n}{2^r}$.

4. If $n = p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}$ then prove the inequality $\tau(n)\phi(n) \geq n$.

5. Prove that there are infinitely many integers n satisfying $\phi(n) = \frac{n}{3}$.

6. Show that Goldbach's Conjecture implies that for each even integer $2n$ there exists integers n_1 and n_2 with $\phi(n_1) + \phi(n_2) = 2n$.

7. Use Euler's theorem to establish the following:
   (a) For any integer a, $a^{13} \equiv a(\mod 2730)$.
   (b) For any odd integer a, $a^{33} \equiv a(\mod 4080)$.

8. For any prime p prove the following assertions:
   (a) $\sigma(p!) = (p + 1)\sigma((p - 1)!)$;
   (b) $\phi(p!) = (p + 1)\phi((p - 1)!)$.

9. Prove that $4|\sigma(4n+3)$ for any positive integer n.

10. If the integer $n > 1$ has the prime factorization $n = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$ then establish that:
$\sum_{d|n} \frac{\phi(d)}{d} = (1 + \frac{k_1(p_1-1)}{p_1})(1 + \frac{k_2(p_2-1)}{p_2}) \dots (1 + \frac{k_r(p_r-1)}{p_r})$.

11. Show that for any integer n, $\phi(n)|n-1$ if and only if n is prime.

12. Prove that $\sum_{d|n} \sigma(d)\phi(\frac{n}{d}) = n\tau(n)$.

13. For a positive integer z, prove that $\displaystyle\sum_{d|z} \frac{\mu^2(d)}{\phi(d)} = \frac{z}{\phi(z)}$.

14. Show that if p and $2p+1$ are both odd primes, then $n = 4p$ satisfies $\phi(n+2) = \phi(n) + 2$.

15. For which positive integer n does $\phi(n)$ divides n?