DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTER OF SCIENCES- MATHEMATICS

SEMESTER –III

ELEMENTARY NUMBER THEORY

DEMATH3OLEC5

BLOCK-2

UNIVERSITY OF NORTH BENGAL

Postal Address:
The Registrar,
University of North Bengal,
Raja Rammohunpur,
P.O.-N.B.U., Dist-Darjeeling,
West Bengal, Pin-734013,
India.
Phone: (O) +91 0353-2776331/2699008
Fax: (0353) 2776313, 2699001
Email: regnbu@sancharnet.in ; regnbu@nbu.ac.in
Wesbsite: www.nbu.ac.in

First Published in 2019

FOREWORD

The Self Learning Material (SLM) is written with the aim of providing simple and organized study content to all the learners. The SLMs are prepared on the framework of being mutually cohesive, internally consistent and structured as per the university's syllabi. It is a humble attempt to give glimpses of the various approaches and dimensions to the topic of study and to kindle the learner's interest to the subject

We have tried to put together information from various sources into this book that has been written in an engaging style with interesting and relevant examples. It introduces you to the insights of subject concepts and theories and presents them in a way that is easy to understand and comprehend.

We always believe in continuous improvement and would periodically update the content in the very interest of the learners. It may be added that despite enormous efforts and coordination, there is every possibility for some omission or inadequacy in few areas or topics, which would definitely be rectified in future.

We hope you enjoy learning from this book and the experience truly enrich your learning and help you to advance in your career and future endeavours.

ELEMENTARY NUMBER THEORY

BLOCK 1

BLOCK 2

BLOCK-2 ELEMENTARY NUMBER THEORY

Introduction To The Block

Number theory, branch of mathematics concerned with properties of the positive integers (1, 2, 3, …). Sometimes called “higher arithmetic,” it is among the oldest and most natural of mathematical pursuits.

Number theory has always fascinated amateurs as well as professional mathematicians. In contrast to other branches of mathematics, many of the problems and theorems of number theory can be understood by laypersons, although solutions to the problems and proofs of the theorems often require a sophisticated mathematical background.

Until the mid-20th century, number theory was considered the purest branch of mathematics, with no direct applications to the real world. The advent of digital computers and digital communications revealed that number theory could provide unexpected answers to real-world problems. At the same time, improvements in computer technology enabled number theorists to make remarkable advances in factoring large numbers, determining primes, testing conjectures, and solving numerical problems once considered out of reach.

UNIT 8: PRIMITIVE ROOTS

STRUCTURE

8.0 OBJECTIVES

Understand the concept of the integer modulo n.

Understand the importance of primitive roots and their theoretical application

8.1 INTRODUCTION

In modular arithmetic, a branch of number theory, a number g is a **primitive root modulo n** if every number a cop rime to n is congruent to a power of g modulo n. That is, g is a primitive root modulo n if for every integer a cop rime ton, there is an integer k such that $g^k \equiv a \pmod{n}$. Such a value k is called the **index** or **discrete logarithm** of a to the base g modulo n. Note that g is a primitive root modulo n if and only if g is a generator of the multiplicative group of integers modulo n.

Gauss defined primitive roots in Article 57 of the Disquisitions Arithmetical (1801), where he credited Euler with coining the term. In Article 56 he stated that Lambert and Euler knew of them, but he was the first to rigorously demonstrate that primitive roots exist for a prime n

8.2 THE INTEGER MODULO N

8.1.1: Definition

Given a positive integer n > 1and an integer a such that gcd(a, n) = 1, the smallest positive integer d for which $a^d \equiv 1 \bmod n$ is called the **order of a modulo n**. Note that Euler's theorem says that $a^{\phi(n)} \equiv 1 (\bmod n)$, so such numbers dd indeed exist. The order of a mod n is sometimes written as ordn(a) for short.

There are ϕ(9) = 6 distinct congruence classes mod 9 of integers that are relatively prime to 9, namely 1,2,4,5,7,8. Compute their orders mod 9.

- The powers of 1 are 1,1,1,…. The order of 1 is 1.
- The powers of 2 are 2,4,8,7,5,1,…. The order of 2 is 6.
- The powers of 4 are 4,7,1,…. The order of 4 is 3.
- The powers of 5 are 5,7,8,4,2,1,…. The order of 5 is 6.
- The powers of 7 are 7,4,1,…. The order of 7 is 3.
- The powers of 8 are 8,1,…. The order of 8 is 2

8.2.2 Basic Properties

(1) If $a^m \equiv 1 (\bmod n)$, the $ord_n(a) | m$.

(2) $ord_n(a) | \varphi(n)$; if p is a prime, then $ord_p(n) | (p-1)$ for any n.

(3)(3) If $a^\ell \equiv a^m (\bmod n)$, then $\ell \equiv m (\bmod ord_n(a))$.

In order to prove property (1), let d =$ord_n(a)$. Since $a^m \equiv 1 (\bmod n)$ $a^{mx+dy} \equiv 1 (\bmod n)$ forv any x nd y. By Bezout's identity, there exist x and y such that mx+dy=gcd(d,m). Then, from the minimality of d, it follows that $d \leq \gcd(m,d)$, which cannot hold unless they are equal and d|m.

(Another way to see (1) is that the minimum period of a periodic sequence divides any other period, essentially by the division algorithm.)

Property (2) follows from property (1) and Euler's theorem, and property (3) follows from property (1) applied to ℓ−m.

Example: Prove that $n | \varphi(a^n - 1)$ for all positive integers a and n.

It is immediate that $ord_{a^n-1}(a) = n$: $a^n \equiv 1 (\bmod a^n - 1)$, and $a^d \equiv 1 (\bmod a^n - 1)$ implies $(a^n - 1) | (a^d - 1)$, so $d \geq n$. Then the result follows from property (1) above.

Example: Prove that any prime factor of the nth Fermat number $2^{2^n} + 1$ is congruent 2^{n+1}. Show that there are infinitely many prime numbers of the form $2^n k+1$ for any fixed n.

Solution: Consider a prime p such that $p|2^{2^n}+1$; that is, $2^{2^n} \equiv -1 (\text{mod} p)$. Then $(2^{2^n}+1) \equiv 1 (\text{mod} p)$ and consequently ordp (2)| 2^{n+1}.

So ordp (2) = 2^k for some $k \leq n+1$. We will prove that in fact k = n + 1. Indeed, if this is not the case, then ord p(2)|2^n and so $2^{2^n} \equiv 1 (\text{mod} p)$. But this implies that $1 \equiv -1 (\text{mod} p)$, so p =2, but this is impossible.

Therefore, we have found that ordp(2) = 2^{n+1} and so $2^{n+1}|(p-1)$ by Property (1) above.

The second part is a direct consequence of the first. Indeed, it is enough to prove that there exists an infinite set of Fermat numbers \large $(2^{2^{n_k}}+1)$nk > a, any two relatively prime. Then we could take a prime factor of each such Fermat number and apply the first part to obtain that each such prime is of the form 2^nk+1.

Not only is it easy to find such a sequence of co-prime Fermat numbers, but in fact any two distinct Fermat numbers are relatively prime. Indeed, suppose that d|gcd(2^{2^a}+1, $2^{2^{a+b}}$+1). Then $2^{2^{a+1}} \equiv 1 (\text{mod } d)$ and so d|$2^{2^{a+1}}-1$.

Combining this with d|$2^{2^{a+1}}$+1, we obtain a contradiction. Hence both parts of the problem are solved.

8.2.3 Theorem

Let the integer a have order k modulo n. Then $a^h = 1 (\text{mod } n)$ if and only if k Ih; in particular, k |Ø(n).

Proof. Suppose that we begin with k |h, so that h = jk for some integer j. Because $a^k = 1 (\text{mod } n)$, With reference to the Congruence Theorem, $(a^k)^j \equiv l^j (\text{mod } n)$ or $a^h = 1 (\text{mod } n)$. Conversely, let h be any positive integer satisfying $a^h = 1 (\text{mod } n)$.

By the Division Algorithm, there exist q and r such that h = qk + r, where 0 ≤S r < k. Consequently,

$$a^h = a^{qk+r} = (a^k)^q a'$$

By hypothesis, both $a^h = 1 (\text{mod } n)$ and $a^k = 1 (\text{mod } n)$, the implication of which is that a' = 1 (mod n). Because 0 ::S r < k, we end up with r = 0;

otherwise, the choice of k as the smallest positive integer such that ak =1 (mod n) is contradicted.

Hence,

$$h = qk, \text{ and } k \mid h.$$

8.2.4.Theorem

If the integer a has order k modulo n, then $a^i = a^j \pmod n$ if and only if $i \equiv j \pmod k$.

Proof. First, suppose that $a^i \equiv a^j \pmod n$, where $i \geq j$. Because a is relatively prime ton, we may cancel a power of a to obtain $a^{i-j} \equiv 1 \pmod n$. According to Theorem 8.1.3, this last congruence holds only if k Ii - j, which is just another way of saying that $i \equiv j \pmod k$.

Conversely, let $i \equiv j \pmod k$. Then we have $i = j + qk$ for some integer q. By the definition of k, $a^k \equiv 1 \pmod n$, so that

$$a^i \equiv a^{j+qk} = a^j (a^k)^q = a^j \pmod n$$

which is the desired conclusion.

8.2. 5.Corollary

If a has order k modulo n, then the integers $a_1, a_2, \ldots, ak$ are incongruent

modulo n.

Proof. If $a^i \equiv a^j \pmod n$ for $1 \leq i \leq j \leq k$, then the theorem ensures that $i \equiv j \pmod k$. But this is impossible unless i = j.

8.2.6. Theorem

If the integer a has order k modulo n and h > 0, then a^h has order k /gcd(h, k) modulo n.

Proof. Let d = gcd(h, k). Then we may write $h = h_1 d$ and $k = k_1 d$, with gcd $(h_1 , k_1) = 1$. Clearly,

$$(a^h)^{k1'} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} = 1 \pmod n$$

If a^h is assumed to have order r modulo n, then Theorem 8.1.3 asserts that $r \mid k_1$. On the other hand, because a has order k modulo n, the

congruence

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

indicates that k | hr; in other words, $k_1 d \mid h_1 dr$ or $k_1 \mid h_1 r$. But $\gcd(k_1, h_1) = 1$, and therefore $k_1 \mid r$. This divisibility relation, when combined with the one obtained earlier, gives k k

$$r = k_1 = \frac{k}{d} = \frac{k}{\gcd(h,k)}$$

proving the theorem.

The preceding theorem has a corollary for which the reader may supply a proof.

8.2.7. Corollary

Let a have order k modulo n. Then ah also has order k if and only if gcd(h , k) = 1.

8.3 THE PRIMITIVE ROOTS

Let us start by computing the powers 3^i modulo 7 for $0 \leq i < \varphi(7) = 6$. We obtain $3^0 = 1$, $3^1 = 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$. Hence, the set $\{3^i \mid 0 \leq i < \varphi(7)\}$ is a reduced residue system modulo 7, that is every integer a not divisible by 7 is congruent to 3^i for a unique integer i modulo φ(7). This fact allows us to replace calculations using only multiplication and exponentiation modulo 7 by calculations using addition modulo φ(7) instead.

Example: Solve the equation $x^5 \equiv 6 \pmod{7}$.

Solution: Let $x \equiv 3^y \pmod{7}$. Since $6 \equiv 3^3 \pmod{7}$, the given equation can now be written $3^{5y} \equiv 3^3 \pmod{7}$, which is equivalent to the congruence $5y \equiv 3 \pmod{6}$. The latter congruence has the unique solution $y \equiv 3 \pmod{6}$, and hence our original equation has the unique solution $x \equiv 6 \pmod{7}$.

Motivated by Example, we will investigate numbers m with the property that there exists a number g such that $\{g^i \mid 0 \leq i < \varphi(m)\}$ is a reduced

residue system. That not all numbers m have this property follows from the following example.

Example: Since $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$ and $\varphi(8) = 4$, it follows that $\{a^i \mid 0 \leq i < 4\}$ is never equal to a reduced residue system modulo 8.

8.3.1Proposition

Let m be a positive integer and a any integer such that (a, m) = 1. Define

$$A = \{k \in \mathbf{Z} \mid a|k| \equiv 1 \pmod m\}.$$

Then A is an ideal in **Z**.

Proof. We have to prove that the set A is closed under subtraction, i.e. that $j, k \in A \Rightarrow j - k \in A$. To prove this we may assume $j \geq k$, because j – k belongs to A if and only if k − j belongs to A.

Suppose $j, k \in A$. If $j \geq k \geq 0$, then $aj \equiv ak \equiv 1 \pmod m$, and hence $a^{j-k} \equiv a^{j-k}\, a^k = a^j \equiv 1 \pmod m$. If $j \geq 0 > k$, then $a^j \equiv a^{-k} \equiv 1 \pmod m$, and we obtain

$$a^{\,j-k} = a^j a^{-k} \equiv 1 \cdot 1 = 1 \pmod m.$$

Finally, if $0 > j \geq k$, then

$$a^{-j} \equiv a^{-k} \equiv 1 \pmod m,$$

and we conclude that

$$a^{j-k} \equiv a^{-j} a^{j-k} = a^{-k} \equiv 1 \pmod m.$$

Thus, in each case $j - k \in A$.

Note that A contains nonzero integers, because $\varphi(m)$ belongs to A by Euler's theorem. The ideal A is generated by a unique positive integer h, which is the smallest positive integer belonging to A, that is $ah \equiv 1 \pmod m$ while $aj \not\equiv 1 \pmod m$ for $1 \leq j < h$.

8.3.2 Definition

The positive generator h of A, i.e. the smallest positive integer such that $ah \equiv 1 \pmod m$, is called the order of a modulo m and is denoted by ord a.

The order ord a of course depends on the modulus m, but since the modulus will always be fixed during a calculation, this ambiguity in the notation causes no difficulties.

For any modulus m, ord 1 = 1.

Example: Modulo 8 we have ord 3 = ord 5 = ord 7 = 2.

Example: Let us compute the order of the numbers 2, 3 and 6 modulo 7.

Our calculations before Example 1 show that ord 3 = 6.

Since $2^2 \equiv 4 \pmod 7$ and

$2^3 \equiv 1 \pmod 7$, ord 2 = 3,

and since $6^2 \equiv 1 \pmod 7$, ord 6 = 2.

The following theorem is an immediate consequence of the fact that the ideal A is generated by h = ord a.

8.3.3 Theorem

Assume (a, m) = 1 and write h = ord a modulo m. Then

(i) $a^n \equiv 1 \pmod m$ if and only if h | n;

(ii) h | φ(m);

(iii) $a^j \equiv a^k \pmod m$ if and only if $j \equiv k \pmod h$;

(iv) the numbers 1, a, a2, . . . , ah−1 are incongruent modulo m, and each power an is congruent to one of these modulo m;

(v) ord ak = h/(h, k).

Proof. (i) follows from the definition of a generator of an ideal.

(ii) follows from (i) and Euler's theorem.

(iii) Assume $k \geq j \geq 0$; then $ak \equiv aj \pmod m$ holds if and only if $ak-j \equiv 1 \pmod m$, because we may divide the former congruence by aj since (a,

m) = 1. The conclusion now follows from (i).

(iv) is of course a consequence of (iii).

(v) By (i), $(a^k)^n \equiv 1 \pmod{m} \Leftrightarrow kn \equiv 0 \pmod{h}$. We can divide the right hand congruence by k provided we change the modulus to h/(h, k). Thus, $(a^k)^n \equiv 1 \pmod{m} \Leftrightarrow n \equiv 0 \pmod{h/(h, k)}$. The smallest positive number n satisfying the last congruence is n = h/(h, k); by definition, this is the order of a^k modulo m. Theorem 8.2.3 (ii) implies that ord $a \leq \varphi(m)$ for every number a which is relatively prime to m.

8.3.4 Definition

Assume that (g, m) = 1. If the order of g modulo m equals φ(m), then g is called a primitive root modulo m, or a primitive root of m.

Example 5 In Example 4 we calculated the order of 3 modulo 7 and found that ord 3 = 6 = φ(7). Consequently, 3 is a primitive root modulo 7.

Example 6 Not every integer has a primitive root. If m = 8, then $a^2 \equiv 1$ for every odd integer and hence ord $a \leq 2 < 4 = \varphi(8)$ for every a relatively prime to 8, that is 8 has no primitive roots.

8.3.5 Theorem

Suppose g is a primitive root modulo m. Then

(i) $\{1, g, g^2, \ldots, g^{\varphi(m)-1}\}$ is a reduced residue system modulo m;

(ii) $g^j \equiv g^k \pmod{m}$ if and only if $j \equiv k \pmod{\varphi(m)}$;

(iii) g^k is a primitive root modulo m if and only if $(k, \varphi(m)) = 1$.

In particular, if there exists a primitive root modulo m, then there are precisely φ(φ(m)) primitive roots.

Proof. Theorem 8.2.5 is just a special case of Theorem 8.2.3.

Example: We have found that 3 is a primitive root modulo 7. Since φ(φ(7)) = φ(6) = 2, there are 2 primitive roots. The other primitive root is 3^5, i.e. 5 (mod 7).

We will show that the only positive integers having primitive roots are 1, 2, 4, p^k and $2p^k$, where p is an odd prime and k an arbitrary positive integer. We start by proving that each prime has primitive roots; for this we will need the following two lemmas.

8.3.6 Lemma

If a has order h and b has order k modulo m, and if (h, k) = 1, then ab has order hk modulo m.

Proof. Let r be the order of ab. Since

$(ab)^{hk} = (a^h)^k(b^k)^h \equiv 1^k \cdot 1^h = 1 \pmod m$,

we conclude that r | hk.

To complete the proof, we have to show that hk | r. Note that

$b^{rh} \equiv (a^h)^r b^{rh} = (ab)^{rh} \equiv 1 \pmod m$, and hence k | rh.

Since (h, k) = 1 it follows that k | r. In a similar way, we show that h | r. Since (h, k) = 1 it now follows that hk | r.

Example: Working modulo 7 we have ord 2 = 3 and ord 6 = 2. Consequently, since

$2 \cdot 6 \equiv 5 \pmod 7$, ord 5 = ord$(2 \cdot 6) = 2 \cdot 3 = 6$.

8.3.7 Lemma

Let p and q be primes, and suppose that qk | (p − 1). Then there exists a number a of order q^k modulo p.

Proof. The congruence $x^{q^k} \equiv 1 \pmod p$ has exactly q^k roots. By Theorem 8.2.3 (i), the order of such a root is a divisor of q^k. If a is a root of order less than q^k, then a is the root of the congruence $x^{q^{k-1}} \equiv 1 \pmod p$, but this congruence has exactly q^{k-1} roots. Hence, there are exactly qk − qk−1 incongruent numbers of order precisely q^k.

8.3.8 Theorem

If p is a prime, then there exist exactly φ(p − 1) primitive roots modulo p.

Proof. By the last statement of Theorem 8.2.5, it is enough to show that there exists at least one primitive root modulo p. Let p − 1 =

$q_1^{k_1}, q_2^{k_2}, \ldots, q_r^{k_r}$ be the factorization of p − 1 into distinct primes. By Lemma 8.2.7 there are integers a_i of order $q_i^{k_i}$ for i = 1, 2, . . . , r. The numbers $q_i^{k_i}$ are pairwise relatively prime, so by repeated use of Lemma 8.5.6 we see that $g = a_1a_2 \cdot \cdot \cdot a_r$ has order p − 1, that is g is a primitive root modulo p. Suppose that g is a primitive root modulo m. If (a, m) = 1, then Theorem 8.2.5 implies that there is a unique integer i, with $0 \leq i \leq \varphi(m) - 1$ such that $g_i \equiv a \pmod{m}$. This fact allows us to make the following definition.

8.3.9 Definition

Let g be a primitive root of m, and suppose (a, m) = 1. The smallest nonnegative integer i such that $g^i \equiv a \pmod{m}$ is called the index of a (to the base g) and is denoted by ind a.

The index depends on both the modulus m and the root g, but since m and g are usually fixed, the notation should cause no confusion.

There is a strong similarity between logarithms and indices, and the following theorem states the most important properties. The proof is simple and is left to the reader.

8.3.10 Theorem

Suppose g is a primitive root modulo m, and let ind a denote the index of a to the base g.

(i) ind 1 = 0 and ind g = 1.

(ii) $a \equiv b \pmod{m}$ if and only if ind a = ind b.

(iii) $\text{ind } ab \equiv \text{ind } a + \text{ind } b \pmod{\varphi(m)}$.

(iv) $\text{ind } a^k \equiv k \text{ ind } a \pmod{\varphi(m)}$, for all nonnegative integers k.

8.3.11 Theorem

Let m be a positive integer having a primitive root, and suppose (a, m) = 1. Then the congruence $x^n \equiv a \pmod{m}$ has a solution if and only if

(1) $$a^{\varphi(m)/(n,\varphi(m))} \equiv 1 \pmod{m}.$$

If the congruence $x^n \equiv a \pmod{m}$ is solvable, then it has exactly $(n, \varphi(m))$ incongruent solutions.

Proof. Let g be a primitive root modulo m, and let $d = (n, \varphi(m))$. Taking indices, we see that the congruence $xn \equiv a \pmod{m}$ holds if and only if $n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\varphi(m)}$. This congruence is solvable if and only if $d \mid \operatorname{ind} a$, and if solutions exist, then there are exactly d incongruent solutions.

To complete the proof, we show that (1) holds if and only if $d \mid \operatorname{ind} a$. Taking indices, we see that (1) is equivalent to $(\varphi(m)/d) \operatorname{ind} a \equiv 0 \pmod{\varphi(m)}$, which holds if and only if $d \mid \operatorname{ind} a$.

If m has a primitive root, then the solutions of a solvable congruence $x^n \equiv a \pmod{m}$ can be found using indices, provided we compute (or have available) a table of indices for the given modulus m.

Since every prime modulus has a primitive root, we have the following corollary of Theorem 8.2.11.

8.3.12 Corollary

Suppose p is prime and $(a, p) = 1$. Then the congruence $xn \equiv a \pmod{p}$ is solvable if and only if

$$a^{(p-1)/(n,p-1)} \equiv 1 \pmod{p}.$$

Remark. The corollary gives an efficient procedure for determining whether the congruence $xn \equiv a \pmod{p}$ is solvable, but to actually find a solution is more difficult. However, if $(n, p - 1) = 1$, this is relatively easy. Use the Euclidean Algorithm to find positive integers s and t such that

$$sn = t(p - 1) + 1;$$

then

$$a^{sn} = a^{t(p-1)}\, a \equiv a \pmod{p},$$

that is a^s is a solution of the congruence $x^n \equiv a \pmod{p}$.

8.3.13 Corollary

Suppose that m has a primitive root and that n | φ(m). Then the congruence $xn - 1 \equiv 0 \pmod{m}$ has exactly n roots.

Proof. The congruence $x^n \equiv 1 \pmod{m}$ is obviously solvable. Hence, by Theorem 8.2.11 it has (n, φ(m)) = n incongruent solutions. We next show that if p is an odd prime, then pk has primitive roots for each k.

8.3.14 Theorem

Suppose that p is an odd prime.

(i) If g is a primitive root modulo p, then g + np is a primitive root modulo p^2 for exactly $p - 1$ values of n modulo p.

(ii) If g is a primitive root modulo p2, then g is a primitive root modulo p^k for all $k \geq 2$.

Proof. Let h denote the order of g +np modulo p2. (h may depend on n.) Then h | φ(p^2), that is h | p(p − 1).

But $(g + np)^h \equiv 1 \pmod{p2}$ implies $(g + np)^h \equiv 1 \pmod{p}$, and by the binomial theorem,

$$(g + np)^h = g^h + \sum_{j=1}^{h} \binom{h}{j} (np)^j g^{h-j} \equiv g^h \pmod{p},$$

And hence $g^h \equiv 1 \pmod{p}$. Since g has order p − 1, it follows that (p − 1) | h.

Thus h = p − 1 or h = p(p − 1). In the latter case, g + np is a primitive root of p^2, and in the former case it is not. We will prove that the former case arises only for one of the p possible values of n.

Let $f(x) = x^{p-1}-1$; then g is a root of the congruence $f(x) \equiv 0 \pmod{p}$ and $f'(g) = (p - 1)g^{p-2} \not\equiv 0 \pmod{p}$, since $(g^{p-2}, p) = 1$. Hence, there is a unique root of the form g + np of the congruence $f(x) \equiv 0 \pmod{p^2}$. This proves our claim.

(ii) It suffices to prove that if g is a primitive root modulo p^k, $k \geq 2$, then g is also a primitive root modulo p^{k+1}. Let h be the order of g modulo p^{k+1}; then $h \mid \varphi(p^{k+1})$, that is $h \mid p^k(p-1)$. Because $g^h \equiv 1 \pmod{p^{k+1}}$ implies $g^h \equiv 1 \pmod{p^k}$ and g is a primitive root modulo pk, $\varphi(pk)$ must divide h, that is $p^{k-1}(p-1) \mid h$.

Thus either

$$h = p^{k-1}(p-1) \text{ or } h = p^k(p-1) = \varphi(p^{k+1}).$$

In the latter case, g is a primitive root modulo p^{k+1} as claimed. We must show that the former case is excluded.

Let $t = \varphi(p^{k-1})$; then $g^t \equiv 1 \pmod{p^{k-1}}$ by Euler's theorem, and therefore $gt = 1 + np^{k-1}$ for some integer n. If $p \mid n$ then we would have $gt \equiv 1 \pmod{p^k}$, which contradicts the fact that g is primitive root modulo p^k. Thus, $p \nmid n$.

By the binomial theorem

$$g^{pt} = (g^t)^p = (1 + np^{k-1})p = 1 + np^k + \frac{p(p-1)}{2} n^2 p^{2k-2} + \ldots$$
$$\equiv 1 + np^k \pmod{p^{k+1}}.$$

Here, we have used that fact that the integer $\frac{p(p-1)}{2} n^2 p^{2k-2} = \frac{p(p-1)}{2} n^2 p^{2k-1}$ is divisible by p^{k+1}, because $2k - 1 \geq k + 1$ when $k \geq 2$, and the remaining omitted terms in the expansion contain even higher powers of p.

Since $p \nmid n$, we now conclude that

$$g^{pt} \not\equiv 1 \pmod{pk+1}.$$

Therefore, $h \neq pt = p\varphi(p^{k-1}) = p^{k-1}(p-1)$, and the proof is complete.

Example: Since $2^2 \equiv -1 \not\equiv 1 \pmod 5$, we conclude that the order of 2 modulo 5 must be 4, that is 2 is a primitive root of 5.

By Theorem 8.2.14, 2 + 5n is a primitive root of 25 for exactly four values of n, $0 \leq n \leq 4$. Since

$\varphi(25) = 20$, the primitive roots of 25 have order 20. The order h modulo 25 of an arbitrary number a is a divisor of 20. If $h < 20$, then either $h \mid 4$ or $h \mid 10$, so it follows that $a^4 \equiv 1 \pmod{25}$ or $a^{10} \equiv 1 \pmod{25}$. Hence, to

find whether a number a has order 20 it is enough to compute a^4 and a^{10} modulo 25; the order is 20 if and only if none of these two powers are congruent to 1. For a = 2 we obtain $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 6$ and $2^{10} \equiv 24$. Hence, the order of 2 is 20, i.e. 2
is a primitive root of 25.
For a = 7 we obtain $7^2 \equiv -1$ and $7^4 \equiv 1 \pmod{25}$, that is the order of 7 is 4, and 7 is not a primitive root of 25. Of course, it now follows that 12, 17 and 22 are primitive roots of 25.
By Theorem8.2.14 (ii), 2 is a primitive root of 5^k for all k.

8.3.15 Theorem

Suppose that p is an odd prime, and let g be a primitive root modulo p^k. If g is odd, then g is also a primitive root modulo $2p^k$, and if g is even, then $g + p^k$ is a primitive root modulo $2p^k$.

Proof. If g is odd, then $g^j \equiv 1 \pmod 2$ for every $j \geq 1$. Thus $g^j \equiv 1 \pmod{2p^k}$ if and only if $g^j \equiv 1 \pmod{pk}$, and hence the order of g modulo $2p^k$ is equal to the order of g modulo p^k, namely $\varphi(pk)$. Since $\varphi(2p^k) = \varphi(p^k)$, g is a primitive root of $2p^k$. If g is even, then g cannot be a primitive root of $2p^k$, for a primitive root is always relatively prime to the modulus. But $g + p^k$ is odd and, since it is congruent to g modulo pk, it is also a primitive root modulo p^k. Hence, $g + p^k$ is a primitive root of $2p^k$ by the preceding argument.
By above Example, 2 is a primitive root of 5^k for each k. Hence, 2+5k is a primitive root of $2 \cdot 5k$ for each k. In particular 7 is a primitive root of 10, and 27 is a primitive root of 50. By the same example, 17 is also a primitive root of 5^k for each k. Since 17 is odd, it follows that 17 is a primitive root of $2 \cdot 5^k$ for each k.

8.3.16 Theorem

There exists a primitive root modulo m if and only if m = 1,2, 4, p^k, or $2p^k$, where p is an odd prime and k is an arbitrary positive integer.

Proof. First note that 1, 2, and 4 have primitive roots (1, 1, and 3, respectively). Theorems 8.2.8, 8.2.14, and 8.2.15 imply that p^k and $2p^k$ have primitive roots whenever p is an odd prime and k is an arbitrary positive integer.

Conversely, to prove that these are the only positive integers having primitive roots, assume m > 2 has a primitive root. By Corollary 8.2.13, the congruence $x^2 \equiv 1 \pmod{m}$ has exactly 2 incongruent solutions (because $2 \mid \varphi(m)$ for all $m \geq 3$). Now implies that m must be either 4, p^k, or $2p^k$, where p is an odd prime.

If G is a general finite group with identity element e, then the order ord a of an element a is defined to be the smallest positive integer n satisfying $a^n = e$, while the order of the group, ord G, is defined to be the number of elements in G.

If h = ord a, then h| ord G and $\{e, a, a^2, \ldots, a^{h-1}\}$ is a subgroup of G. This subgroup coincides with G if ord a = ord G, and G is then called a cyclic group with a as a generator.

Applying these general notions to the specific case when G is the group Z_m^* of all residue classes modulo m that are relatively prime to m, we see that the order h of an integer a modulo m coincides with the order of the residue class a in Z_m^*, that $h|\varphi(m)$, that a number g is a primitive root modulo m if and only if the residue class g generates Z_m^*, and that there exists a primitive root modulo m if and only if the group $Z_m^*$is a cyclic group. Using the language of groups we can state Theorem 8.2.16 as follows: The group Z_m^* is cyclic if and only if m = 1, 2, 4, p^k or $2p^k$, where p is an odd prime and k is an arbitrary positive integer.

Check your Progress

1. Define order of modulo.

2. What is primitive root?

3.Prove ‘If a has order h and b has order k modulo m, and if (h, k) = 1, then ab has order hk modulo m’.

8.4 SUMMARY

Primitive roots play a crucial role in many theoretical investigations

8.5KEYWORDS

1. Order –The arrangement of things in relation to each other according to a particular sequence or pattern.
2. Notation - A system of symbols used to represent special things.
3. Cyclic Group – A **cyclic group** is a **group** that can be generated by a single element
4. Identity Element - In **mathematics**, an **identity element** or neutral **element** is a special type of **element** of a set with respect to a binary operation on that set, which leaves any **element** of the set unchanged when combined with it
5. Arbitary Positive integer: An arbitrary integer is basically the same as any integer. If a math problem says: "Let n be an arbitrary integer", it means that n can be any integer. A random integer in other words.

8.6 QUESTION FOR REVIEW

1. Prove, If $a^p \equiv 1 (\mathrm{mod} n)$ with prime p and $n \nmid a-1$, then ordn a = p.
2. Find the smallest R_n divisible by 13.
3. Determine all the primitive roots of the primes p = 11, 19, and 23, expressing each as a
power of some one of the roots.
4. For a prime p > 3, prove that the primitive roots of p occur in incongruent pairs r, r'
where rr' =1 (mod p).
[Hint: If r is a primitive root of p, consider the integer $r' = r^{P-2}$.]
5. Given that 3 is a primitive root of 43, find the following:
(a) All positive integers less than 43 having order 6 modulo 43

8.7 SUGGESTED READINGS

1.David M. Burton, Elementary Number Theory, University of New Hampshire.

2.G.H. Hardy, and , E.M. Wrigh,. An Introduction to the Theory of Numbers (6th ed, Oxford University Press, (2008).

3.W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.

4.A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.

5.I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.

6.T.M. Apostol, Introduction to Analytic number theory, UTM, Springer, (1976).

7.J. W. S Cassel, A. Frolich, Algebraic number theory, Cambridge.

8.M Ram Murty, Problems in analytic number theory, springer.

9.M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer.

8.8 ANSWERS TO CHECK YOUR PROGRESS

1. Provide the definition and example – 8.1

2. provide the explanation and example – 8.2

3.Provide the proof with example – 8.2.6

UNIT 9: FERMAT'S LITTLE THEOREM

STRUCTURE

9.0 OBJECTIVE

Understand the concept of Euler's theorem

Comprehend the Little Fermat's Theorem

Understand the algorithm of Fermat's Factorization

Comprehend the Wilson's Theorem

9.1 INTRODUCTION

Pierre de Fermat first wrote what would become his "Little Theorem" in 1679. As was typical of Fermat, he did not include a proof for fear the proof would be too long [1]. The first proof of this theorem was published more than fifty years later by Leonhard Euler, in 1736 [1]. Using the modular arithmetic notation published by Johann Carl Friedrich Gauss in 1801[1],

9.2 EULER'S THEOREM

Definition For [a] ∈ Um, the powers of the residue class are given by$[a]^1$ = [a], $[a]^2$ = [a][a], etc.

9.2.1 Lemma

If [a] ∈ $U_m$then $[a]^n$∈ Um for n ≥ 1, and $[a]^n$= $[a^n]$.

Proof. We will check this by induction on n. The n = 1 base case is trivial:$[a]^1$ = [a] = $[a^1]$, and by assumption [a] ∈ U_m.

For the inductive step, supposethat $[a]^k$= $[a^k]$ ∈ U_m. for k ≥ 1 and consider the k + 1-st power.

$[a]^{k+1}$ = $[a]^k$[a] = $[a^k]$[a] = $[a^ka]$ = $[a^{k+1}]$

By induction the theorem holds for all n ≥ 1.

9.2.2 Theorem (Euler's Theorem)

If m >0, and a is relatively prime to m,then $a^{\varphi(m)}$≡ 1 (mod m).

Proof. For m >0, we have that gcd(a, m) = 1 if and only if [a] ∈ U_m. The priorresult gives that a^n ≡ 1 (mod m) ⇐⇒$[a^n]$ = [1] ⇐⇒$[a]^n$= [1].

Therefore,Euler's Theorem is equivalent to the following: if m >0 and [a] ∈ $U_m$then

$[a]^{\varphi(m)}$ = [1].

We will write X_1, X_2, . . . , $X_{\varphi(m)}$ for the residue classes in U_m.We first show that if X ∈ $U_m$then the set O = {XX_1, XX_2, . . . , $XX_{\varphi(m)}$}equals the set Um. Containment one way is easy: any member of O is a memberof $U_m$by the closure property of groups. For containment the other way, consider X_i∈ U_m,and note that Theorem of groups shows that the equation X⊙ x = X_i has a solution x = X_j for some j, so X_i = $XX_j$is an element of O.

Next, for any X ∈ Um consider the product XX_1XX_2· · · $XX_{\varphi(m)}$. Theassociative property says that we can parenthesize this term in any way, andthe prior paragraph then gives that the product is $(XX_1)(XX_2)$ · · · $(XX_{\varphi(m)})$ =X_1X_2· · · $X_{\varphi(m)}$.

Finally, let A = X_1X_2· · · $X_{\varphi(m)}$, and for any X ∈ $U_m$consider $X_{\varphi(m)}$A.The

commutative property of Group Theorem gives that

$$X^{\varphi(m)}A = X^{\varphi(m)}X_1X_2 \cdot \cdot \cdot X^{\varphi(m)} = (XX_1)(XX_2) \cdot \cdot \cdot (XX^{\varphi(m)}).$$

The prior paragraph then shows that $X^{\varphi(m)}A = A$.

Multiplying both sides of that equation by the inverse $A*$of A gives

$(X^{\varphi(m)}A)A* = X^{\varphi(m)}(AA*) = X^{\varphi(m)}[1] = X^{\varphi(m)}$on the left and $AA* = [1]$ on the right, as desired.

Example Fix m = 12. The positive integers a < m with gcd(a, m) = 1are 1, 5, 7 and 11, and so φ(m) = 4.

Solutions: We will check Euler's result for all four.
First, $1^4 \equiv 1 \pmod{12}$ is clear.
Next, $5^2 \equiv 1 \pmod{12}$ since $12 \mid 25-1$, and
so $5^4 \equiv (5^2)^2 \equiv 12 \pmod{12}$.
From that one, and because $7 \equiv -5 \pmod{12}$
and 4 is even, $7^4 \equiv 5^4 \pmod{12} \equiv 1 \pmod{12}$.
And, fourth, $11 \equiv -1 \pmod{12}$and again since 4 is even we have that
$11^4 \equiv (-1)^4 \pmod{12} \equiv 1 \pmod{12}$.

9.3 FERMAT'S LITTLE THEOREM

9.3.1 Theorem (Fermat's Little Theorem)

If p is prime, and a is relatively prime top, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Where p is prime, φ(p) = p − 1.

Example Fermat's Little Theorem can simplify the computation of a mod p where p is prime. Recall that if $a^n \equiv r \pmod{p}$ where $0 \leq r < p$, thena^nmod p = r. We can do two things to simplify the computation:
(i) replace aby a mod p, and (ii) replace n by n mod (p − 1).

Suppose that we want to calculate $1234^{7865435}$ mod 11. Note that 1234

≡−1 + 2 − 3 + 4 (mod 11), that is, 1234 ≡ 2 (mod 11). Since gcd(2, 11) = 1 wehave that $2^{10} \equiv 1 \pmod{11}$.

Now 7865435 = (786543) · 10 + 5 so

$2^{7865435} \equiv 2^{(786543)\cdot 10+5} \pmod{11}$

$\equiv (2^{10})^{786543} \cdot 2^5 \pmod{11}$

$\equiv 1^{786543} \cdot 2^5 \pmod{11}$

$\equiv 2^5 \pmod{11}$,

and $2^5 = 32 \equiv 10 \pmod{11}$.

Hence, $1234^{7865435} \equiv 10 \pmod{11}$. It follows that $1234^{7865435} \bmod 11 = 10$.

Remark Fermat's theorem is called "little " as a contrast with Fermat'sLast Theorem, which states that xn + yn = zn has no solutions x, y, z ∈ Nwhen n >2. For many years this was the most famous unsolved problem in Mathematics, until it was proved by Andrew Wiles in 1995, over 350 years afterit was first mentioned by Fermat.

Corollary 9.3.2 .

If pis a prime, then $a^p \equiv a \pmod{p}$ for any integer a.

Proof. When p | a, the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a \pmod{p}$. If p ∤ a, then according to Fermat's theorem, we have $a^{p-1} \equiv 1 \pmod{p}$. When this congruence is multiplied by a, the conclusion $a^p \equiv a \pmod{p}$ follows. There is a different proof of the fact that $a^p \equiv a \pmod{p}$, involving induction on a. If a= 1, the assertion is that $1^p \equiv 1 \pmod{p}$, which clearly is true, as is the case a = 0. Assuming that the result holds for a, we must confirm its validity for a + 1. In light of the binomial theorem,

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

where the coefficient $\binom{p}{k}$ is given by

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k}$$

Our argument hinges on the observation that $\binom{p}{k}$ =0 (mod p) for 1 ≤ k ≤ p - 1. To see this, note that

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1) \equiv 0 \pmod{p}$$

by virtue of which p | k! or p| $\binom{p}{k}$. But p | k! implies that p | j for some j satisfying 1 ≤ j ≤ k ≤ p -1, an absurdity. Therefore, p | $\binom{p}{k}$. or, converting to a congruence statement,

$$\binom{p}{k} \equiv 0 \pmod{p}$$

The point we wish to make is that

$$(a+1)^p = a^p + 1 = a + 1 \pmod{p}$$

where the rightmost congruence uses our inductive assumption. Thus, the desired conclusion holds for a + 1 and, in consequence, for all a ≥ 0. If a happens to be a negative integer, there is no problem: because a≡ r (mod p) for some r, where 0 ≤ r ≤ p - 1, we get $a^p \equiv r^P \equiv r \equiv a \pmod{p}$.

Lemma 9.3.3:

If p and q are distinct primes with aP =a (mod q) and aq =a (mod p), then $a^{pq} \equiv a \pmod{pq}$.

Proof. The last corollary tells us that $(a^q)^p \equiv a^q \pmod{p}$, whereas $a^q \equiv a \pmod{p}$ holds by hypothesis. Combining these congruences, we obtain $a^{pq} \equiv a \pmod{p}$ or, in different terms, pI a^{pq} -a. In an entirely similar manner, q | a^{pq} -a. pq | a^{pq} -a, which can be recast as $a^{pq} \equiv a \pmod{pq}$.

Example: Compute $11^{470} \pmod{37}$.

Solution: Since 37 is a prime, by Fermat's little theorem,

$$a^{36} \equiv 1 \pmod{37}.$$

Hence

$$a^{r+36b} \equiv a^r \pmod{37}.$$

Write, using the Euclidean algorithm,

$$470 = 36b + r, \qquad 0 \le r < 37$$
$$= 36 \cdot 13 + 2$$
$$\Rightarrow 11^{470} \equiv 11^2 \pmod{37}$$
$$\equiv 10 \pmod{37}.$$

Example: Show that the inverse of 5 modulo 101 is 5^{99}

Solution: By Fermat's Little Theorem, $5^{100} \equiv 1 \pmod{101}$, so
$5^{99} \cdot 5 \equiv 5 \cdot 5^{99} \equiv 1 \pmod{101}$,
which by definition means that 5^{99} is the inverse of 5 modulo 101

CHECK YOUR PROGRESS 1

1. Define power of residue class

2. State and explain Fermat's Little Theorem

9.4 THE FERMAT-KRAITCHIK FACTORIZATION METHOD

Fermat's factorization method, named after Pierre de Fermat, is based on the representation of an odd integer as the difference of two squares:

The Fermat method can be applied to arbitrary odd n to try to find a divisor/complementary divisor pair that are relatively close together, if such a pair exists.

Suppose that n = ab with a > b odd. Notice that n = ab

$$= \left(\frac{a+b}{2} + \frac{a-b}{2}\right)\left(\frac{a+b}{2} - \frac{a-b}{2}\right)$$
$$= \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

If a and b are close together, then:

$\frac{a-b}{2}$ is relatively small; specifically we assume $\frac{a-b}{2\sqrt{2b}} < \epsilon$

$\frac{a+b}{2}$ is not much larger than $\sqrt{n}$

To quantify this final statement note that

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 \Rightarrow \left(\frac{a+b}{2}\right)^2 - n = \left(\frac{a-b}{2}\right)^2$$

and hence

$$\left(\frac{a+b}{2} - \sqrt{n}\right)\left(\frac{a+b}{2} + \sqrt{n}\right) = \left(\frac{a-b}{2}\right)^2.$$

Since

$$\left(\frac{a+b}{2} + \sqrt{n}\right) > 2b \quad \text{and} \quad \left(\frac{a-b}{2}\right)^2 > 0$$

we obtain

$$0 < \frac{a+b}{2} - \sqrt{n} < \left(\frac{a-b}{2\sqrt{2b}}\right)^2 < \epsilon^2.$$

9.4.1 The Algorithm: Fermat Factorization

Moral: If n is the product of two distinct odd numbers that are close together, then

$n = t^2 - s^2$

where t is slightly larger than $\sqrt{n}$ and s is relatively small. How can we

$$\sqrt{t_0^2 - n}, \sqrt{(t_0+1)^2 - n}, \sqrt{(t_0+2)^2 - n}, \sqrt{(t_0+3)^2 - n}, \ldots$$

use this to factor n? Set $t_0 = \lceil \sqrt{n} \rceil$ and successively compute

until one obtains

$$\sqrt{(t_0+k)^2 - n} = s \in \mathbb{N}.$$

If we set $t = t_0 + k$, then $n = t^2 - s^2 = (t + s)(t - s)$.

Remarks:

- ✓ Because of our assumption on (a − b)/2, this process is guaranteed to stop after roughly ϵ^2 steps.
- ✓ The factors (t + s) and (t − s) are nontrivial because t ~ $\sqrt{n}$ while s ~ 0.

Example: Apply the Fermat Factorization Method to factor n = 2251644881930449333.

Solution: We have $t_0 = d\sqrt{n} = 1500548194$.

Moreover, we find that

$$\sqrt{t_0^2 - n} = \sqrt{586212303} = 24211.821\ldots,$$
$$\sqrt{(t_0+1)^2 - n} = 2\sqrt{896827173} = 59894.145\ldots,$$
$$\sqrt{(t_0+2)^2 - n} = \sqrt{6588405083} = 81168.990\ldots,$$
$$\sqrt{(t_0+3)^2 - n} = 97926$$

so that $t = t_0 + 3 = 1500548197$ and $s = 97926$. Hence $n = pq$ with

$p = t + s = 1500646123$,

$q = t - s = 1500450271$,

both of which turn out to be prime.

Note

$$\left(\frac{p-q}{2\sqrt{2q}}\right)^2 = 3.1955\ldots.$$

Example: The integer n =8956494142912946049415883818712449246261041215620422273183844943817234975145408604748034940414795 29 is the product of two primes. Use Fermat Factorization to find them.

Solution : We have

$t_0 = d\sqrt{n}$

= 29927402397991286489627871143011285937749436382209

and with the aid of a computer we find that

$q(t_0 + 18)^2 - n = 33408832099552561140000000$.

Hence

s = 33408832099552561140000000,

t = 29927402397991286489627871143011285937749436382227,

so that the prime factorization of n is pq where

p = 29927402397991286489627837734179186385188296382227,

q = 29927402397991286489627904551843385490310576382227.

Note that $\left(\frac{p-q}{2\sqrt{2p}}\right)^2$ = 18.6476 . . ..

Remark: Factoring n in this manner only took a matter of minutes using Maple. However, after over 8 hours neither Maple nor PARI could successfully factor n naïvely.

Example To illustrate the application of Fermat's method, let us factor the integer n = 119143. Solution : From a table of squares, we find that $345^2 < 119143 < 346^2$; thus it suffices to consider values of k^2 - 119143 for those k that satisfy the inequality $346 \leq k < (119143 + 1)/2 = 59572$.

The calculations begin as follows:

346^2 - 119143 = 119716- 119143 = 573

347^2 - 119143 = 120409- 119143 = 1266

348^2 - 119143 = 121104- 119143 = 1961

349^2 - 119143 = 121801 - 119143 = 2658

350^2 - 119143 = 122500- 119143 = 3357

351^2 - 119143 = 123201- 119143 = 4058

352^2 - 119143 = 123904- 119143 = 4761 = 69^2

This last line exhibits the factorization

$119143 = 352^2 - 69^2 = (352 + 69)(352- 69) = 421 . 283$

the two factors themselves being prime. In only seven trials, we have obtained the prime factorization of the number 119143. Of course, one does not always fare so luckily; it may take many steps before a difference turns out to be a square.

Example. Suppose we wish to factor the positive integer n = 2189 and happen to notice that $579^2 = 18^2 \pmod{2189}$.

Solution : Then we compute

$$\gcd(579- 18, 2189) = \gcd(561 , 2189) = 11$$

using the Euclidean Algorithm:

$$2189 = 3 . 561 + 506$$

$$561 = 1. 506 +55$$

$$506 = 9 . 55 + 11$$

$$55= 5. 11$$

This leads to the prime divisor 11 of 2189. The other factor, namely 199, can be obtained by observing that

gcd(579 + 18, 2189) = gcd(597, 2189) = 199

Why weconsider 579. As 579, whose bsquare modulo 2189 also turns out to be a perfect square. In looking for squares close to multiples of 2189, it was observed that

$$81^2 - 3 \cdot 2189 = -6 \text{ and } 155^2 - 11 \cdot 2189 = -54$$

which translates into

$$81^2 = -2 \cdot 3 \pmod{2189} \text{ and } 155^2 = -2 \cdot 33 \pmod{2189}$$

When these congruences are multiplied, they produce

$$(81 \cdot 155)^2 = (2 \cdot 3^2)^2 \pmod{2189}$$

Because the product $81 \cdot 155 = 12555 = -579 \pmod{2189}$, we ended up with the congruence $579^2 = 18^2 \pmod{2189}$.

The basis of our approach is to find several x_i having the property that each x_i is, modulo n, the product of small prime powers, and such that their product's square is congruent to a perfect square. When n has more than two prime factors, our factorization algorithm may still be applied; however, there is no guarantee that a particular solution ofthe congruence

$$x^2 = y^2 \pmod{n}, \text{ with } x \not\equiv \pm y \pmod{n},$$

will result in a nontrivial divisor of n.

Example Let n = 12499 be the integer to be factored. The first square just larger than n is $112^2 = 12544$. So we begin by considering the sequence of numbers $x^2 - n$ for x = 112, 113, ... As before, our interest is in obtaining a set of values $x_1, x_2, \bullet\bullet\bullet, x_k$ for which the product $(x_i - n) \cdot \cdot \cdot (x_k - n)$ is a square, say y^2 • Then $(x_1 \bullet \bullet \bullet x_k)^2 = y^2 \pmod{n}$, which might lead to a nontrivial factor of n.

A short search reveals that

$$112^2 - 12499 = 45$$

$$117^2 - 12499 = 1190$$

$$121^2 - 12499 = 2142$$

or, written as congruences,

$$112^2 = 32 \bullet 5 \pmod{12499}$$

$$117^2 = 2.\ 5.\ 7 \cdot 17 \pmod{12499}$$

$$121^2 = 2.\ 32 \bullet 7 \cdot 17 \pmod{12499}$$

Multiplying these together results in the congruence

$$(112 \cdot 117 \cdot 121)^2 = (2 \cdot 32 \cdot 5 \cdot 7 \cdot 17)^2 \pmod{12499}$$

that is,

$$15855842 = 107102 \pmod{12499}$$

But we are unlucky with this square combination. Because

$$1585584 = 10710 \pmod{12499}$$

only a trivial divisor of 12499 will be found. To be specific,

$$\gcd(1585584 + 10710, 12499) = 1$$

$$\gcd(1585584 - 10710, 12499) = 12499$$

After further calculation, we notice that

$$113^2 = 2 \cdot 5 \cdot 33 \pmod{12499}$$

$$127^2 = 2.\ 3 \cdot 5 \cdot 112 \pmod{12499}$$

which gives rise to the congruence

$$(113 \cdot 127)2 = (2 \cdot 32 \cdot 5 \cdot 11)2 \pmod{12499}$$

This reduces modulo 12499 to

$$1852^2 = 990^2 \pmod{12499}$$

and fortunately $1852 \not\equiv \pm 990 \pmod{12499}$.

Calculating

$\gcd(1852 - 990, 12499) = \gcd(862, 12499) = 431$

produces the factorization $12499 = 29 \cdot 431$.

9.5 WILSON'S THEOREM

A positive integer n (>1) is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$. At first glance it seems that proving (1) is a really difficult job, but proving (2) shouldn't be that hard. Surprisingly, the situation is exactly opposite. Proofs of (1) and (2) are included separately below.

(1): Assuming n a composite number, we show a contradiction. If n is a composite number then it has at least one divisor d less than n, that is $d \leq n-1$. But since $(n-1)!$ is the product of all positive integers from 1 to $n-1$, the product must contain d and thus be divisible by d. So we have $(n-1)! \equiv 0 \pmod{d}$. Also $(n-1)! \equiv 0 \not\equiv -1 \pmod{d}$ since $d|n$, contradicting the hypothesis. So n can't be composite, hence prime.

(2): Consider the $\mathbb{Z}_p$ This is just the set of integers modulo p, i.e. contains all integers from 0 to $p-1$. All the operations are done in modulo p. For example, in this field $5 + (p - 2) = 3$ since

$$5 + (p-2) = p+3 \equiv 3 \pmod{p}.$$

Now consider the polynomial $f(x) = x^{p-1}-1$, which clearly has $p-1$ roots by the fundamental theorem of algebra. Also $x^{p-1}-1 \equiv 0 \pmod{p}$ for all $1 \leq x \leq p-1$ by Fermat's little theorem
since p is a prime. So in $\mathbb{Z}_p$ these must be the $p-1$ roots of f. Hence we can write

$$x^{p-1} - 1 = \prod_{k=1}^{p-1}(x-k) = (-1)^{p-1}\prod_{k=1}^{p-1}(k-x) = \prod_{k=1}^{p-1}(k-x)$$

because for odd primes, $p-1$ is even, implying $(-1)^{p-1}=1$, and for even prime 2 we have $(-1)^{p-1} = -1 \equiv 1 \pmod{2}$. Now simply plugging in x=0 in the last equation we get

$$-1 = \prod_{k=1}^{p-1} k = (p-1)!$$

$\mathbb{Z}_p$. $(p-1)! \equiv -1 \pmod{p}$.

Example: Prove that $437|(18!+1)$.

Solution : First notice that $437=19\times23$ and so it suffices to prove that

$$18!\equiv -1 \pmod{19}, \pmod{23}.$$

Now since 19 is a prime, $18!\equiv -1 \pmod{19}$ immediately follows by Wilson's theorem. Also noting that 23 is a prime, we have \begin

$$24\times 18! = 18!\times(-1)\times(-2)\times(-3)\times(-4)$$

$$\equiv 18!\times 19\times 20\times 21\times 22$$

$$= 22! \equiv -1 \equiv -24 \pmod{23},$$

and thus $18!\equiv -1 \pmod{23}$ as well.

Therefore, 437|(18!+1).

Example: Let a ∈ N such that

factorization

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{23}=\frac{a}{23!}.$$

Find a(mod13).

Solution : Rewrite the equation as

$$a = 23! + \frac{23!}{2} + \frac{23!}{3} + \cdots + \frac{23!}{23}.$$

Clearly all the terms in the right side are integers. Also except \frac{23!}{13}1323!, all the quotients contain the factor 1313 and thus are divisible by 1313. Therefore, we get

$$\begin{aligned} a = & \quad 23! + \frac{23!}{2} + \frac{23!}{3} + \cdots + \frac{23!}{23} \\ \equiv & \quad \frac{23!}{13} = 1\times 2\times\cdots\times 12\times 14\times\cdots\times 23 \\ \equiv & \quad (1\times 2\times\cdots\times 12)\times(1\times 2\times\cdots\times 10) \\ = & \quad 12!\times 10! \overset{\text{Wilson's}}{\equiv} 12\times 10! \pmod{13}. \end{aligned}$$

So we know that $a \equiv 12\times10!(\text{mod}13)$. Now we use $11!\equiv1\equiv66(\text{mod}13)$, which follows byWilson's. $10!\equiv6(\text{mod}13)$. Finally we have

$$a \equiv 12\times10! \equiv 12\times6 \equiv 7(\text{mod}13)$$

Example: Let p be an odd prime. Let $A=\{a1,a2,\ldots,ap\}$ and $B=\{b1,b2,\ldots,bp\}$ be complete sets of residue classes modulo p. Show that the set $\{a1b1,a2b2,\ldots,apbp\}$ is not a complete set of residue classes.

We will prove by contradiction. Suppose there exist sets A, B which give us a complete set of residue classes.

Solution : First, if there exists $a_i \equiv b_j \equiv 0$, then $aibi\equiv ajbj\equiv0$, which would not give us a complete set of residue classes. Thus, we may assume that $a\,i \equiv bi \equiv 0(\text{mod}p)$. WLOG, i=p.

By Wilson's theorem, we get that

$$\prod_{i=1}^{p-1} a_i \equiv -1 \pmod{p} \text{ and } \prod_{i=1}^{p-1} b_i \equiv -1 \pmod{p}.$$

If $\{aibi\}_{i=1}^{p-1}$ form a complete set of non-zero residue class, then we must have

$$-1 \equiv \prod_{i=1}^{p-1} a_i b_i \equiv \prod_{i=1}^{p-1} a_i \prod_{i=1}^{p-1} b_i \equiv (-1)\times(-1) \equiv 1 \pmod{p}.$$

Since p is an odd prime, $p > 2p > 2$ and we have $-1\not\equiv1(\text{mod}p)$, which is a contradiction. Hence, {aibi} is not a complete set of residue classes.

Check Your Progress 2

3. Explain Femat's Factorization Method

4. What do you understand by Wilson's Theorem

9.6 SUMMARY

Fermat's Little Theorem is much easier toprove, but has more far-reaching consequences for applications to cryptographyand secure transmission of data on the Internet. Fermat's theorem has many applications and is central to much of what is done in number theory. In the least, it can be a labor-saving device in certain calculations. Fermat Factorization method is used for factoring large numbers.--

9.7 KEYWORDS

1. Residue Class: A **residue class** is a complete set of integers that are congruent modulo for some positive integer
2. Factorization : In **math**, **factorization** is when you break a number down into smaller numbers that, multiplied together, give you that original number.
3. **Congruence: in mathematics**, a term employed in several senses, each connoting harmonious relation, agreement, or correspondence
4. **Trivial :** In mathematics, the adjective **trivial** is frequently used for objects (for example, groups or topological spaces) that have a very simple structure. The noun **triviality** usually refers to a simple technical aspect of some proof or definition.

9.8 QUESTIONS FOR REVIEW

1. Use Fermat's theorem to verify that 17 divides $11^{104} + 1$.

2. Find the units digit of 3^{100} by the use of Fermat's theorem.

3. Assuming that a and bare integers not divisible by the prime p, establish the following:

(a) If $a^P = b^P \pmod p$, then $a = b \pmod p$.

4. Use Fermat's method to factor each of the following numbers:

(a) 2279.

(b) 10541.

5. (a) Factor the number 4537 by searching for x such that $x^2 - k \cdot 4537$ is the product of small prime powers.

9.9 SUGGESTED READINGS

- David M. Burton, Elementary Number Theory, University of New Hampshire.
- G.H. Hardy, and , E.M. Wrigh,. An Introduction to the Theory of Numbers (6th ed, Oxford University Press, (2008).
- W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.
- A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.
- I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.
- T.M. Apostol, Introduction to Analytic number theory, UTM, Springer, (1976).
- J. W. S Cassel, A. Frolich, Algebraic number theory, Cambridge.
- M Ram Murty, Problems in analytic number theory, springer.
- M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer.

9.10 ANSWERS TO CHECK YOUR PROGRESS

1. [HINT: Provide definition and example 9.1]
2. [HINT: Provide statement, proof and example 9.2.1]
3. [HINT: Provide algorithm of Fermat's Factorization and example --9.3.1]
4. [HINT: Provide explanation—9.4]

UNIT 10: ARITHMETIC FUNCTIONS I

STRUCTURE

10.0 OBJECTIVE

Understand the concept of Arithmetic Functions and its properties
Learn the concept of Mobius Inversion Formula
Understand the Greatest Integer Function

10.1 INTRODUCTION

In number theory, an arithmetic, arithmetical, or number-theoretic function is for most authors any function f(n) whose domain is the positive integers and whose range is a subset of the complex numbers. Hardy & Wright include in their definition the requirement that an arithmetical function "expresses some arithmetical property of n".
An example of an arithmetic function is the divisor function whose value at a positive integer n is equal to the number of divisors of n.
There is a larger class of number-theoretic functions that do not fit the above definition, e.g. the prime-counting functions.

10.2 ARITHMETIC FUNCTIONS

Functions that are defined for all positive integers and whose range is a subset of **R** (or more generally **C**) are called arithmetic functions. We have already considered one very important arithmetic functions – the Euler φ-function. Other important arithmetic functions to be considered in this section are

• τ(n), the number of positive divisors of n;

• σ(n), the sum of the positive divisors of n;

• σk(n), the sum of the kth powers of the positive divisors of n.

We will use the following sum and product conventions. $\sum_{d|n} f(d)$ and $\prod_{d|n} f(d)$ denote the sum and product, respectively, of f(d) over all positive divisors d of n.

For example,

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

Using this notation, we have

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d \qquad \sigma_k(n) = \sum_{d|n} d^k$$

Note that the divisor functions τ(n) and σ(n) are special cases of $\sigma_k(n)$, since $\tau(n) = \sigma_0(n)$ and $\sigma(n) = \sigma_1(n)$.

10.2.1 Definition

An arithmetic function f(n) is called multiplicative if it is not identically zero and satisfies f(mn) = f(m)f(n) for every pair of relatively prime positive integers m and n. If f(mn) = f(m)f(n) for each pair m and n, relatively prime or not, then f(n) is said to be completely multiplicative.

If f is a multiplicative function, then f(n) = f(n)f(1) for every positive integer n, and since there is an n for which f(n) ≠ 0, it follows that f(1) = 1. Using mathematical induction, it is easy to prove that if $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers, then

$$f(m_1 m_2 \cdots m_r) = f(m_1)f(m_2) \cdots f(m_r).$$

In particular, this holds whenever the integers $m_1, m_2, \ldots, m_r$ are powers of distinct primes. Thus, if n = $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ is the canonical

factorization of the integer n > 1 as a product of powers of distinct primes, then f(n) = f($p_1^{k_1}$)f($p_2^{k_2}$) · · · f($p_r^{k_r}$). Therefore, the value of f(n) for every n is completely determined by the values f(p^k) for all prime powers.

We already know that φ(n) is multiplicative and we have used this fact to obtain a formula for φ(n).

OR

Definition. A number-theoretic function f is said to be multiplicative if

f(mn) = f(m)f(n)

whenever gcd(m, n) = 1

10.2.2 Theorem

Let f(n) be a multiplicative function, and let F (n) = $\sum_{d|n} f(d)$. Then F (n) is multiplicative.

Proof. Let (m, n) = 1. If d | mn, then d = d1d2, where d1 | m and d2 | n. Moreover, d1 = (m, d), d2 = (n, d) and (d1, d2) = 1, and the factorization is unique. Consequently,

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m}\sum_{d_2|n} f(d_1d_2) = \sum_{d_1|m}\sum_{d_2|n} f(d_1)f(d_2)$$
$$= \sum_{d_1|m} f(d_1)\sum_{d_2|n} f(d_2) = F(m)F(n).$$

10.2. 3 Corollary

(i) The functions τ(n), σ(n), and more generally, $\sigma_k(n)$ are multiplicative.

(ii) If n = $p_1^{k_1}, p_2^{k_2}, \ldots, p_r^{k_r}$, then

$$\tau(n) = \prod_{j=1}^{r}(k_j + 1) \qquad and \qquad \sigma(n) = \prod_{j=1}^{r}\left(\frac{p_j^{k_j+1} - 1}{p_j - 1}\right).$$

Proof.

(i) Since $\sigma_k(n) = \sum_{d|n} d^k$ and the function f(n) = n^k is (completely) multiplicative, it follows from the previous theorem that σk(n) is

multiplicative. τ(n) and σ(n) are special cases.

(ii) The positive divisors of p^k are 1, p, p^2, . . . , p^k, and hence $\tau(p^k) = k + 1$ and $\sigma(p^k) = \sum_{j=0}^{k} p^j = (p^{k+1} - 1)/(p - 1)$. The formulas for τ(n) and σ(n) follow from this.

10.2.4 Theorem

For every positive integer n, $\sigma(d) = \sum_{d|n} n$.

Proof. Write F (n) = $\sum_{d|n} \varphi(d)$; then F (n) is multiplicative by Theorem 10.2. Since the function G(n) = n is also multiplicative, it suffices to verify that F (p^k) = p^k for all prime powers p^k in order to prove that F (n) = n for all n.

But $\varphi(p^j) = p^j - p^{j-1}$ for $j \geq 1$, and hence

$$F(p^k) = \sum_{d|p^k} \phi(d) = \sum_{j=0}^{k} \phi(p^j) = 1 + \sum_{j=1}^{k} (p^j - p^{j-1}) = p^k.$$

Let f(n) be an arithmetic function, and define F (n) = $\sum_{d|n} f(n)$.Is thefunction f uniquely determined by the function F ? We have

$$\begin{cases} F(1) = f(1) \\ F(2) = f(1) + f(2) \\ F(3) = f(1) \quad + f(3) \\ F(4) = f(1) + f(2) \quad + f(4) \\ F(5) = f(1) \quad + f(5) \\ \quad \vdots \\ F(n) = f(1) + \quad \ldots \quad + f(n) \end{cases}$$

This can be viewed as a triangular system of linear equations with f(1), f(2),. . . , f(n) as unknowns. It is now obvious that f(n) is a linear combination of F (1), F (2), . . . , F (n) with integral coefficients. In particular, the function f is uniquely determined by the function F . Our next objective is to derive a formula for f(n), and for this we will need the following function.

Notes

Example. The number 180 = 22 • 32 · 5 has

r(180) = (2 + 1)(2 + 1)(1 + 1) = 18

positive divisors. These are integers of the form

$2^{a_1}.3^{a_2}.5^{a_3}$

where $a_1 = 0, 1, 2$; $a_2 = 0, 1, 2$; and $a_3 = 0, 1$.

Specifically, we obtain

1,2,3,4,5,6,9, 10, 12, 15, 18,20,30,36,45,60,90, 180

The sum of these integers is

$$\sigma(180) = \frac{2^3 - 1}{2 - 1}\,\frac{3^3 - 1}{3 - 1}\,\frac{5^2 - 1}{5 - 1} = \frac{7}{1}\,\frac{26}{2}\,\frac{24}{4} = 7 \cdot 13 \cdot 6 = 546$$

CHECK YOUR PROGRESS 1

1. What is Arithmetic Function?

2. Explain multiplicative.

10.3 THE MOBIUS INVERSION FORMULA

10.3.1 Definition

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is divisible by } p^2 \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_1, p_2, \ldots, p_r \text{ are distinct primes.} \end{cases}$$

The function μ is called Mobius' μ-function.

10.3.2 Theorem

The function μ(n) is multiplicative and

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. Multiplicativity is obvious. Define F (n) = $\sum_{d|n} \mu(d)$; then F (n) is multiplicative by Theorem 10.2. Since μ(p) = −1 and μ(p^j) = 0 for j ≥ 2, we have

$$F(p^k) = \sum_{j=0}^{k} \mu(p^j) = \mu(1) + \mu(p) = 1 - 1 = 0,$$

for all primes p and all k ≥ 1.

Hence, F (n) = 0 for all n > 1, and F (1) = μ(1) = 1.

Let us see what happens if JL(d) is evaluated for all the positive divisors d of an integer n and the results are added. In the case where n = 1, the answer is easy;

here,

$$\sum_{d|1} \mu(\mathrm{d}) = \mu(1) = 1$$

Suppose that n > **1** and put

$$F(n) = \sum_{d|n} \mu(\mathrm{d})$$

To prepare the ground, we first calculate F(n) for the power of a prime, say, n = pk.

$$F(p^k) = \sum_{d \mid p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k)$$
$$= \mu(1) + \mu(p) = 1 + (-1) = 0$$

The positive divisors of pk are just the k + 1 integers 1, p, p2, ... , pk, so that Because f.L is known to be a multiplicative function, an appeal to Theorem 6.4 is legitimate; this result guarantees that F also is multiplicative. Thus, if the canonical factorization ofn is n = p~1 p~2 • • • p~', then F (n) is the product ofthe values assigned to F for the prime powers in this representation:

$$F(n) = F(p_1^{k_1})F(p_2^{k_2}) \cdots F(p_r^{k_r}).$$

For an illustration of this last theorem, consider n = 10. The positive divisors of 10 are 1, 2, 5, 10 and the desired sum is

$$\sum_{d \mid 10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10)$$
$$= 1 + (-1) + (-1) + 1 = 0$$

10.3.3 Theorem

(Mobius' inversion formula) Let f be an arbitrary arithmetic function. If F (n) = $\sum_{d \mid n} f(d)$ for every positive integer n, then

$$f(n) = \sum_{d \mid n} \mu(d) F(n/d).$$

Proof. Using the definition of F we obtain

$$\sum_{d \mid n} \mu(d) F(n/d) = \sum_{d \mid n} \mu(d) \sum_{k \mid (n/d)} f(k) = \sum_{\text{all } d,\ k \text{ with } dk \mid n} \mu(d) f(k).$$

Now we can reverse the order of summation and write the last sum in the form

$$\sum_{\text{all } d,\ k \text{ with } dk|n} \mu(d)f(k) = \sum_{k|n} f(k) \sum_{d|(n/k)} \mu(d).$$

By Theorem 10.2.2, $\Sigma_{d|(n/k)}\ \mu(d)$ = 0 except for k = n, when the value is 1. Hence, $\Sigma_{d|(n/k)}\ \mu(d)F\ (n/d)$ = $\Sigma_{k|n}\ f\ (k)\Sigma_{d|(n/k)}\ \mu(d)$ = f(n). The following converse is also true.

10.3.4 Theorem

If f(n) = $\Sigma_{d|n}\mu(d)$ F (n/d) for every positive integer n, then F (n) = $\Sigma_{d|n}f\ (d)$

Proof. Define G(n) = $\Sigma_{d|n}f\ (d)$ then f(n) = $\Sigma_{d|n}\mu(d)$G(n/d) by Theorem 10.2.3. Thus,

$$\sum_{d|n} \mu(d)F(n/d) = \sum_{d|n} \mu(d)G(n/d)$$

holds for all n.

We will use induction to show that this implies that F (n) = G(n) for all positive integers n.

First of all, taking n = 1 in (1) we get μ(1)F (1/1) = μ(1)G(1/1), that is F (1) = G(1). Suppose that we have F (m) = G(m) for all m < n. Since n/d < n for all positive divisors d of n except for d = 1, (1) now simplifies to μ(1)F (n/1) = μ(1)G(n/1), and we conclude that F (n) = G(n). This completes the induction.

For n ≥1, we define the sum

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

Then M(n) is the difference between the number of square-free positive integers k ~ n with an even number of prime factors and those with an odd number of prime factors.

For example, M(9) = 2 – 4 = –2.

Check Your Progress 2

3. State Mobius μ Function?

4. Explain Mobius inverse Function.

10.4 THE GREATEST INTEGER FUNCTION

Definition. For a real number x, denote by bxc the largest integer less than or equal to x.

A couple of trivial facts about bxc:

- $\lfloor x \rfloor$ is the unique integer satisfying $x - 1 < \lfloor x \rfloor \leq x$.
- $\lfloor x \rfloor = x$ if and only if x is an integer.
- Any real number x can be written as $x = \lfloor x \rfloor + \theta$, where $0 \leq \theta < 1$.

PROPERTIES

For x a real number and n and integer:

1. bx + nc = bxc + n.

2. $$\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor & \text{if } x = \lfloor x \rfloor, \\ -\lfloor x \rfloor - 1 & \text{if } x \neq \lfloor x \rfloor. \end{cases}$$

3. $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$ if $n \geq 1$.

4. $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$. More generally,

$$\lfloor nx \rfloor = \sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor .$$

10.4.1 Theorem

If n is a positive integer and $\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]$ p a prime, then the exponent of the highest power of p that divides n! is

where the series is finite, because $[n/ p^k] = 0$ for $p^k > n$.

Proof. Among the first n positive integers, those divisible by p are p, 2p, ... , tp, where t is the largest integer such that $tp \leq n$; in other words, t is the largest integer less than or equal to say n/p (which is to say $t = [n/ p]$). Thus, there are exactly [n/ p] multiples of p occurring in the product that defines n!, namely,

$$p, 2p, \ldots, \left[\frac{n}{p} \right] p \qquad (1)$$

The exponent of p in the prime factorization of n! is obtained by adding to the number of integers in Eq. (1), the number of integers among 1, 2, ... , n divisible by p^2, and then the number divisible by p^3, and so on. Reasoning as in the first paragraph, the integers between 1 and n that are divisible by p^2 are

$$p^2, 2p^2, \ldots, \left[\frac{n}{p^2} \right] p^2 \qquad (2)$$

which are $[n/p^2]$ in number. Of these, $[n/ p^3]$ are again divisible by p:

$$p^3, 2p^3, \ldots, \left[\frac{n}{p^3} \right] p^3 \qquad (3)$$

After a finite number of repetitions of this process, we are led to conclude that the total number of times p divides n! is

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]$$

This result can be cast as the following equation, which usually appears under the name of the Legendre formula:

$$n! = \prod_{p \le n} p^{\sum_{k=1}^{\infty} [n/p^k]}$$

Example: We would like to find the number of zeros with which the decimal representation of 50! terminates. In determining the number of times 10 enters into the product 50!, it is enough to find the exponents of 2 and 5 in the prime factorization of 50!, and then to select the smaller figure.

By direct calculation we see that

$$[50/2] + [50/22] + [50/23] + [50/24] + [50/25]$$
$$= 25 + 12 + 6 + 3 + 1$$
$$=47$$

Theorem 10.4.1

tells us that 247 divides 50!, but 248 does not. Similarly, $[50/5] + [50/5^2]$ = 10 + 2 = 12 and so the highest power of 5 dividing 50! is 12. This means that 50! ends with 12 zeros

Theorem 10.4.2

. If n and r are positive integers with $1 \leq r < n$, then the binomial coefficient

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is also an integer.

Proof. The argument rests on the observation that if a and b are arbitrary real numbers, then [a+ b] ~[a]+ [b]. In particular, for each primefactor p of r!(n- r)!,

$$\left[\frac{n}{p^k}\right] \geq \left[\frac{r}{p^k}\right] + \left[\frac{(n-r)}{p^k}\right] \qquad k = 1, 2, \ldots$$

Adding these inequalities, we obtain

The left-hand side of Eq. (1) gives the exponent of the highest power of the prime p that divides n!, whereas the right-hand side equals the highest power of this prime contained in **r!(n- r)!.** Hence, p appears in the numerator of **n! /r!(n- r)!** at least as many times as it occurs in the denominator. Because this holds true for every prime divisor of the denominator, **r!(n- r)!** mustdividen!, making **n!/r!(n- r)!** an integer.

10.4.3 Corollary

For a positive integer r, the product of any r consecutive positive integers is divisible by r!.

Proof. The product of r consecutive positive integers, the largest of which is n, is

$$n(n - l)(n - 2) \cdot \cdot \cdot (n - r + 1)$$

Now we have

Because **n!/r !(n - r)!** is an integer by the theorem, it follows that r! must divide the product n(n - 1) · ··(n - r + 1), as asserted.

10.4.4 Theorem

Let f and F be number-theoretic functions such that

$$F(n) = \sum_{d|n} f(d)$$

Then, for any positive integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$$

Proof. We begin by noting that

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d \mid n} f(d) \qquad (1)$$

The strategy is to collect terms with equal values of f(d) in this double sum. For a fixed positive integer k ~ N, the term f(k) appears in Ldln f(d) if and only if k is a divisor of n. (Because each integer has itself as a divisor, the right-hand side of Eq. (1) includes f(k), at least once.) Now, to calculate the number of sums Ld_1 n f(d) in which f(k) occurs as a term, it is sufficient to find the number of integers among 1, 2, ... , N, which are divisible by k. There are exactly [N / k] ofthem:

k, 2k, 3k, ... , $\left[\frac{N}{k}\right] k$

Thus, for each k such that 1 ~ k ~ N, f(k) is a term of the sum $\sum_{d|n} f(d)$ for [N / k] different positive integers less than or equal to N. Knowing this, we may rewrite the double sum in Eq. (1) as and our task is complete.

$$\sum_{n=1}^{N} \sum_{d \mid n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

Corollary 1. If N is a positive integer, then

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$$

Proof. Noting that r(n) = Ld|n 1, we may writer for F and take ftobetheconstant function f(n) = 1 for all n.

In the same way, the relation a (n) = $\sum_{d|n} d$ yields Corollary 2.

Corollary 2. If N is a positive integer, then

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \left[\frac{N}{n}\right]$$

Example Consider the case N = 6. The definition of r tells us that

$$\sum_{n=1}^{6} \tau(n) = 14$$

From Corollary 1,

$$\begin{aligned}\sum_{n=1}^{6}\left[\frac{6}{n}\right] &= [6]+[3]+[2]+[3/2]+[6/5]+[1]\\ &= 6+3+2+1+1+1\\ &= 14\end{aligned}$$

as it should. In the present case, we also have

$$\sum_{n=1}^{6}\sigma(n) = 33$$

and a simple calculation leads to

$$\begin{aligned}\sum_{n=1}^{6} n\left[\frac{6}{n}\right] &= 1[6]+2[3]+3[2]+4[3/2]+5[6/5]+6[1]\\ &= 1\cdot 6+2\cdot 3+3\cdot 2+4\cdot 1+5\cdot 1+6\cdot 1\\ &= 33\end{aligned}$$

Check Your Progress 3

5. Define the Greatest Integer Function

2. State the properties of the Greatest Integer Function

10.5 SUMMARY

Arithmetic functions are real- or complex-valued functions defined on the set \mathbb{Z^+}Z+ of positive integers. They describe arithmetic properties of numbers and are widely used in the field of number theory.

10.6 KEYWORDS

1. Range : The **Range** is the difference between the lowest and highest values.

2. **Induction:** is a **mathematical** technique which is used to prove a statement, a formula or a theorem is true for every natural number.

3. Positive Divisor: A **positive** proper **divisor** is a **positive divisor** of a number , excluding itself. For example, 1, 2, and 3
are **positive** proper **divisors** of 6, but 6 itself is not.

4. Exponent: An **exponent** refers to the number of times a number is multiplied by itself.

10.7 QUESTIONS FOR REVIEW

1. Prove the following.
(a) r(n) is an odd integer if and only if n is a perfect square.
(b) a(n) is an odd integer if and only if n is a perfect square or twice a perfect square.

2. If n is a square-free integer, prove that $r(n) = 2^r$, where r is the number of prime divisors
of n.

3. For each positive integer n, show that $\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3) = 0$

4. Given integers a and b > 0, show that there exists a unique integer r with $0 \leq r < b$
satisfying a= [ajb]b + r.

5. Find the highest power of 5 dividing 1000! and the highest power of 7 dividing 2000!.

10.8 SUGGESTED READINGS

- David M. Burton, Elementary Number Theory, University of New Hampshire.
- G.H. Hardy, and , E.M. Wrigh,. An Introduction to the Theory of Numbers (6th ed, Oxford University Press, (2008).
- W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.
- A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.
- I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.
- T.M. Apostol, Introduction to Analytic number theory, UTM, Springer, (1976).
- J. W. S Cassel, A. Frolich, Algebraic number theory, Cambridge.
- M Ram Murty, Problems in analytic number theory, springer.
- M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer.

10.9 ANSWERS TO CHECK YOUR PROGRESS

1.[HINT: Provide both alternate definition with example 10.1.1]

2.[HINT: Provide statement of theorem related to arithmetic function being multiplicative with proof 10.1.2]

3.[HINT:Provide the definition, example and statement of theorem 10.2.1]

4.[HINT:Provide the definition, example and statement of theorem 10.2.3]

5.[HINT:Provide the definition and example 10.3 Definition]

6.[HINT: Provide properties and explain one example that applies the property 10.3 Properties]

Notes

UNIT 11: ARITHMETIC FUNCTION II

STRUCTURE

11.0 OBJECTIVE

In this unit you will explore the maggoldt function and the Dirichlet product of arithmetic functions and understand the concept of Formal Power Series and the Bell Series

11.1 INTRODUCTION

Arithmetic functions are real- or complex-valued functions defined on the set Z+ of positive integers. They describe arithmetic properties of numbers and are widely used in the field of number theory. Arithmetic functions are different from typical functions in that they cannot usually be described by simple formulas, so they are often evaluated in terms of their average or asymptotic behavior.

11.2 THE MANGOLDT FUNCTION

The von Mangoldt function, denoted by an upper-case lambda $\Lambda(n)$, is an arithmetic function that plays a critical role in the distribution of primes.

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime } p \text{ and integer } m \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

11.2.1. Theorem

We have

$$\sum_{d|n} \Lambda(d) = \log n \quad (n \in \mathbb{N}).$$

Proof. For n = 1, the identity holds since Λ(1) = 0 = log 1. For n ≥ 2 we have, by the definition of Λ,

$$\sum_{d|n} \Lambda(d) = \sum_{p^m|n} \log p = \log n.$$

(For the last step note that, for each prime power pα||n, each of the terms $p^1, p^2, \ldots, p^\alpha$ contributes a term log p to the sum, so the total contribution arising from powers of p is α(log p) = log p^α. Adding up those contributions over all prime powers $p^\alpha||n$, gives $\sum_{p^\alpha||n} \log p^\alpha = \log \prod_{p^\alpha||n} p^\alpha = \log n$.

The main motivation for introducing the von Mangoldt function is that the partial sums Pn≤x Λ(n) represent a weighted count of the prime powers $p^m \leq x$, with the weights being log p, the "correct" weights to offset the density of primes. It is not hard to show that higher prime powers (i.e.,those with m ≥ 2) contribute little to the above sum, so the sum is essentially a weighted sum over prime numbers. In fact, studying the asymptotic behavior of the above sum is essentially equivalent to studying the behavior of the prime counting function π(x); for example, the PNT is equivalent to the assertion that limx→∞(1/x) $\sum_{n<x} \Lambda(n)$ = 1. In fact, most proofs of the PNT proceed by first showing the latter relation, and then deducing from this the original form of the PNT. The reason for doing this is that, because of the identity in the above theorem (and some similar relations), working with Λ(n) is technically easier than working directly with the characteristic function of primes.

11.3 THE DIRICHLET PRODUCT OF ARITHMETIC FUNCTIONS

The two obvious operations on the set of arithmetic functions are pointwise addition and multiplication. The constant functions f = 0 and f = 1 are neutral elements with respect to these operations, and the additive and multiplicative inverses of a function f are given by −f and 1/f, respectively.

While these operations are sometimes useful, by far the most important operation among arithmetic functions is the so-called **Dirichlet product**, an operation that, at first glance, appears mysterious and unmotivated, but which has proved to be an extremely useful tool in the theory of arithmetic functions.

Definition. Given two arithmetic functions f and g, the **Dirichlet product** (or **Dirichlet convolution**) of f and g, denoted by $f * g$, is the arithmetic function defined by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

In particular, we have $(f * g)(1) = f(1)g(1)$, $(f * g)(p) = f(1)g(p) + f(p)g(1)$ for any prime p, and $(f * g)(p^m) = \sum_{k=0}^{m} f(p^k)g(p^{m-k})$ for any prime power p^m.

It is sometimes useful to write the Dirichlet product in the symmetric form

$$(f * g)(n) = \sum_{ab=n} f(a)g(b),$$

where the summation runs over all pairs (a, b) of positive integers whose product equals n. The equivalence of the two definitions follows immediately from the fact that the pairs (d, n/d), where d runs over all divisors of n, are exactly the pairs (a, b) of the above form.

One motivation for introducing this product is the fact that the definitions of many common arithmetic functions have the form of a Dirichlet

product, and that many identities among arithmetic functions can be written concisely as identities involving Dirichlet products.

11.3.1 Theorem

(Properties of the Dirichlet product)**.**

(i) The function e acts as a unit element for $*$, i.e., $f * e = e * f = f$ for all arithmetic functions f .

(ii) The Dirichlet product is commutative, i.e., $f * g = g * f$ for all f and g.

(iii) The Dirichlet product is associative, i.e., $(f * g) * h = f * (g * h)$ for all f, g, h.

(iv) If $f(1) \neq 0$, then f has a unique Dirichlet inverse, i.e., there is a unique function g such that $f * g = e$.

Proof. (i) follows immediately from the definition of the Dirichlet product. For the proof of (ii) (commutativity) and (iii) (associativity) it is useful to work with the symmetric version of the Dirichlet product, i.e., $(f * g)(n) = \sum_{ab=n} f(a)g(b)$. The commutativity of $*$ is immediate from this representation. To obtain the associativity, we apply this representation twice to get

where
$$((f * g) * h)(n) = \sum_{dc=n} (f * g)(d)h(c) = \sum_{dc=n} \sum_{ab=d} f(a)g(b)h(c)$$
$$= \sum_{abc=n} f(a)g(b)h(c),$$

the last sum runs over all triples (a, b, c) of positive integers whose product is equal to n. Replacing (f, g, h) by (g, h, f) in this formula yields the same final (triple) sum, and we conclude that $(f * g) * h = (g * h) * f = f * (g * h)$, proving that $*$ is associative.

It remains to prove (iv). Let f be an arithmetic function with $f(1) \neq 0$. By definition, a function g is a Dirichlet inverse of f if $(f * g)(1) = e(1) = 1$ and $(f * g)(n) = e(n) = 0$ for all $n \geq 2$. Writing out the Dirichlet product $(f * g)(n)$, we see that this is equivalent to the infinite system of equations

$$(A_1) \qquad f(1)g(1) = 1,$$

$$(A_n) \qquad \sum_{d|n} g(d)f(n/d) = 0 \quad (n \geq 2).$$

We need to show that the system (An)∞ n=1 has a unique solution g. We do this by inductively constructing the values g(n) and showing that these values are uniquely determined. For n = 1, equation (A1) gives g(1) = 1/f(1), which is well defined since f(1) ≠ 0. Hence, g(1) is uniquely defined and (A1) holds. Let now n ≥ 2, and suppose we have shown that there exist unique values g(1), . . . , g(n −1) so that equations (A_1)–(A_{n-1}) hold. Since f (1) ≠ 0, equation (An) is equivalent to

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} g(d)f(n/d).$$

Since the right-hand side involves only values g(d) with d < n, this determines g(n) uniquely, and defining g(n) by above equation we see that (A_n) (in addition to (A_1)–(A_{n-1})) holds. This completes the induction argument.

11.3.2 Theorem

(Dirichlet product and multiplicative functions)**.**

(i) If f and g are multiplicative, then so is f ∗ g.

(ii) If f is multiplicative, then so is the Dirichlet inverse f −1.

(iii) If f ∗ g = h and if f and h are multiplicative, then so is g.

(iv) (Distributivity with pointwise multiplication) If h is completely multiplicative, then h(f ∗ g) = (hf) ∗ (hg) for any functions f and g.

Remarks. (i) The product of two completely multiplicative functions is multiplicative (by the theorem), but not necessarily completely multiplicative.

For example, the divisor function d(n) can be expressed as a product 1 ∗ 1 in which each factor 1 is completely multiplicative, but the divisor function itself is only multiplicative in the restricted sense (i.e., with the

coprimality condition). The same applies to the Dirichlet inverse: if f is completely multiplicative, then f −1 is multiplicative, but in general not completely multiplicative.

(ii) By Theorem 1.8, any function f with $f(1) \neq 0$ has a Dirichlet inverse. Since a multiplicative function satisfies $f(1) = 1$, any multiplicative function has a Dirichlet inverse.

(iii) Note that the distributivity asserted in property (iv) only holds when the function h is completely multiplicative. (In fact, one can show that this property characterizes completely multiplicative functions: If h is any non-zero function for which the identity in (iv) holds for all functions f and g, then h is necessarily completely multiplicative.)

Proof. (i) Let f and g be multiplicative and let $h = f * g$. Given n_1 and n_2 with $(n_1, n_2) = 1$, we need to show that $h(n_1n_2) = h(n_1)h(n_2)$. To this end we use the fact (see the proof of Theorem 1.7) that each divisor $d|n_1n_2$ can be factored uniquely as $d = d_1d_2$ with $d_1|n_1$ and $d_2|n_2$, and that, conversely, given any pair (d1, d2) with d1|n1 and d2|n2, the product $d = d_1d_2$ satisfies $d| n_1n_2$. Hence

$$h(n_1n_2) = \sum_{d|n_1n_2} f(d)g(n_1n_2/d) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1d_2)g((n_1n_2)/(d_1d_2)).$$

Since (n1, n2) = 1, any divisors $d_1|n_1$ and $d_2|n_2$ satisfy $(d_1, d_2) = 1$ and $(n_1/d_1, n_2/d_2) = 1$. Hence, in the above double sum we can apply the multiplicativity of f and g to obtain

$$\begin{aligned} h(n_1n_2) &= \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)g(n/d_1)f(d_2)g(n_2/d_2) \\ &= (f * g)(n_1)(f * g)(n_2) = h(n_1)h(n_2), \end{aligned}$$

which is what we had to prove.

(ii) Let f be a multiplicative function and let g be the Dirichlet inverse of f. We prove the multiplicativity property

(A) g(n1n2) = g(n1)g(n2) if (n1, n2) = 1

by induction on the product $n = n_1n_2$. If $n_1n_2 = 1$, then $n_1 = n_2 = 1$, and (A) holds trivially. Let $n \geq 2$ be given, and suppose (A) holds whenever $n_1n_2 < n$. Let n_1 and n_2 be given with $n_1n_2 = n$ and $(n_1, n_2) = 1$. Applying the identity (A_n) above, we obtain, on using the multiplicativity of f and that of g for arguments < n,

$$0 = \sum_{d|n_1n_2} f(d)g(n_1n_2/d)$$

$$= \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)f(d_2)g(n_1/d_1)g(n_2/d_2) + (g(n_1n_2) - g(n_1)g(n_2))$$

$= (f * g)(n_1)(f * g)(n_2) + (g(n_1n_2) - g(n_1)g(n_2))$

$= e(n_1)e(n_2) + (g(n_1n_2) - g(n_1)g(n_2)),$

$= g(n_1n_2) - g(n_1)g(n_2),$

since, by our assumption $n = n_1n_2 \geq 2$, at least one of n1 and n2 must be ≥ 2, and so $e(n_1)e(n_2) = 0$. Hence we have $g(n_1n_2) = g(n_1)g(n_2)$. Thus, (A) holds for pairs (n_1, n_2) of relatively prime integers with $n_1n_2 = n$, and the induction argument is complete.

(iii) The identity $f * g = h$ implies $g = f^{-1} * h$, where f^{-1} is the Dirichlet inverse of f. Since f and h are multiplicative functions, so is f^{-1} (by (ii)) and $f^{-1} * h$ (by (i)). Hence g is multiplicative as well.

(iv) If h is completely multiplicative, then for any divisor d|n we have h(n) = h(d)h(n/d). Hence, for all n

$$h(f * g)(n) = h(n) \sum_{d|n} f(d)g(n/d) = \sum_{d|n} h(d)f(d)h(n/d)g(n/d)$$

= ((hf) ∗ (hg))(n), proving (iv).

Check YOUR PROGRESS 1

1. Define Dirichlet product

2. State any two properties of Dirichlet product and prove them

Application I: Proving identities for multiplicative arithmetic functions.

The above results can be used to provide simple proofs of identities for arithmetic functions, using the multiplicatively of the functions involved. To prove an identity of the form f ∗ g = h in the case when f, g, and h are known to be multiplicative functions, one simply shows, by direct calculation, that (∗) (f ∗ g)(p^m) = h(p^m) holds for every prime power p^m. Since, by the above theorem, the multiplicativity of f and g implies that of f ∗ g, and since multiplicative functions are uniquely determined by their values at prime powers, (∗) implies that the identity

(f ∗ g)(n) = h(n)

holds for all n ∈ N.

Examples

(1) **Alternate proof of the identity** $\sum_{d|n} \mu(d)$ = e(n)**.** The identityvcan be written as μ ∗ 1 = e, and since all three functions involved are multiplicative, it suffices to verify that the identity holds on prime powers. Since e(pm) = 0 and (μ ∗ 1)(pm) = $\sum_{k=0}^{m} \mu(p^k)$ = 1 − 1 + 0 −0 · · · = 0, this is indeed the case.

(2) **Proof of** $\sum_{d|n} \mu^2(d)/\phi(d) = n/\phi(d)$ **.** This identity is of the form f ∗ 1 = g with f = μ^2/ϕ and g = id /ϕ.The functions f and g are both quotients of multiplicative functions and therefore are multiplicative.

Hence all three functions in the identity $f * 1 = g$ are multiplicative, and it suffices to verify the identity at prime powers.We have

$$g(p^m) = p^m /\varphi(p^m) = p^m /(p^m - p^{m-1}) = (1 - 1/p)^{-1},$$

and

$$(f * 1)(p^m) = \sum_{d|n} (\mu^2(p^k)/\phi(p^k)) = 1+1/(p-1) = (1 - 1/p)^{-1},$$

and

so $g(p^m) = (f * 1)(p^m)$ for every prime power p^m. Thus the identity holds at prime powers, and therefore it holds in general.

(3) **The Dirichlet inverse of λ.** Since $\mu * 1 = e$, the function 1 is the Dirichlet inverse of the Moebius function. To find the Dirichlet inverse of λ, i.e., the unique function f such that $\lambda * f = e$, note first that since λ and e are both multiplicative, f must be multiplicative as well, and it therefore suffices to evaluate f at prime powers. Now, for any prime power p^m,

$$0 = e(p^m) = \sum_{k=0}^{m} f(p^k)\lambda(p^{m-k}) = \sum_{k=0}^{m} f(p^k)(-1)^{m-k},$$

so $f(pm) = -\sum_{k=0}^{m} f(p^k) (-1)^k$. This implies f(p) = 1, and by induction $f(p^m) = 0$ for $m \geq 2$. Hence f is the characteristic function of the squarefree numbers, i.e., $\lambda^{-1} = \mu^2$.

Application II: Evaluating Dirichlet products of multiplicative functions.

Since the Dirichlet product of multiplicative functions is multiplicative, and since a multiplicative function is determined by its values on prime powers, to evaluate a product $f * g$ with both f and g multiplicative, it suffices to compute the values of $f * g$ at prime powers. By comparing these values to those of familiar arithmetic functions, one can often identify $f * g$ in terms of familiar arithmetic functions.

Examples

(1) **The function** $\lambda * 1$**.** We have $(\lambda * 1)(p^m) = \sum_{k=0}^{m} \lambda(p^k) = \sum_{k=0}^{m} f(-1)^k$, which equals 1 if m is even, and 0 otherwise. However, the latter values are exactly the values at prime powers of the characteristic function of the squares, which is easily seen to be multiplicative. Hence $\lambda * 1$ is equal to the characteristic function of the squares.

(2) **The function** $f_k(n) = \sum_{d \mid n,(d,k)=1} \mu(d)$. Here k is a fixed positive integer, and the summation runs over those divisors of n that are relatively prime to k. We have $f_k = g_k * 1$, where $g_k(n) = \mu(n)$ if (n, k) = 1 and $g_k(n) = 0$ otherwise. It is easily seen that g_k is multiplicative, so f_k is also multiplicative. On prime powers p^m, $g_k(p^m) = -1$ if m = 1 and p ł k and $g_k(p^m) = 0$ otherwise, so $f_k(p^m) = \sum_{i=0}^{m} g(p^k) = 1 - 1 = 0$ if p łv k, and $f_k(p^m) = 1$ otherwise. By the multiplicativity of f_k it follows that f_k is the characteristic function of the set $A_k = \{n \in N : p|n \Rightarrow p|k\}$.

Application III: Proving the multiplicativity of functions, using known identities. This is, in a sense, the previous application in reverse. Suppose we kow that $f * g = h$ and that f and h are multiplicative. Then, by Theorem 1.10, g must be multiplicative as well.

Examples

(1) **Multiplicativity of** φ**.** Since $\varphi * 1 = id$ (see Theorem 1.5) and the functions 1 and id are (obviously) multiplicative, the function φ must be multiplicative as well. This is the promised proof of the multiplicativity of the Euler function (part (ii) of Theorem 1.5).

(2) **Multiplicativity of** d(n) **and** $\sigma(n)$**.** Since $d = 1 * 1$, and the function 1 is multiplicative, the function d is multiplicative as well. Similarly, since $\sigma = id * 1$, and 1 and id are multiplicative, σ is multiplicative.

Check your progress 2

3. What do you understand by **Dirichlet inverse of** λ

4. What is λ*1?

11.4 FORMAL POWER SERIES

In calculus an infinite series of the form

$$\sum_{n=0}^{\infty} a(n)x^n = a(0) + a(1)x + a(2)x^2 + \cdots + a(n)x^n + \cdots$$

Is called power series in x. Both x and coefficient a(n) are called real or complex numbers. To each power series there corresponds a radius of convergence r ≥ 0 such that series converges absolutely if |x| < r and diverges if |x| > r. (The radius can be + ∞)

Consider the following sequence

$$(a(0), a(1), \ldots, a(n), \ldots).$$

a(0) – constant coefficient of the series

If A(x) and B(x) are two formal series then

$$A(x) = \sum_{n=0}^{\infty} a(n)x^n \qquad \text{and } B(x) = \sum_{n=0}^{\infty} b(n)x^n,$$

We define

Equality: $A(x) = B(x)$ means that $a(n) = b(n)$ for all $n \geq 0$.
Sum: $A(x) + B(x) = \sum_{n=0}^{\infty} (a(n) + b(n))x^n$.
Product: $A(x)B(x) = \sum_{n=0}^{\infty} c(n)x^n$, where

where

$$c(n) = \sum_{k=0}^{n} a(k)b(n-k).$$

{c(n)} is called as Caunchy product of sequence {a(n)} and {b(n)}

In modern algebra, formal power series form a ring. The ring has zero element for addition which we denote by 0

$$0 = \sum_{n=0}^{\infty} a(n)x^n, \quad \text{where } a(n) = 0 \text{ for all } n \geq 0,$$

An identity element for multiplication which we denote by 1

$$1 = \sum_{n=0}^{\infty} a(n)x^n, \quad \text{where } a(0) = 1 \text{ and } a(n) = 0 \text{ for } n \geq 1.$$

A formal power series is called formal polynomial if all its coefficients are 0 from some point on.

For each formal power series

$$A(x) = \sum_{n=0}^{\infty} a(n)x^n$$ -With constant coeffiecient a(0) $\neq 1$

$$B(x) = \sum_{n=0}^{\infty} b(n)x^n,$$ - uniquely determined formal series such that A(x)B(x) = 1.Its coeffiecient can be determined by solving infinite system of equation

$$\begin{aligned} a(0)b(0) &= 1 \\ a(0)b(1) + a(1)b(0) &= 0, \\ a(0)b(2) + a(1)b(1) + a(2)b(0) &= 0, \\ &\vdots \end{aligned}$$

in succession for b(0), b(1),b(2), …The series B(x) is called the inverse of A(x) and is denoted by $A(x)^{-1}$ or by 1/A(x)

11.5 Bell series

If f is a multiplicative function of r variables, then its (formal) Bell series to the base p
(p prime) is defined by

$$f_{(p)}(x_1, \ldots, x_r) = \sum_{e_1, \ldots, e_r = 0}^{\infty} f(p^{e_1}, \ldots, p^{e_r}) x_1^{e_1} \cdots x_r^{e_r},$$

where the constant term is 1. The main property is the following: for every f, g ∈ Mr

$$(f * g)_{(p)}(x_1, \ldots, x_r) = f_{(p)}(x_1, \ldots, x_r) g_{(p)}(x_1, \ldots, x_r).$$

The connection of Bell series to Dirichlet series and Euler products is given by

$$D(f; z_1, \ldots, z_r) = \prod_p f_{(p)}(p^{-z_1}, \ldots, p^{-z_r}),$$

valid for every f ∈ M_r. For example, the Bell series of the gcd function $f(n_1, \ldots, n_r) = \gcd(n_1, \ldots, n_r)$ is

$$f_{(p)}(x_1, \ldots, x_r) = \frac{1 - x_1 \cdots x_r}{(1 - x_1) \cdots (1 - x_r)(1 - p x_1 \cdots x_r)}.$$

The Bell series of other multiplicative functions, in particular of c(m, n), s(m, n), $\sigma(n_1, \ldots, n_r)$ and $c_n(k)$ can be given from their Dirichlet series representations and using the relation . Note that in the one variable case the Bell series to a fixed prime of the unitary convolution of two multiplicative functions is the sum of the Bell series of the functions, that is

$$(f \times g)_{(p)}(x_1) = f_{(p)}(x_1) + g_{(p)}(x_1),$$

This is not valid in the case of r variables with r > 1.

Check Your Progress 3

5. Explain the formal Power series.

6. What is Bell Series ?

11.6 SUMMARY

An arithmetic function is any real- or complex-valued function defined on the set N of positive integers. Arithmetic functions are different from typical functions in that they cannot usually be described by simple formulas, so they are often evaluated in terms of
their average or asymptotic behavior.

11.7 KEYWORDS

1. **Neutral Element:** In **mathematics**, an **identity element**, or **neutral element**, is a special type of **element** of a set with respect to a binary operation on that set, which leaves any **element** of the set unchanged when combined with it.
2. **Weighted** Average. A method of computing a kind of arithmetic **mean** of a set of numbers in which some elements of the set carry more importance (**weight**) than others
3. Unique Function: A special relationship where each input has a single output.
4. Constant Function : In **mathematics**, a **constant function** is a **function** whose (output) value is the same for every input value.

11.8 QUESTIONS FOR REVIEW

1. Let f be a multiplicative function. We know that the Dirichlet inverse f^{-1} is then also multiplicative. Show that f^{-1} is completely multiplicative if and only if $f(p^m) = 0$ for all prime powers pm with $m \geq 2$ (i.e., if and only if f is supported by the squarefree numbers).
2. Given an arithmetic function f, a "Dirichlet square root" of f is an arithmetic function g such that $g * g = f$. Prove by elementary techniques that the constant function 1 has two Dirichlet square roots, of the form ±g, where g is a multiplicative function, and find the values of g at prime powers.
3. Let f be a multiplicative function satisfying $\lim pm \to \infty f(pm) = 0$. Show that $\lim n \to \infty f(n) = 0$.
4. 1.12 An arithmetic function f is called periodic if there exists a positiveinteger k such that $f(n + k) = f(n)$ for every $n \in N$; the integer k is called a period for f. Show that if f is completely multiplicative and periodic with period k, then the values of f are either 0 or roots of unity. (An root of unity is a complex number z such that $z^n = 1$ for some $n \in N$.)

11.9 SUGGESTED READINGS

- David M. Burton, Elementary Number Theory, University of New Hampshire.
- G.H. Hardy, and , E.M. Wrigh,. An Introduction to the Theory of Numbers (6th ed, Oxford University Press, (2008).
- W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.
- A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.
- I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.
- T.M. Apostol, Introduction to Analytic number theory, UTM, Springer, (1976).
- J. W. S Cassel, A. Frolich, Algebraic number theory, Cambridge.
- M Ram Murty, Problems in analytic number theory, springer.

• M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer.

11.10 ANSWERS TO CHECK YOUR PROGRESS

1.[HINT: Provide the definition, representation and example 11.2 Definition]

2.[HINT: Provide the statement and proof 11.2.1]

3.[Provide explanation with representation-- Application I example 3]

4.[Provide the explanation of the function --Application II example 1]

5.[HINT: Provide the definition and explanation 11.3]

6.[HINT: Provide the definition and explanation 11.4]

UNIT 12: EULER PHI FUNCTION

STRUCTURE

12.0 OBJECTIVE

In this unit we will study properties of euler phi function and The Sum of Divisor Function.

12.1 INTRODUCTION

This UNIT is the part ofthe theory arising out ofthe result known as Euler's Generalization ofFermat's Theorem. In a nutshell, Euler extended Fermat's theorem, which concerns congruences with prime moduli, to arbitrary moduli.

Leonhard Euler's totient function, $\phi(n)$, is an important object in number theory, counting the number of positive integers less than or equal to nn which are relatively prime ton.

12.2 EULER PHI FUNCTION

Euler's totient function (also called the Phi function) counts the number of positive integers less than n that are coprime ton. That is $\phi(n)$ is the number of $m \in N$ such that $\gcd(m,n)=1$.

The totient function appears in many applications of elementary number theory, including Euler's theorem, primitive roots of unity, cyclotomic polynomials, and constructible numbers in geometry.

12.2.1. Definition

For n ≥ 1, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

As an illustration of the definition, we find that ϕ (30) = 8; for, among the positive integers that do not exceed 30, there are eight that are relatively prime to 30; specifically,

1, 7, 11, 13, 17,19,23,29

The function ϕ > is usually called the Euler phi-function (sometimes, the indicator or totient) after its originator; the functional notation ϕ (n), however, is credited to Gauss. If n is a prime number, then every integer less than n is relatively prime to it; whence, ϕ (n) = n – 1. On the other hand, if n > 1 is composite, then n has adivisor d such that 1 < d < n. It follows that there are at least two integers among 1, 2, 3, ... , n that are not relatively prime to n, namely, d and n itself. As a result, $\emptyset$ (n) $\leq n - 2$. This proves that for n > 1,

$\emptyset$ (n) = $n - 1$ if and only if n is prime

12.2.2 Theorem

If p is prime, then ϕ (p) = p − 1. Conversely, if p is an integer such that φ(p) = p − 1, then p is prime.

Proof. The first part is obvious since every positive integer less than p is relatively prime to p. Conversely, suppose that p is not prime. Then p = 1 or p is a composite number. If p = 1, then ϕ (p) ≠ p − 1. Now if p is composite, then p has a positive divisor. Thus φ(p) 6= p − 1. We have a contradiction and thus p is prime.

Lemma. Given integers a, b, c, gcd(a, bc)= 1 if and only if gcd(a, b)= 1 and gcd(a, c) = 1.

Proof. First suppose that gcd(a, bc) = 1, and put d = gcd(a, b). Then d |a and d |b, whence d |a and d |bc. This implies that gcd(a, bc) ≥ d, which forces d = 1. Similar reasoning gives rise to the statement gcd(a, c) = 1.
For the other direction, take gcd(a, b)= 1 = gcd(a, c) and assume that gcd(a, bc)= $d_1 > 1$. Then d_1 must have a prime divisor p. Because $d_1 \mid bc$, it follows that p | bc; in consequence, p | b or p | c. If p |b, then (by virtue of the fact that p | a) we have gcd(a, b) ≥ p, a contradiction. In the same way, the condition p |c leads to the equally false conclusion that gcd(a, c) ≥ p. Thus, $d_1 = 1$ and the lemma is proven.

12.2.3 Theorem

Let **p** be a prime and **m** a positive integer, then $\varphi(p^m) = p^m - p^{m-1}$.

Proof. Note that all integers that are relatively prime to p^m and that are less than p^m are those that are not multiple of p. Those integers are p,2p,3p, ..., p^{m-1} p.

There are p^{m-1} of those integers that are not relatively prime to p^m and that are less than $p^{m.}$ Thus

$$\phi(pm) = p^m - p^{m-1}.$$

Example. $\phi(7^3) = 7^3 - 7^2 = 343 - 49 = 294.$

Also $\phi(2^{10}) = 2^{10} - 2^9 = 512.$

12.2.4 Theorem

Let m and n be two relatively prime positive integers. Then

$$\phi(mn) = \phi(m)\,\phi(n).$$

Proof. Denote φ(m) by s and let $k_1, k_2, ..., k_s$ be a reduced residue system modulo m. Similarly, denote $\phi(n)$ by t and let $k'_1, k'_2, ..., k'_t$ be a reduced residue system modulo n. Notice that if x belongs to a reduced residue system modulo mn, then

(x, m) = (x, n) = 1.

Thus

$x \equiv k_i \pmod m$ and $x \equiv k'_j \pmod n$

for some i, j. Conversely, if

$x \equiv k_i \pmod m$ and $x \equiv k'_j \pmod n$

some i, j then (x, mn) = 1 and thus x belongs to a reduced residue system modulo mn. Thus a reduced residue system modulo mn can be obtained by by determining all x that are congruent to k_i and k'_j modulo m and n respectively. By the Chinese remainder theorem, the system of equations

$x \equiv k_i \pmod m$ and $x \equiv k'_j \pmod n$

has a unique solution. Thus different i and j will yield different answers. Thus

$\phi(mn) = st.$

12.2..5 Theorem

Let $n = p_1^{a_1}, p_2^{a_2} \ldots p_s^{a_s}$ be the prime factorization of n. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right).$$

Proof. By Theorem 12.1.3, we can see that for all $1 \leq i \leq k$

$$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right).$$

Thus by Theorem 12.1.4,

$$\begin{aligned}\phi(n) &= \phi(p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s})\\ &= \phi(p_1^{a_1})\phi(p_2^{a_2})\ldots\phi(p_s^{a_s})\\ &= p_1^{a_1}\left(1-\frac{1}{p_1}\right)p_2^{a_2}\left(1-\frac{1}{p_2}\right)\ldots p_s^{a_s}\left(1-\frac{1}{p_s}\right)\\ &= p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_s}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_s}\right).\end{aligned}$$

Example Note that

$\varphi(200) = \varphi(2^3 5^2) = 200\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 80.$

12.2.6.Theorem

Let n be a positive integer greater than 2. Then φ(n) is even.

Proof. Let $n = p_1^{a_1}, p_2^{a_2}\ldots p_k^{a_k}$ Since ϕ is multiplicative, then

Thus by Theorem 39, we have

$$\phi(p_j^{a_j}) = p_j^{a_j-1-1}(p_j - 1).$$

We see then $\phi(p_j^{a_j})$ is even if p_j is an odd prime. Notice also that if p_j = 2, then it follows that $\phi(p_j^{a_j})$ is even. Hence ϕ (n) is even.

12.2.7. Theorem

Let n be a positive integer. Then

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

Proof. Split the integers from 1 to n into classes. Put an integer m in the class C_d if the greatest common divisor of m and n is d. Thus the number of integers in the C_d class is the number of positive integers not

exceeding n/d that are relatively prime to n/d. Thus we have Φ (n/d) integers in $C_{d.}$ Thus we see that

$$n = \sum_{d|n} \phi(n/d).$$

As d runs over all divisors of n, so does n/d. Hence

$$n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d).$$

12.3 THE SUM-OF-DIVISORS FUNCTION

The sum of divisors function, denoted by σ(n), is the sum of all positive divisors of n.

Example. σ(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.

Note that we can express σ(n) as σ(n) = Pd|n d.

12.3.1 .Theorem

The sum of divisors function σ(n) is multiplicative.

Proof. Let f(n) = n and notice that f(n) is multiplicative. As a result, σ(n) is multiplicative.

Once we found out that σ(n) is multiplicative, it remains to evaluate σ(n) at powers of primes and hence we can derive a formula for its values at any positive integer.

12.3.2.Theorem

Let p be a prime and let n = $p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ t be a positive integer. Then $\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1},$

and as a result,

$$\sigma(n) = \prod_{j=1}^{t} \frac{p_j^{a_j+1} - 1}{p_j - 1}$$

Proof. Notice that the divisors of pa are 1, p, ^{p2}, ..., p^a. Thus

$$\sigma(p^a) = 1 + p + p^2 + \ldots + p^a = \frac{p^{a+1}-1}{p-1}$$

where the above sum is the sum of the terms of a geometric progression.

Now since σ(n) is multiplicative, we have

$$\begin{aligned}\sigma(n) &= \sigma(p^{a_1})\sigma(p^{a_2})\ldots\sigma(p^{a_t}) \\ &= \frac{p_1^{a_1+1}-1}{p_1-1}.\frac{p_2^{a_2+1}-1}{p_2-1}\ldots\frac{p_t^{a_t+1}-1}{p_t-1} \\ &= \prod_{j=1}^{t}\frac{p_j^{a_j+1}-1}{p_j-1}\end{aligned}$$

Example: $\sigma(200) = \sigma(2^3 5^2) = \frac{2^3-1}{2-1}\frac{5^2-1}{5-1} = 15.31 = 465.$

The Number-of-Divisors Function

The number of divisors function, denoted by τ(n), is the sum of all positive divisors of n.

Example. τ(8) = 4.

We can also express τ(n) as τ(n) = Pd|n 1.

We can also prove that τ(n) is a multiplicative function.

12.3.3.Theorem

The number of divisors function τ(n) is multiplicative.

Proof. As we know that with f(n) = 1, τ(n) is multiplicative.

We also find a formula that evaluates τ(n) for any integer n.

12.3.4.Theorem

Let p be a prime and let n = $p_1^{a1}, p_2^{a2} \cdots p_t^{at}$ t be a positive integer. Then

$$\tau(p^a) = a + 1,$$

and as a result,

$$\tau(n) = \prod_{j=1}^{t}(a_j + 1).$$

Proof. The divisors of pa as mentioned before are 1, p, p^2, ..., p^a. Thus

$$\tau(p^a) = a + 1$$

Now since τ(n) is multiplicative, we have

$$\tau(n) = \tau(p^{a_1})\tau(p^{a_2})\ldots\tau(p^{a_t}))$$

$$= (a_1 + 1)(a_2 + 1)\ldots(a_t + 1)$$

$$= \prod_{j=1}^{t}(a_j + 1).$$

Example: $\tau(200) = \tau(2^3 5^2) = (3 + 1)(2 + 1) = 12$.

Check Your Progress

1.Explain the sum of divisor and number of divisor concept

2. What is Euler's Phi Function?

12.4 SOME PROPERTIES OF THE PHI-FUNCTION

12.4.1 Theorem

Gauss. For each positive integer $n \geq 1$

$$n = \sum_{d \mid n} \phi(d)$$

the sum being extended over all positive divisors of n.

Proof. The integers between 1 and n can be separated into classes as follows: If d is a positive divisor of n, we put the integer m in the class sd provided that gcd(m, n) =d.

Stated in symbols,

Sd = {m | gcd(m, n) = d; $1 \leq m \leq n$}

Now gcd(m , n) = d if and only if gcd(m | d , n | d) = 1. Thus, the number of integers in the class S_d is equal to the number of positive integers not exceeding n|d that are relatively prime to n|d; in other words, equal to ϕ (n |d). Because each of then integers in the set {1, 2, ... , n} lies in exactly one class S_d, we obtain the formula

$$n = \sum_{d \mid n} \phi\left(\frac{n}{d}\right)$$

But as d runs through all positive divisors of n, so does n|d; hence,

$$\sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$$

which proves the theorem.

Example. A simple numerical example of what we have just said is provided by n = 10. Here, the classes Sd are

S_1={1,3,7,9}

S_2 = {2, 4, 6, 8}

S_5 = {5}

S_{10} = {10}

These contain ϕ (10) = 4, ϕ (5) = 4, ϕ (2) = 1, and ϕ (1) = 1 integers,

respectively.

Therefore,

$$\sum_{d \mid 10} \phi(d) = \phi(10) + \phi(5) + \phi(2) + \phi(1)$$
$$= 4 + 4 + 1 + 1 = 10$$

12.4.2. Theorem

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

Proof. Let a $_1$, a_2 , ... ,$a_{\phi(n)}$) be the positive integers less than nand relatively prime to n. Now because gcd(a, n) = 1 if and only if gcd(n – a, n) = 1, the numbers n – a_1,n – a_2, ... ,n – $a_{\phi(n)}$ are equal in some order to a_1, a_2, ... , $a_{\phi(n)}$Thus,

$a_1 + a_2 + \cdots + a_{\phi(n)} = (n - a_1) + (n - a_2) + \cdots +$,n – $a_{\phi(n)}$

$= \phi(n)$ n - (at + az + ·· · + $a_{\phi(n)}$)

Hence,

2(a, + az + · ·· + $a_{\phi(n)}$) = $\phi(n)$ n

leading to the stated conclusion.

Example. Consider the case where n = 30. The ϕ (30) = 8 integers that are less than 30 and relatively prime to it are

1,7, 11, 13, 17,19,23,29

In this setting, we find that the desired sum is

1 + 7 + 11 + 13 + 17 + 19 + 23 + 29 = 120 =$\frac{1}{2}$. 30. 8

Also note the pairings

1+ 29 = 30 7+23=30 11 + 19 = 30 13 + 17 = 30

12.4.3 Theorem

For any positive integer n,

$$\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}$$

Proof: The proof is deceptively simple. If we apply the inversion formula to

$$F(n) = n = \sum_{d \mid n} \phi(d)$$

the result is

$$\begin{aligned} \phi(n) &= \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) \\ &= \sum_{d \mid n} \mu(d) \frac{n}{d} \end{aligned}$$

Let us again illustrate the situation where n = 10. As easily can be seen,

$$\begin{aligned} 10 \sum_{d \mid 10} \frac{\mu(d)}{d} &= 10\left[\mu(1) + \frac{\mu(2)}{2} + \frac{\mu(5)}{5} + \frac{\mu(10)}{10}\right] \\ &= 10\left[1 + \frac{(-1)}{2} + \frac{(-1)}{5} + \frac{(-1)^2}{10}\right] \\ &= 10\left[1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{10}\right] = 10 \cdot \frac{2}{5} = 4 = \phi(10) \end{aligned}$$

It is easy to determine the value ofthe phi function for any positive integer n using above Theorem. Suppose that the prime-power decomposition of n is $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, and consider the product

$$P = \prod_{p_i \mid n} \left(\mu(1) + \frac{\mu(p_i)}{p_i} + \cdots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}}\right)$$

Multiplying this out, we obtain a sum of terms of the form

$$\frac{\mu(1)\mu(p_1^{a_1})\mu(p_2^{a_2}) \cdots \mu(p_r^{a_r})}{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}} \qquad 0 \le a_i \le k_i$$

or, because μ is known to be multiplicative,

$$\frac{\mu(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})}{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}} = \frac{\mu(d)}{d}$$

where the summation is over the set of divisors d = $p_1^{a_1}, p_2^{a_2} \cdots p_r^{a_r}$ of n. Hence, P = $\sum_{d|n} \mu(d)/d$. It follows from Theorem 11.3.3 that

$$\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d} = n \prod_{p_i \mid n} \left(\mu(1) + \frac{\mu(p_i)}{p_i} + \cdots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}} \right)$$

But $\mu(p_i^{a_i})$ = 0 whenever $a_i \geq 2$. As a result, the last-written equation reduces to

$$\phi(n) = n \prod_{p_i \mid n} \left(\mu(1) + \frac{\mu(p_i)}{p_i} \right) = n \prod_{p_i \mid n} \left(1 - \frac{1}{p_i} \right)$$

12.5 SUMMARY

Euler's Phi Function has been applied to subjects as diverse as constructible polygons and Internet cryptography

12.6 KEYWORDS

1. Multiple - a multiple is the product of any quantity and an integer.
2. Consequence definition is - a conclusion derived through logic : inference
3. yield - "results in'
4. Summation - In **mathematics**, **summation** is the addition of a sequence of any kind of numbers, called addends or summands; the result is their **sum** or total.

12.7 QUESTIONS FOR REVIEW

1. Calculate ϕ (1001), ϕ 5040), and ϕ (36,000).

2. Verify that the equality $\phi(n)= \phi(n+1)= \phi(n+2)$ holds when n = 5186.

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

4. Prove that if the integer n has r distinct odd prime factors, then $2^r \mid \phi(n)$

5. Show that if n is an odd integer, then φ(4n) = 2φ(n).

12.8 SUGGESTED READINGS

1. David M. Burton, Elementary Number Theory, University of New Hampshire.

2. G.H. Hardy, and , E.M. Wrigh,. An Introduction to the Theory of Numbers (6th ed, Oxford University Press, (2008).

3. W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.

4. A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.

5. I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.

6. T.M. Apostol, Introduction to Analytic number theory, UTM, Springer, (1976).

7. J. W. S Cassel, A. Frolich, Algebraic number theory, Cambridge.

8.M Ram Murty, Problems in analytic number theory, springer.

M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer

12.9 ANSWERS TO CHECK YOUR PROGRESS

1. [HINT:Provide the explanation and representation 12.2]
2. [HINT:Provide definition with representation12.1.1]

UNIT 13: CONTINUED FRACTIONS

STRUCTURE

13.0 OBJECTIVE

In this unit we will study properties of Continued Fraction and Simple Continued Fraction.

13.1 INTRODUCTION

In mathematics, a **continued fraction** is an expression obtained through an iterative process of representing a number as the sum of its integer part and the reciprocal of another number, then writing this other number as the sum of its integer part and another reciprocal, and so on.

13.2 CONTINUED FRACTION

In this and the following section, we will describe a technique for writing any real number as an iterated sequence of quotients. For example, the rational number 157/30 can be expanded as follows

$$\frac{157}{30} = 5 + \frac{7}{30} = 5 + \frac{1}{\frac{30}{7}} = 5 + \frac{1}{4 + \frac{2}{7}} = 5 + \frac{1}{4 + \frac{1}{\frac{7}{2}}} = 5 + \frac{1}{4 + \frac{1}{3 + \frac{1}{2}}}$$

and the last expression is called a finite continued fraction. To expand an irrational number, we need infinite continued fractions; for example

$$\sqrt{2}+1 = 2+(\sqrt{2}-1) = 2+\frac{1}{\sqrt{2}+1} = 2+\cfrac{1}{2+\cfrac{1}{\sqrt{2}+1}}$$

$$= 2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\sqrt{2}+1}}} = 2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\ddots}}}}$$

13.2.1 Definition

Let $a_0, a_1, \ldots, a_n$ be real numbers, all positive except possibly a_0. The expression

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots+\cfrac{1}{a_{n-1}+\cfrac{1}{a_n}}}}}$$

is called a finite continued fraction and is denoted by $\langle a_0, a_1, \ldots, a_n \rangle$ The numbers a_k are called the terms or the partial quotients of the continued fraction.

If the reader does not like the dots in the above definition, the following recursive definition should satisfy her completely:

$$\langle a_0 \rangle = a_0$$

$$\langle a_0, a_1 \rangle = a_0 + 1/a_1$$

$$\langle a_0, a_1, \ldots, a_n \rangle = \langle a_0, a_1, \ldots, a_{n-2}, a_{n-1} + \tfrac{1}{a_n} \rangle \text{ if } n \geq 2.$$

The reason for assuming $a_k > 0$ for $k \geq 1$ in the above definition is that this guarantees that no division by zero will occur. A continued fraction with n + 1 terms can be compressed by viewing it as composed of two shorter continued fractions as follows, which is very useful in induction proofs.

13.2.2 Proposition

Let 1 ≤ k ≤ n. Then

$$(i)\ \langle a_0, a_1, \ldots, a_n\rangle = \langle a_0, a_1, \ldots, a_{k-1}, \langle a_k, a_{k+1}, \ldots, a_n\rangle\rangle, \quad \text{and}$$
$$(ii)\ \langle a_0, a_1, \ldots, a_n\rangle = a_0 + \frac{1}{\langle a_1, \ldots, a_n\rangle}.$$

Proof. The formulas should be obvious from the very definition of continued fractions. For a formal proof of (i), use induction on the number m of terms in the innermost continued fraction $\langle a_k, a_{k+1}, \ldots, a_n\rangle$. If m = 1, that is k = n, then $\langle a_n\rangle$ = a_n, and there is nothing to prove. If m = 2, then $\langle a_{n-1}, a_n\rangle$ = $a_{n-1} + 1/a_n$, and the identity (i) coincides with the recursive definition of $a_0, a_1, \ldots, a_n$.

Now suppose inductively that the identity (i) holds whenever the innermost continued fraction has m terms, and consider the case when $\langle a_k, a_{k+1}, \ldots, a_n\rangle$. has m + 1 terms. By the induction hypothesis applied twice and the case m = 2 applied once, we obtain

$$\begin{aligned}\langle a_0, a_1, \ldots, a_n\rangle &= \langle a_0, a_1, \ldots, a_{k-1}, a_k, \langle a_{k+1}, \ldots, a_n\rangle\rangle \\ &= \langle a_0, a_1, \ldots, a_{k-1}, \langle a_k, \langle a_{k+1}, \ldots, a_n\rangle\rangle\rangle \\ &= \langle a_0, a_1, \ldots, a_{k-1}, \langle a_k, a_{k+1}, \ldots, a_n\rangle\rangle.\end{aligned}$$

This completes the induction argument.(ii) is a special case of (i), obtained by taking k = 1

13.2.3 Definition

Let $(a_n)_{n=0}^{\infty}$ be a sequence of real numbers, all positive exept possibly a0. The sequence $\langle a_0, a_1, \ldots, a_n\rangle_{n=0}^{\infty}$ n=0 is called an infinite continued fraction and is denoted by a0, a1, a2, ... The infinite continued fraction is said to converge if the limit

$$\lim_{n\to\infty} \langle a_0, a_1, \ldots, a_n\rangle$$

exits, and in that case the limit is also denoted by $\langle a_0, a_1, a_2, \ldots,\rangle$. In order to determine the convergence of a given infinite continued fraction

we need to consider the finite continued fractions $\langle a_0, a_1, \ldots, a_n \rangle$ for increasing values of n. Suppose now that we have computed the value of $\langle a_0, a_1, \ldots, a_n \rangle$ and want to compute the value of $\langle a_0, a_1, \ldots, a_n, a_{n+1} \rangle$ without having to repeat the whole computation from scratch. The recursion formula (ii) in Proposition 13.1.2 will then be of no use, since it defines $\langle a_0, a_1, \ldots, a_n, a_{n+1} \rangle$ in terms of a0 and $\langle a_0, a_1, \ldots, a_n, a_{n+1} \rangle$ and not in terms of $\langle a_0, a_1, \ldots, a_n \rangle$ and a_{n+1}. Fortunately, there is an easy way to compute the continued fractions $\langle a_0, a_1, \ldots, a_n \rangle$ in succession, and we will now describe this method.

13.2.4 Definition

Let $(a_n)_{n=0}^N$ be a finite ($N \in \mathbf{N}$) or infinite ($N = \infty$) sequence of real numbers, all positive except possibly a0, and define two sequences $(p_n)_{n=-2}^N$ and $(q_n)_{n=-2}^N$ ecursively as follows:

$p_{-2} = 0, \quad p_{-1} = 1, \quad p_n = a_n p_{n-1} + p_{n-2} \quad \text{if } n \geq 0,$

$q_{-2} = 1, \quad q_{-1} = 0, \quad q_n = a_n q_{n-1} + q_{n-2} \quad \text{if } n \geq 0.$

The pair (p_n, q_n), as well as the quotient p_n/q_n (where $n \geq 0$), is called the nth convergent of the given sequence $(a_n)_{n=0}^N$ or, equivalently, of the corresponding continued fraction. Obviously, $q_0 = 1$, and $q_n > 0$ for all $n \geq 0$. Thus, $(q_n)_{n=0}^N$ is a positive sequence.

The connection between continued fractions and convergents is given by the next theorem, which also contains some crucial identities.

13.2.5 Theorem

Let $(a_n)_{n=0}^N$ be a sequence of real numbers, all positive except possibly a_0, with corresponding convergents (p_n, q_n), and write $c_n = p_n/q_n$. Then

(i) $\langle a_0, a_1, \ldots, a_n \rangle = c_n$, for all $n \geq 0$;

(ii) $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$, if $n \geq -1$;

(iii) $c_n - c_{n-1} = (-1)^{n-1}/q_{n-1} q_n$, if $n \geq 1$;

(iv) $p_nq_{n-2} - p_{n-2}q_n = (-1)^n a_n$, if $n \geq 0$;

(v) $c_n - c_{n-2} = (-1)_n a_n / q_n q_{n-2}$, if $n \geq 2$.

Proof. (i): The case n = 0 is trivial, because $c_0 = p_0/q_0 = a_0/1 = a_0$. Suppose inductively that (i) holds for all continued fractions with n terms, and let $\langle a_0, a_1, \ldots, a_n \rangle$ be a continued fraction with n + 1 terms. Since

$$\langle a_0, a_1, \ldots, a_n \rangle = \langle a_0, a_1, \ldots, a_{n-2} + a_{n-1} + 1/a_n \rangle$$

and since the latter continued fraction has n terms and its (n− 1)st convergent equals $((a_{n-1} + 1/a_n)p_{n-2} + p_{n-3})$, $(a_{n-1} + 1/a_n)q_{n-2} + q_{n-3})$, we conclude that

$$\langle a_0, a_1, \ldots, a_n \rangle = \frac{(a_{n-1} + 1/a_n)p_{n-2} + p_{n-3}}{(a_{n-1} + 1/a_n)q_{n-2} + q_{n-3}} = \frac{a_n(a_{n-1}p_{n-2} + p_{n-3}) + p_{n-2}}{a_n(a_{n-1}q_{n-2} + q_{n-3}) + q_{n-2}}$$
$$= \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.$$

This completes the induction step.

(ii) Write $z_n = p_nq_{n-1} - p_{n-1}q_n$. Using the recursive definitions, we obtain $z_n = p_nq_{n-1} - p_{n-1}q_n = (a_np_{n-1} + p_{n-2})q_{n-1} - p_{n-1}(a_nq_{n-1} + q_{n-2}) = p_n - 2q_{n-1} - p_{n-1}q_{n-2} = -z_{n-1}$, for $n \geq 0$, and it follows at once that $z_n = (-1)^{n-1} z_{-1}$. But $z_{-1} = 1$, since $p_{-1} = q_{-2} = 1$ and $p_{-2} = q_{-1} = 0$. Hence, $z_n = (-1)^{n-1}$, as required.

(iii) follows from (ii) upon division by $q_{n-1}q_n$, which is nonzero for $n \geq 1$.

(iv) Using the recursive definition of pn and qn and equality (ii), we obtain

$p_nq_{n-2} - p_{n-2}q_n = (a_np_{n-1} + p_{n-2})q_{n-2} - p_{n-2}(a_nq_{n-1} + q_{n-2})$

$= a_n(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = a_n(-1)^{n-2} = (-1)^n a_n$.

(v) follows from (iv) upon division by q_nq_{n-2}.

Example 1 We use Theorem 13.1.5 to evaluate the continued fraction $\langle -2, 5, 4, 3, 2, 1\rangle$

The computations are easily caried out by using the following table:

n	-2	-1	0	1	2	3	4	5
a_n			-2	5	4	3	2	1
p_n	0	1	-2	-9	-38	-123	-284	-407
q_n	1	0	1	5	21	68	157	225

The entries are computed according to the recursive formulas given in Definition 13.1.4. For example, to find $p_4 = a_4p_3 + p_2$, multiply $a_4 = 2$ by the last computed p-value p_3 (= −123) and add the preceding term p_2 (= −38) to obtain $p_4 = 2(-123) + (-38) = -284$. Finally, note that

$$\langle -2, 5, 4, 3, 2, 1\rangle = p_5/q_5 = -407/225.$$

The successive convergents are −2, −9/5, −38/21, −123/68, −284/157, and −407/225.

13.2.6 Corollary

Let $(a_n)_{n=0}^{N}$ =0 be a finite or infinite sequence of real numbers, all positive except possibly a0, with convergents $c_n = p_n/q_n$. The convergents c_{2i} with even indices form a strictly increasing sequence and the convergents c_{2j+1} with odd indices form a strictly decreasing sequence, and $c_{2i} < c_{2j}+1$, that is $c_0 < c_2 < \cdots < c_{2i} < \cdots < c_{2j+1} < \cdots < c_3 < c_1$.

Proof. We have $c_n - c_{n-2} = (-1)^n a_n/q_nq_{n-2}$, by Theorem 13.1.5 (v). Hence, if $n \geq 2$ is even, then $c_n - c_{n-2} > 0$ and if $n \geq 3$ is odd, then $c_n - c_{n-2} < 0$.

Finally, by Theorem 13.1.5 (iii), $c_{2k+1} - c_{2k} = 1/q_{2k}q_{2k+1} > 0$. Thus, if $i \geq j$, then $c_{2j} < c_{2i} < c_{2i+1}$ and $c_{2i} < c_{2i+1} < c_{2j+1}$.

Example: We computed the continued fraction $\langle -2, 5, 4, 3, 2, 1\rangle$ and its successive convergents. It is easily verified that

$$-2 < -\frac{38}{21} < -\frac{284}{157} < -\frac{407}{225} < -\frac{123}{68} < -\frac{9}{5}$$

in accordance with Corollary 13.1.6

Let $(a_n)_{n=0}^{\infty}$ be a sequence of real numbers, all positive except possibly a0, with convergents $c_n = p_n/q_n$. By Theorem 13.1.5, $c_n = \langle -2, 5, 4, 3, 2, 1 \rangle$. Corollary 13.1.6 implies that the sequence $(c_{2k})_{k=0}^{\infty}$ of convergents with even indices is strictly increasing and bounded above by c1. Hence, the limit c'= $\lim_{k\to\infty} c_{2k}$ exists. Similarly, the sequence $(c_{2k})_{k=0}^{\infty}$ is strictly decreasing and bounded below by c_0. Therefore, the limit c" = $\lim_{k\to\infty} c_{2k+1}$ exists, too, and obviously $c_{2k} < c_0 \leq c'' < c_{2k+1}$ for all k

The limit

$$c = \lim_{n\to\infty} c_n = \lim_{n\to\infty} \langle a_0, a_1, \ldots, a_n \rangle$$

exists if and only if c' = c", that is if and only if $c_{2k+1} - c_{2k} \to 0$ as $k \to \infty$. By Theorem 13.1.5, $0 < c_{2k+1} - c_{2k} < 1/q_{2k}q_{2k+1}$. Therefore, $\lim_{n\to\infty} q_n = \infty$ is a sufficient condition for the existence of the limit c, i.e. for the convergence of the infinite continued fraction $\langle a_0, a_1, a_2 \ldots \rangle$. Our next proposition gives a condition on the sequence $(a_n)_{n=0}^{\infty}$ which will guarantee that $q_n \to \infty$.

13.2.7 Proposition

Let $(a_n)_{n=0}^{\infty}$ be a sequence with convergents (p_n, q_n) and assume that there is a constant $\alpha > 0$ such that $a_n \geq \alpha$ for all $n \geq 1$. Then $q_n \to \infty$ as $n \to \infty$. More precisely, there is a constant $r > 1$ and a positive constant C such that $q_n \geq Cr^n$ for all $n \geq 0$. The sequence $(q_n)_{n=1}^{\infty}$ n=1 is strictly increasing if $a_n \geq 1$ for all $n \geq 1$.

Proof. By assumption, $q_n = a_n q_{n-1} + q_{n-2} \geq \alpha\, q_{n-1} + q_{n-2}$ for all $n \geq 1$. Let r denote the positive root of the quadratic equation $x^2 = \alpha x + 1$, that is $r = \alpha/2 + \sqrt{1 + \alpha^2/4}$ and let C denote the smallest of the two numbers 1 and a_1/r. Then $q_0 = 1 \geq Cr^0$ and $q_1 = a_1 \geq Cr^1$. We claim that $q_n \geq Cr^n$ for all n

≥ 0. This follows by induction, because if $q_k \geq Cr^k$ for $0 \leq k \leq n-1$, then $q_n \geq Cr^{n-1} + Cr^{n-2} = Cr^{n-2}(\alpha r + 1) = Cr^{n-2} \cdot r^2 = Cr^n$. Obviously, $r > 1$, so it follows that $qn \to \infty$ as $n \to \infty$. If $a_n \geq 1$ for all $n \geq 1$, then $qn = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} > q_{n-1}$ for all $n \geq 2$, which means that the sequence $(q_n)_{n=1}^{\infty}$ is strictly increasing.

13.2.8 Definition

A sequence $(a_n)_{n=0}^{\infty}$ of real numbers will be called admissible if there is a positive constant α such that $an \geq \alpha$ for all $n \geq 1$. A sequence $(a_n)_{n=0}^{\infty}$ consisting of integers, all positive except possibly a_0, is obviously admissible with $\alpha = 1$. In particular, for such sequences the corresponding sequence $(qn)\infty$ n=1 is strictly increasing and unbounded. The discussion preceding Proposition 13.1.7 may now be summarized as follows:

13.2.9 Theorem

Let $(a_n)_{n=0}^{\infty}$ be an admissible sequence with convergent $cn = p_n/q_n$. The infinite continued fraction $\xi = \langle a_0, a_1, a_2 \ldots, \rangle$ is then convergent, and it satisfies

(1) $$c_{2n} < \xi < c_{2n+1} \quad and$$

(2) $$\frac{a_{n+2}}{q_n q_{n+2}} < |\xi - c_n| < \frac{1}{q_n q_{n+1}}$$

for all $n \geq 0$.

Proof. It only remains to prove (2). By (1), for each $n \geq 0$, the number ξ belongs to the interval with endpoints c_n and c_{n+1}, and hence

$$|\xi - c_n| < |c_{n+1} - c_n| = \frac{1}{q_n q_{n+1}},$$

where the last equality follows from Theorem 13.1.5 (iii). Moreover, the number c_{n+2} lies strictly between the numbers c_n and ξ. Consequently,

$$|\xi - c_n| > |c_{n+2} - c_n| = \frac{a_{n+2}}{q_n q_{n+2}},$$

where the last equality is a consequence of Theorem 13.1.5 (v). This completes the proof of the theorem.

13.2.10 Theorem

Let $(a_n)_{n=0}^{\infty}$ be an admissible sequence of real numbers, let k be a positive integer, and write ξk = $\langle a_k, a_{k+1}, a_{k+2} \dots, \rangle$. Then

$$\langle a_0, a_1, a_2 \dots, \rangle = \langle a_0, a_1, a_2 \dots, a_{k-1}, \xi k \rangle,$$

Proof. Write ξ = $\langle a_0, a_1, a_2 \dots, \rangle$ = = $\lim_{n\to\infty} \langle a_0, a_1, \dots, a_n \rangle$.

By letting n → ∞ in the relation

$$\langle a_0, a_1, \dots, a_n \rangle = a_0 + \frac{1}{\langle a_0, a_1, \dots, a_n \rangle},$$

we obtain

ξ = $a_0 + 1/\xi_1 = \langle a_0, \xi 1 \rangle$.

(Note that ξ1 > a1 > 0.) This proves the case k = 1. In particular, we have $\xi_k = \langle a_k, \xi_{k+1} \rangle$for each k.

The general case now follows by induction. Assume that the theorem holds for a certain k ≥ 1; then

$$\xi = \langle a_0, a_1, a_2 \dots, a_{k-1}, \xi k \rangle, = \langle a_0, a_1, a_2 \dots, a_{k-1}, \langle a_k, \xi_{k+1} \rangle \rangle,$$

$$= \langle a_0, a_1, a_2 \dots, a_{k-1}, a_k, \xi_{k+1} \rangle,$$

where the last equality follows from Proposition 13.1.2. This completes the induction step.

Example Let us use Theorem 13.1.10 to compute the periodic infinite continued fraction ξ = $\langle 1, 2, 3, 1, 2, 3, \dots \rangle = \overline{\langle 1, 2, 3 \rangle}$where the bar over

1, 2, 3 indicates that this block of integers is repeated indefinitely. By periodicity, $\xi = \langle 1, 2, 3, \xi_3 \rangle$ with $\xi_3 = \xi$, that is $\xi = \langle 1, 2, 3, \xi \rangle$. To compute the value of this finite continued fraction we use convergents, which are computed in the following table

n	-2	-1	0	1	2	3
a_n			1	2	3	ξ
p_n	0	1	1	3	10	$10\xi + 3$
q_n	1	0	1	2	7	$7\xi + 2$

It follows that

$$\xi = \langle 1, 2, 3, \xi \rangle = \frac{p_3}{q_3} = \frac{10\xi + 3}{7\xi + 2}.$$

Solving for ξ we obtain the quadratic equation $7\xi^2 - 8\xi - 3 = 0$ with the roots $(4 \pm \sqrt{37})/7$. Since $\xi > 0$, we conclude that $\xi = (4 + \sqrt{37})/7$.

Example: To compute the infinite periodic continued fraction

$$\eta = \langle 0, 1, \overline{1, 2, 3,} \rangle$$

we start by writing $\eta = \langle 0, 1, \xi \rangle$, where $\xi = \langle \overline{1, 2, 3} \rangle$, and

$$\eta = 0 + 1/(1 + 1/\xi) = \xi/(\xi + 1).$$

The value of ξ was computed in the previous example. Inserting $\xi = (4 + \sqrt{37})/7$ into the expression for η, we obtain $\eta = (1 + \sqrt{37})/12$.

Example: $\xi = \langle 1, 1, 1, \ldots \rangle = \langle \overline{1} \rangle$ is the simplest possible infinite continued fraction. We will see later that this number plays a special role when it comes to approximation of irrational numbers by rational numbers.

Since $\xi = \langle 1, \xi \rangle$, ξ satisfies the equation $\xi = 1 + 1/\xi$, that is $\xi^2 = \xi + 1$. This quadratic equation

has the roots $(1\pm\sqrt{5})/2$, and since ξ is positive we conclude that $\langle 1, 1, 1, \dots \rangle = (1 + \sqrt{5})/)/2$.

Check Your Progress 1

1. Define Finite and Infinite Continued fraction.

2. Prove the statement: Let $(a_n)_{n=0}^{\infty}$ be an admissible sequence of real numbers, let k be a positive integer, and write ξk = $\langle a_k, a_{k+1}, a_{k+2} \dots, \rangle$.

13.3 SIMPLE CONTINUED FRACTIONS

13.3.1 Definition

A finite or infinite continued fraction is called simple, if all its terms are integers.

We recall that all terms of a continued fraction, except possibly the first term a_0, are by default supposed to be positive. In particular, all terms of a simple continued fraction, except possibly the first one, are positive integers.

This means that the terms of an infinite simple continued fraction form an admissible sequence (with α = 1), so there are no convergence problems: The infinite simple continued fractions are automatically convergent.

The value of a finite simple continued fraction is a rational number. Of course, this follows easily from the recursive definition of finite continued fractions, but we can also deduce it from the following theorem.

13.3.2 Theorem

Let (pn, qn) be the nth convergent of a finite or infinite simple continued fraction. The numbers pn and qn are then relatively prime integers for each n. Thus, the fractions cn = pn/qn, n ≥ 0, are rational numbers in reduced form.

Proof. It follows at once from their defining recursive relations that p_n and q_n are integers when the terms a_n of the continued fraction are integers. Relative primeness is a consequence of the identity

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}.$$

13.3.3Corollary

Every finite simple continued fraction $\langle a_0, a_1, \ldots, a_n \rangle$ is a rational number.

Proof. Because $\langle a_0, a_1, \ldots, a_n \rangle = p_n/q_n$.

13.3.4 Theorem

The value of an infinite simple continued fraction is irrational.

Proof. Assume $\xi = \langle a_0, a_1, a_2 \ldots \rangle$ is rational and write ξ = a/b with integers a and b. By Theorem 13.1.9,

$$0 < |a/b - p_n/q_n| < 1/q_n q_{n+1}.$$

Multiplying by bq_n we obtain

$$0 < |aq_n - bp_n| < bq_{n+1}$$

.By choosing n so large that $b/q_{n+1} < 1$, which is possible since $q_{n+1} \to \infty$, we obtain the inequality $0 < |aq_n - bp_n| < 1$. Since aqn − bpn is an integer, this is a contradiction.

13.3.5 Theorem

Every real number can be expressed as a simple continued fraction. The fraction is finite if and only if the real number is rational.

Proof. Let ξ be a real number, and define a0 = [ξ]. We use the following

recursive algorithm to define a (possibly empty) finite or infinite sequence a1, a2, . . . of positive integers.

Step 0**:** If $\xi = a_0$, then $\xi = \langle a_0 \rangle$, and the algorithm stops. Otherwise, $0 < \xi - a_0 < 1$, and we define $\xi 1 = 1/(\xi - a_0)$, noting that $\xi_1 > 1$ and that $\xi = \langle a_0, \xi_1 \rangle$ We then proceed to step 1.

Step k **for** k = 1**,** 2**,** . . . **:** Suppose the positive integers $a_1, a_2, \ldots, a_{k-1}$ and the real number $\xi_k > 1$ have been defined and that $\xi = \langle a_0, a_1, a_2 \ldots, a_{k-1}, \xi k \rangle$,. Define $a_k = [\xi_k]$.

If $\xi_k = a_k$, then $\xi = \langle a_0, a_1, a_2 \ldots, a_k \rangle$, and the algorithm stops. Otherwise, define $\xi_{k+1} = 1/(\xi_k - a_k)$, which is then a real number > 1, note that $\xi_k = \langle a_k, \xi_{k+1} \rangle$, and $\xi = \langle a_0, a_1, a_2 \ldots, a_{k-1}, \xi k \rangle$,and proceed to step k + 1.

If the algorithm stops, then ξ is a finite simple continued fraction. Otherwise it defines an infinite sequence (an)∞ n=0. Define η = ha0, a1, a2, . . .i, and let cn = pn/qn denote the nth convergent of the infinite continued fraction η. Since $\xi = \langle a_0, a_1, \ldots, a_n, \xi_{n+1} \rangle$, , the numbers c_{n-1} and c_n are also convergents of ξ. It therefore follows from Theorem 13.1.9 and Corollary 13.1.6 that ξ and η both lie between the numbers c_{n-1} and c_n. Hence,

$$|\xi - \eta| < |c_n - c_{n-1}| = \frac{1}{q_{n-1} q_n}$$

.

Since $q_n \to \infty$ as $n \to \infty$, we conclude that $\xi = \eta = \langle a_0, a_1, a_2 \ldots \rangle$

Example Using the algorithm of Theorem 13.2.5 we compute the continued fraction expansion of $\sqrt{2}$ as follows:

$a_0 = [\sqrt{2}] = 1$, $\xi_1 = 1/(\xi - a0) = 1/(\sqrt{2} - 1) = \sqrt{2} + 1$;

$a_1 = [\xi_1] = 2$, $\xi_2 = 1/(\xi_1 - a1) = 1/(\sqrt{2} - 1) = \sqrt{2} + 1 = \xi_1$.

Since $\xi_2 = \xi_1$, we conclude that $a_2 = a_1$ and $\xi_3 = \xi_2$, etc. Hence, $a_n = a_1 = 2$ for all $n \geq 1$.

Therefore, $\sqrt{2} = \langle 1, 2, 2, 2, \ldots \rangle = \langle 1, 2 \rangle$.

Since k = k − 1 + 1/1, any integer k can be written in two ways as a simple continued fraction: k = $\langle k \rangle = \langle k-1, 1 \rangle$ = It follows that every rational number has at least two different representations as finite simple continued fractions, because if $\langle a_0, a_1, \ldots, a_n \rangle$ is a representation with an > 1, then

$\langle a_0, a_1, \ldots, a_n - 1, 1 \rangle$ is a different representation ending in 1.

Conversely, if $\langle a_0, a_1, \ldots, a_n, 1 \rangle$ is a continued fraction ending in 1, then $\langle a_0, a_1, \ldots, a_n, 1 \rangle = \langle a_0, a_1, \ldots, a_{n+1} \rangle$.

However, these are the only different ways to represent a rational number as a simple continued fraction. For the proof of this fact we shall need the following lemma.

13.3.6 Lemma

Let a_0, b_0 be integers, let a_1, a_2, . . . , a_n be positive integers, and let x, y be two real numbers ≥ 1. Then

(1) $b_0 = \langle a_0, x \rangle \Rightarrow$ x = 1 and $a_0 = b_0 - 1$

(2) $a_0 \neq b0 \Rightarrow \langle a_0, x \rangle \Rightarrow \neq \langle b_0, y \rangle \Rightarrow$

(3) $\langle a_0, a_1, \ldots, a_n, x \rangle = \langle a_0, a_1, \ldots, a_n, y \rangle \Rightarrow$ x = y

Proof. (1): Suppose $b_0 = \langle a_0, x \rangle$ and x > 1. Then

$a_0 < \langle a_0, x \rangle = b_0 = a_0 + 1/x < a_0 + 1$,

which is a contradiction, since b_0 is an integer.
Hence, x = 1, and $b_0 = a_0 + 1$.

(2): Suppose $a_0 < b_0$; then $\langle a_0, x \rangle = a_0 + 1/x \leq a_0 + 1 \leq b_0 < \langle b_0, y \rangle$

(3): If $\langle a_0, x \rangle \Rightarrow$i = $\langle a_0, y \rangle \Rightarrow$ then obviously x = y, so the assertion holds when n = 0. Now suppose that the implication is true with n replaced by n − 1, and assume that $\langle a_0, a_1, \ldots, a_n, x \rangle = \langle a_0, a_1, \ldots, a_n, y \rangle$ Since $\langle a_0, a_1, \ldots, a_n, x \rangle = \langle a_0, a_1, \ldots, a_{n-1} \langle a_n, x \rangle \rangle$ and the other continued fraction may be shortened analogously, it follows from our induction hypothesis that first $\langle a_n, x \rangle = \langle a_n, y \rangle$, and then x = y.

13.3.7 Theorem

Each integer k has exactly two representations as simple continued fractions, viz. $\langle k \rangle$and $\langle k-1, 1 \rangle$. Each nonintegral rational number has exactly two representations as simple continued fractions, and they are of the form ha0, a1, . . . , ani and ha0, a1, . . . , an − 1, 1i, where n ≥ 1 and an > 1. Each irrational number has a unique representation as an infinite simple continued fraction.

Proof. We have already noted that each rational number has two different representations as finite simple continued fractions, and that each irrational has one representation as infinite simple continued fraction, so it suffices to prove that these representations are the only one.

First assume that k is an integer and k = $\langle a_0, a_1, \ldots, a_n \rangle$ = $\langle a_0, \langle a_1, \ldots, a_n \rangle \rangle$ with n ≥ 1. It then follows from Lemma 13.2.6 (1) that a_0 = k − 1 and x = $\langle a_1, \ldots, a_n \rangle$ = 1. If n ≥ 2, then x > a1 ≥ 1, which is impossible.

Hence n = 1 and a_1 = 1, that isk = $\langle k \rangle$ and $k = \langle k-1, 1 \rangle$, 1i are the only representations of k

as a simple continued fraction.

Let now $\langle a_0, a_1, \ldots, a_n \rangle = \langle b_0, b_1, \ldots, b_m \rangle$ be two representations of a nonintegral rational number, and assume that m ≥ n. Suppose there is an index k < n such that $a_k \neq b_k$, and let k denote the least such index.

Writing the continued fraction $\langle a_0, a_1, \ldots, a_n \rangle$ as

$\langle a_0, \ldots a_{k-1} \langle a_k, \ldots, a_n \rangle \rangle$and similarly for $\langle b_0, b_1, \ldots, b_m \rangle$ we then

conclude, using Lemma 13.2.6 (3), that

$\langle a_k, \ldots, a_n \rangle = \langle b_1, \ldots, b_m \rangle$ or equivalently that

$\langle a_k, a_{k+1}, \ldots, a_n \rangle = b_k, b_{k+1}, \ldots, b_m$

However, this is impossible because of (2). Thus, $a_k = b_k$ for all $k < n$ and we conclude using (3) that $a_n = \langle b_n, \ldots, b_m \rangle$ But a_n is an integer, and we already know that there are only two possible representations of integers as simple continued fractions; either $m = n$ and $a_n = b_n$, or $m = n+1$, $bn = a_{n-1}$ and $b_{n+1} = 1$.

Let finally ξ be an irrational number, and suppose $\xi = \langle a_0, a_1, a_2 \ldots \rangle = \langle b_0, b_1, b_2 \ldots \rangle$ are two different representations of ξ. Then there is a first index k such that $ak \neq bk$, and we conclude from (3) that

$\langle a_k, a_{k+1}, a_{k+2} \ldots \rangle = \langle b_k, b_{k+1}, b_{k+2} \ldots \rangle$

However, this contradicts (2).

Check Your Progress 2

3. What is simple continued fraction ?

4. Prove - Every real number can be expressed as a simple continued fraction. The fraction is finite if and only if the real number is rational

13.4 SUMMARY

Continued fractions are, in some ways, more "mathematically natural" representations of a real number than other representations such as decimal representations, and they have several desirable properties

13.5 KEYWORDS

1.Succession - In **math**, the terms successor directly after a given number.

2.**partial quotient** refers to a method used in solving large division **mathematical** problems.

3.**Recursion** (adjective: **recursive**) occurs when a thing is **defined** in terms of itself or of its type

4.**Coincide definition** is - to occupy the same place in space or time.

13.6 QUESTIONS FOR REVIEW

1.Prove that if the irrational number $x > 1$ is represented by the infinite continued fraction $[a_0 ; a_1, a_2 , ...]$, then $1/x$ has the expansion $[0; a_0 ; a_1, a_2 , ...]$, Use this fact to find the value of $[0; 1, 1, 1, ...] = [0; T]$.

2. Evaluate $[1; 2, \overline{1}]$ and $[1; 2, 3, \overline{1}]$.

3. Determine the infinite continued fraction representation of each irrational number below: $\sqrt{5}$

4.Given the infinite continued fraction [1; 3, 1, 5, 1, 7, 1, 9, ...], find the best rational approximation a/b with

denominator $b < 25$.

13.7 SUGGESTED READINGS

- David M. Burton, Elementary Number Theory, University of New Hampshire.
- G.H. Hardy, and , E.M. Wrigh,. An Introduction to the Theory of Numbers (6th ed, Oxford University Press, (2008).
- W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.
- A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.
- I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.

- T.M. Apostol, Introduction to Analytic number theory, UTM, Springer, (1976).
- J. W. S Cassel, A. Frolich, Algebraic number theory, Cambridge.
- M Ram Murty, Problems in analytic number theory, springer.
- M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer

13.8 ANSWERS TO CHECK YOUR PROGRESS

1. [HINT: Provide the definition and representation 13.1.4]
2. [HINT: Provide the proof 13.1.10]
3. [HINT:Provide the definition and example 13.2.1]
4. [HINT:Provide the proof 13.2.5]

UNIT 14: PERIODIC CONTINUED FRACTION AND PELL'S EQUATION

STRUCTURE

14.0 OBJECTIVE

Understand the concept of Periodic Continued Fractions

Understand the concept of Continued Fraction Expansion of $\sqrt{d}$

Understand the concept of Pell's Equation

14.1 INTRODUCTION

In above unit we computed some periodic simple continued fractions and found that they were roots of quadratic equations with integer coefficients. The goal of this section is to prove that this property characterizes the periodic simple continued fractions, that is an irrational number has a periodic continued fraction expansion if and only if it satifies a quadratic equation with integer coefficients.

14.2 PERIODIC CONTINUED FRACTIONS

14.2.1 Definition

An infinite sequence $(a_n)_{n=0}^{\infty}$is called periodic if there is a non-zero integer p and an integer m such that

$a_n = a_n+p$ for all $n \geq m$.

The integer p is called a period of the sequence. If p and q are two different periods for the sequence, then p − q is a period, too, because $a_n+p-q = a_n+p-q+q = a_n+p = a_n$ for all sufficiently large integers n. Thus, the set of all periods together with the number 0 is an ideal in **Z**. It follows that there exists a smallest positive integer r such that all periods of the sequence are multiples of r.

This uniquely determined number is called the period and the period length of the sequence.

A periodic sequence with period p > 0 can be written in the form

$b_0, b_1, \ldots, b_{m-1}, c_0, c_1, \ldots, c_{p-1}, c_0, c_1, \ldots, c_{p-1}, \ldots$

$= b_0, b_1, \ldots, b_{m-1}, \overline{c_0, c_1, \ldots, c_{p-1}}$

where the bar over the $c_0, c_1, \ldots, c_{p-1}$ indicates that this block of numbers is repeated indefinitely.

A periodic sequence $(a_n)_{n=0}^{\infty}$ with period p > 0 is called purely periodic if $a_n = a_n+p$ holds for all $n \geq 0$. Purely periodic sequences are of the form $a_0, a_1, \ldots, a_{p-1}$.

14.2.2 Definition

An infinite continued fraction $\langle a_0, a_1, a_2 \ldots \rangle$ is called (purely) periodic if the corresponding sequence $(a_n)_{n=0}^{\infty}$ of terms is (purely) periodic. Of course, the period of a periodic continued fraction is by definition the period of the sequence of terms.

Let $\xi = \langle a_0, a_1, a_2 \ldots \rangle$ be a continued fraction and write

$$\xi k = \langle a_k, a_{k+1}, a_{k+2} \ldots \rangle$$

If ξ is a periodic continued fraction with period p, then obviously there is an integer m such that $\xi n = \xi n+p$ holds for all $n \geq m$. Conversely, if $\xi n+p$

= ξn holds for some number n, then ξ is a periodic continued fraction with p as a period (and the period r is some divisor of p).

14.2.3 Definition

An irrational number ξ is called a quadratic irrational (or algebraic of degree two) if it is the root of a quadratic polynomial with integer coefficients, that is if $a\xi^2 + b\xi + c = 0$ for suitable integer coefficients a, b, and c with $a \neq 0$.

14.2.4 Proposition

A real number ξ is a quadratic irrational if and only if it has the form $\xi = r + s\sqrt{d}$, where d is a positive integer that is not a perfect square, r and s are rational numbers and $s \neq 0$.

Proof. Any real irrational solution of a quadratic equation $ax^2 + bx + c = 0$ obviously has this form. Conversely, a real number of this form is irrational and satisfies the quadratic equation $(x - r)^2 = s^2d$, which can be turned into a quadratic equation with integer coefficients upon multiplication by the squares of the denominators of r and s.

14.2.5 Definition

Let d be a positive integer that is not a perfect square. We define $\mathbf{Q}[\sqrt{d}\,]$ to be the set of all real numbers ξ of the form $\xi = r + s\sqrt{d}$, with r and s rational. The number $\xi_0 = r - s\sqrt{d}$ is called the conjugate of ξ.

14.2.6 Proposition

$\mathbf{Q}[\sqrt{d}]$ is a number field, that is if ξ and η are numbers in $\mathbf{Q}[\sqrt{d}\,]$, then their sum ξ + η, difference ξ − η, product ξη, and quotient ξ/η also belong to $\mathbf{Q}[\sqrt{d}\,]$, the quotient of course provided $\eta \neq 0$.

14.2.7 Proposition

Suppose ξ, η ∈ **Q**[√d]. Then (ξ + η)' = ξ' + η', (ξ − η)' = ξ' − η', (ξη)' = ξ'η', and (ξ/η)' = ξ'/η'.

14.2.8 Proposition

If the number ξ has a periodic simple continued fraction expansion, then ξ is a quadratic irrational.

Proof. Being an infinite continued fraction, ξ is irrational. We will prove that ξ ∈ **Q**[√d] for a suitable positive integer d that is not a perfect square.

Assume

$$\xi = \langle b_0, b_1, \ldots, b_{m-1}, \overline{c_0, c_1, \ldots, c_{r-1}} \rangle$$

and let $\eta = \langle \overline{c_0, c_1, \ldots, c_{r-1}} \rangle$. Then $\eta = \langle c_0, c_1, \ldots, c_{r-1}, \eta \rangle$.

Let (p_k, q_k) be the convergents of the continued fraction $\langle c_0, c_1, \ldots, c_{r-1} \rangle$.

Then

$$\eta = \langle c_0, c_1, \ldots, c_{r-1}, \eta \rangle = \frac{\eta p_{r-1} + p_{r-2}}{\eta q_{r-1} + q_{r-2}},$$

and solving for η we see that η satisfies a quadratic equation with integer coefficients. Hence, η is a quadratic irrational, that is η ∈ **Q**[√d] for a suitable positive integer d that is not a perfect square. Similarly, in terms of the convergents (P_k, Q_k) of $\langle b_0, b_1, \ldots, b_{m-1} \rangle$, we have

$$\xi = \langle b_0, b_1, \ldots, b_{m-1}, \eta \rangle = \frac{\eta P_{m-1} + P_{m-2}}{\eta Q_{m-1} + Q_{m-2}},$$

so by Proposition 14.1.6, ξ belongs to **Q**[√d]. The converse of Proposition 14.1.8 is true, that is every quadratic irrational has a periodic simple continued fraction expansion. The proof of this needs some preparatory work.

14.2.9 Lemma

If ξ is a quadratic irrational, then ξ can be written in the form

$$\xi = \frac{u + \sqrt{d}}{v},$$

where d is an integer that is not a perfect square, u and v are integers, and v | (d − u^2).

Proof. By Proposition 14.1.4, ξ = r + s$\sqrt{D}$, where D is an integer that is not a perfect square, r and s are rational numbers and s ≠ 0. We can obviously write r = a/c and s = b/c, where a, b, and c are integers and b > 0. Then

$$\xi = \frac{a + b\sqrt{D}}{c} = \frac{a|c| + \sqrt{b^2c^2D}}{c|c|} = \frac{u + \sqrt{d}}{v},$$

and the integers u = a|c|, v = c|c| and d = b^2c^2D satisfy the requirement v | (d − u^2). Suppose ξ_0 is a quadratic irrational. Using Lemma 14.1.9, we first write ξ_0 = (u_0 +$\sqrt{d}$)/v_0, where d is an integer that is not a perfect square, and u0 and v0 are integers, and v_0 | (d − u_0^2).

We then recall the recursive algorithm in Theorem 13.1.5 for obtaining the continued fraction expansion of $\langle a_0, a_1, a_2 \ldots \rangle$ of ξ_0. The terms a_n are

$$a_0 = [\xi_0], \quad \xi_{n+1} = \frac{1}{\xi_n - a_n}, \quad \text{and} \quad a_{n+1} = [\xi_{n+1}] \qquad \text{for } n = 0, 1, 2, \ldots,$$

given by and we have ξ_0 = $\langle a_0, a_1, \ldots, a_n, \xi_{n+1} \rangle$ for all n.

Now suppose inductively that ξn = (un +$\sqrt{d}$)/v_n, with integers u_n and v_n that satisfy v_n | (d − u^2 n). Then

$$\xi_{n+1} = \frac{1}{\xi_n - a_n} = \frac{1}{\frac{\sqrt{d} - (a_n v_n - u_n)}{v_n}} = \frac{\sqrt{d} + (a_n v_n - u_n)}{\frac{d - (a_n v_n - u_n)^2}{v_n}} = \frac{u_{n+1} + \sqrt{d}}{v_{n+1}},$$

where $u_{n+1} = a_n v_n - u_n$ and $v_{n+1} = (d - u_{n+1}^2)/v_n$.

Clearly, u_{n+1} is an integer and $u_{n+1} \equiv -u_n \pmod{v_n}$. Hence by the induction assumption,

$d - u_{n+1}^2 \equiv d - u_n^2 \equiv 0 \pmod{vn}$, that is v_n divides $d - u_{n+1}^2$. Therefore, v_{n+1} is also an integer, and $v_{n+1} \mid (d - u_{n+1}^2)$, because $v_n v_{n+1} = d - u_{n+1}^2$.

By induction, we have thus proved the validity of the following algorithm:

14.2.10 Theorem

Suppose $\xi_0 = (u_0 + \sqrt{d})/v_0$, where d is a positive integer that is not a perfect square, u0 and v0 are integers and $v0 \mid (d - u_0^2)$. Define recursively the sequences $(u_n)_0^\infty$, $(v_n)_0^\infty$, $(a_n)_0^\infty$ and $(\xi_n)_0^\infty$ as follows:

$$\xi_n = \frac{u_n + \sqrt{d}}{v_n}, \qquad a_n = [\xi_n]$$

$$u_{n+1} = a_n v_n - u_n, \qquad v_{n+1} = \frac{d - u_{n+1}^2}{v_n}, \qquad for\ n \geq 0.$$

Then u_n and v_n are integers, $v_n \mid (d - u_n^2)$, and $\xi_0 = \langle a_0, a_1, \ldots, a_n, \xi_{n+1} \rangle$ for all n, and $\xi 0 = \langle a_0, a_1, a_2, \ldots \rangle$

Example: Let us compute the continued fraction expansion of the number $(1 - \sqrt{5})/3$ using the algorithm of Theorem 14.1.10. Since $36 \mid (5 - 12)$, we first have to put the number in the form of Lemma 23.9. Multiplying numerator and denominator by −3, we obtain

$$\xi_0 = \frac{-3 + \sqrt{45}}{-9},$$

that is $u_0 = -3$, $v_0 = -9$, and $d = 45$. Now v0 | (d−u2 0), so we can start the algorithm. The result of the computations is shown in the following table

n	0	1	2	3	4	5	6	7	8	9
u_n	−3	12	−1	5	5	3	6	6	3	5
v_n	−9	11	4	5	4	9	1	9	4	5
a_n	−1	1	1	2	2	1	12	1	2	2

Since $(u_9, v_9) = (u_3, v_3)$, we conclude that $\xi_9 = \xi_3$. Thus,

$$\frac{1-\sqrt{5}}{3} = \langle -1, 1, 1, \overline{2, 2, 1, 12, 1, 2} \rangle.$$

14.2.11 Lemma

Let ξ be a quadratic irrational and define ξn as in Theorem 14.1.10. If the conjugate $\xi'_k < < 0$ for some index k, then $-1 < \xi'_n < 0$ for all n > k.

Proof. By induction, it suffices to prove that $\xi'_n < < 0$ implies $-1 < \xi'_n < +1 < 0$. So assume $\xi'_n < < 0$. Using the relation $\xi_{n+1} = 1/(\xi_n - a_n)$ and taking conjugates, we obtain ξn 0 +1 = $1/(\xi'_n - a_n)$. Since $a_n \geq 1$, the denominator $\xi'_n < - a_n$ is strictly less than −1, so it follows that $-1 < \xi'_n < +1 < 0$.

14.2.12 Lemma

Let ξ be a quadratic irrational, and define ξ_n and an = $[\xi_n]$ as above. If −1 < $\xi'_n < 0$, then an = $[-1/\xi'_{n+1}]$.

Proof. We have $\xi'_{n+1} = 1/(\xi'_n - a_n)$, whence $-1/\xi'_n + 1 = an - \xi'_n$. Since 0 < $-\xi'_n < 1$, it follows that $[-1/\xi'_{n+1}].] = [a_n - \xi'_n] = a_n$.

14.2.13 Lemma

If ξ is a quadratic irrational, then there exists an index k such that $\xi'_k < 0$.

Proof. Let (p_k, q_k) denote the kth convergent of ξ. Since $\xi = \langle a_0, a_1, \ldots, a_{n-1}, \xi_n \rangle$, we have

$$\xi = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}},$$

and solving for ξn we obtain

$$\xi_n = \frac{q_{n-2}\xi - p_{n-2}}{p_{n-1} - q_{n-1}\xi} = -\frac{q_{n-2}}{q_{n-1}}\left(\frac{\xi - p_{n-2}/q_{n-2}}{\xi - p_{n-1}/q_{n-1}}\right).$$

By taking conjugates, we get

$$\xi_n' = -\frac{q_{n-2}}{q_{n-1}}\left(\frac{\xi' - p_{n-2}/q_{n-2}}{\xi' - p_{n-1}/q_{n-1}}\right).$$

We now use the fact that the convergents pn/qn converge to ξ as n tends to infinity and that ξ' ≠ ξ. It follows that the expression within parenthesis converges to (ξ' − ξ)/(ξ' − ξ), that is to 1, as n tends to infinity. Consequently, the expression within parenthesis is certainly > 0 when n is big enough, that is ξ'_n has the same sign as $-q_{n-2}/q_{n-1}$, which is negative since q_n is positive for all n ≥ 0.

14.2.14 Theorem

A real number ξ has a periodic simple continued fraction expansion if and only if it is a quadratic irrational.

Proof. We have already proved that a periodic continued fraction is a quadratic irrational (Proposition 14.1.8). To prove the converse, let ξ = ξ ' be a quadratic irrational and write

$$\xi_n = \frac{u_n + \sqrt{d}}{v_n}$$

as in Theorem 14.1.10. By Lemma 14.1.13, there is an index k such that

$\xi'_k < 0$,

and by Lemma 14.1.11, −1 < $\xi'_n < 0$ for all n > k. Since ξn > 1 for all n ≥ 1, we conclude that

$$1 < \xi_n - \xi_n' = \frac{2\sqrt{d}}{v_n} \quad \text{and} \quad 0 < \xi_n + \xi_n' = \frac{2u_n}{v_n}$$

for all n > k. Hence 0 < vn < 2 $\sqrt{d}$ and $u_n > 0$ if n > k. Moreover, using the relation d − $u_{n+1}^2 = v_n v_{n+1} > 0$, we obtain $u_{n+1}^2 =$ < d, that is $u_{n+1} <$ $\sqrt{d}$ for n > k. Thus, if n > k + 1, then $0 < u_n <$ $\sqrt{d}$ and 0 < vn < 2 $\sqrt{d}$. Hence, the ordered pairs (un, vn) can assume only a fixed number of possible pair values, and so there are distinct integers i and j with j > i such that $u_j = u_i$ and $v_j = v_i$. This implies that $\xi_i = \xi_j = \xi_{i+(j-i)}$, and hence ξ has a periodic continued fraction expansion.

14.2.15 Definition

A quadratic irrational ξ = r + s $\sqrt{d}$ is called reduced it ξ > 1 and its conjugate ξ0 = r − s $\sqrt{d}$. satisfies $-1 < \xi_0 < 0$.

14.2.16 Theorem

The simple continued fraction expansion of the real quadratic irrational number ξ is purely periodic if and only if ξ is reduced. Also, if ξ = $\langle a_0, a_1, \ldots, a_{r-1} \rangle$,, then −1/ξ0 = $\langle \overline{a_{r-2}, a_{r-1}, \ldots, a_1, a_0} \rangle$.

Proof. Suppose ξ = ξ0 is a reduced quadratic irrational, and use Theorem 14.1.10 to write ξn = (un + $\sqrt{d}$)/vn. Since −1 < ξ0 0 < 0 by assumption, we have −1 < ξn 0 < 0 and an = [−1/ξn 0 +1] for all n ≥ 0 by Lemma 14.1.11 and Lemma 14.1.12. We know from Theorem 14.1.14 that ξ has a simple periodic continued fraction expansion. Let r be the period length; then there is a smallest number m ≥ 0 such that

$$\xi_{n+r} = \xi_n \text{ for all } n \geq m.$$

We must prove that m = 0.

Assume m ≥ 1. Starting from ξm = ξm+r we first obtain $\xi_m' =$

ξ'_{m+r} by taking conjugates, and hence $a_{m-1} = [-1/\xi'_m] = [-1/\xi'_{m+r}] = a_{m+r-1}$. Since

$$\frac{1}{\xi_{m-1} - a_{m-1}} = \xi_m = \xi_{m+r} = \frac{1}{\xi_{m+r-1} - a_{m+r-1}},$$

we then conclude that $\xi_{m-1+r} = \xi_{m-1}$, which violates the definition of m. Thus m = 0, and ξ is purely periodic.

Conversely, suppose that ξ is purely periodic, say $\xi = \langle a_0, a_1, \ldots, a_{r-1} \rangle$, where $a_0, a_1, \ldots, a_{r-1}$ are positive integers. Then $\xi > a0 \geq 1$. Let (p_n, q_n) denote the nth convergent of ξ; then

$$\xi = \langle a_0, a_1, \ldots, a_{r-1}, \xi \rangle = \frac{p_{r-1}\xi + p_{r-2}}{q_{r-1}\xi + q_{r-2}}.$$

Thus ξ satisfies the quadratic equation
$f(x) = q_{r-1}x^2 + (q_{r-2} - p^{r-1})x - p_{r-2} = 0.$

This equation has two roots, ξ and its conjugate ξ' .Since ξ > 1, we need only prove that f(x) has a root between −1 and 0 to establish that −1 < ξ' < 0. We will do this by showing that f(0) < 0 and f(−1) > 0.

Note that p_n is positive for all $n \geq -1$ (since a0 > 0). Hence, $f(0) = -p_{r-2} < 0$. Next we see that $f(-1) = q_{r-1} - q_{r-2} + p_{r-1} - p_{r-2} = (a_{r-1} - 1)(q_{r-2} + p_{r-2}) + q_{r-3} + p_{r-3}$
$\geq q_{r-3} + p_{r-3} > 0.$

Thus, ξ is reduced. Finally, to prove that $-1/\xi_0$ has the stated continued fraction expansion, we suppose that $\xi = \langle \overline{a_0, a_1, \ldots, a_{r-1}} \rangle$,. Taking conjugates in the relation $\xi_n = 1/(\xi_{n-1} - a_{n-1})$ we obtain $\xi'_n = = 1/(\xi'_n = -1 - a_{n-1})$, which can be rewritten as

$$-1/\xi'_n = a_{n-1} + \frac{1}{-1/\xi'_{n-1}} \quad \text{for all } n \geq 1.$$

Since $-1/\xi_n' > 1$ for all n, the above equation can be expressed as a continued fraction expansion

$$-1/\qquad\qquad \xi_n' = \langle a_{n-1}, -1/\xi_{n-1}' \rangle.$$

Starting with $-1/\xi'$, iterating and using the fact that $\xi = \xi' = \xi r$, we thus obtain

$$-1/\xi' = -1/\xi_0' = -1/\xi_r' = \langle a_{r-1}, -1/\xi_{r-1}' \rangle = \langle a_{r-1}, a_{r-2}, -1/\xi_{r-1}' \rangle = \ldots$$

$$= \langle a_{r-2} a_{r-1}, \ldots, a_1, a_0, -1/\xi_0' \rangle$$

Hence, $-1/\xi' = \langle a_{r-2} a_{r-1}, \ldots, a_1, a_0 \rangle$

Example: The quadratic irrational $(2 + \sqrt{10})/3$ is reduced. Its continued fraction expansion is easily computed with the aid of Theorem 23.10. Since $3 \mid (10 - 22)$, we can start with u0 = 2, v0 = 3 and d = 10. The computations are summarized in the following table:

n	0	1	2	3
u_n	2	1	2	2
v_n	3	3	2	3
a_n	1	1	2	1

Since (u3, v3) = (u0, v0), the period is 3 and $(2 + \sqrt{10})/3 = \langle 1,1,2 \rangle$

Check Your Progress 1

1. Define Quadatic irrational and pure periodic continued fraction.

2. Explain 'A real number ξ has a periodic simple continued fraction expansion if and only if it is a quadratic irrational'.

14.3 CONTINUED FRACTION EXPANSION OF $\sqrt{D}$

14.3.1Theorem

Let d be a positive integer that is not a perfect square. The simple continued fraction expansion of $\sqrt{d}$ is of the form

$$\langle a_0, \overline{a_1, \ldots, a_{r-1}, 2a_0} \rangle$$

where $a_0 = [\sqrt{d}]$ and $a_j = a_{r-j}$ for j = 1, 2, ..., r − 1.

Proof. Let $a_0 = [\sqrt{d}\,]$ and $\xi = a_0 + \sqrt{d}$. Then ξ is reduced, because ξ > 1 and $\xi' = a_0 - \sqrt{d}$ satisfies $-1 < \xi_0 < 0$. By Theorem 23.16, ξ has a purely periodic continued fraction expansion starting with $[\xi] = 2a_0$, say

(1) $\xi = a_0 + \sqrt{d} = \langle \overline{2a_0,\ a_0, a_1, \ldots, a_{r-1}} \rangle =$
$\langle \overline{2a_0,\ a_0, a_1, \ldots, a_{r-1}, 2a_0} \rangle$

If we subtract a_0 from each side, we get

$\sqrt{d} = \langle a_0, \overline{a_1, \ldots, a_{r-1}, 2a_0} \rangle$

To prove that the sequence $a_1, a_2, \ldots, a_{r-1}$ is "symmetric", we note that

$$\xi = a_0 + \sqrt{d} = 2a_0 + \sqrt{d} - a_0 = 2a_0 - \xi' = 2a_0 + \frac{1}{-1/\xi'} = \langle 2a_0, -1/\xi' \rangle.$$

By Theorem 14.1.16,

$-1/\xi' = \langle \overline{a_{r-1}, a_{r-2}, \ldots, a_1, 2a_0} \rangle$

and hence

$\xi = \langle 2a_0, \overline{a_{r-1}, a_{r-2}, \ldots, a_1, 2a_0} \rangle$

A comparison with (1) gives $a_j = a_{r-j}$ for $1 \le j \le r-1$.

Example: To compute the continued fraction expansion of $\sqrt{19}$ we use Theorem 14.1.10 with $u_0 = 0$, $v_0 = 1$ and $d = 19$. We get the following table:

n	0	1	2	3	4	5	6	7
u_n	0	4	2	3	3	2	4	4
v_n	1	3	5	2	5	3	1	3
a_n	4	2	1	3	1	2	8	2

It follows that the expansion has period length 6, and that $\sqrt{19} = \langle 4, 2, 1, 3, 1, 2, 8 \rangle$

14.3.2 Theorem

Let (pn, qn) denote the nth convergent of d, let the integers u_n and v_n be defined for the number $\xi = \sqrt{d}$ as in Theorem 14.1.10, that is $\xi_n = (u_n + \sqrt{d})/v_n$ with $v_n \mid (d - u^2n)$, and let r be the period length of the continued fraction expansion of $\sqrt{d}$). Then

(i) $p_n^2 - dq_n^2 = (-1)^{n-1} v_{n+1}$ for every $n \ge -1$;

(ii) $v_n > 0$ for every $n \ge 0$;

(iii) $v_n = 1$ if and only if $r \mid n$.

Proof. Write $\sqrt{d} = \langle a_0, a_1, a_2 \ldots, \rangle, = \langle a_0, a_1, a_2 \ldots, \xi_{n+1} \rangle$

(i) We have

$$\sqrt{d} = \frac{\xi_{n+1} p_n + p_{n-1}}{\xi_{n+1} q_n + q_{n-1}} = \frac{(u_{n+1} + \sqrt{d}) p_n + v_{n+1} p_{n-1}}{(u_{n+1} + \sqrt{d}) q_n + v_{n+1} q_{n-1}},$$

which can also be written as

$u_{n+1}\ p_n + v_{n+1}\ p_{n-1} - dq_n - (u_{n+1}\ q_n + v_{n+1}\ q_{n-1} - p_n)\sqrt{d} = 0.$

Since $\sqrt{d}$ is irrational, it follows that

$$\begin{cases} u_{n+1}p_n + v_{n+1}p_{n-1} - dq_n = 0 \\ u_{n+1}q_n + v_{n+1}q_{n-1} - p_n = 0 \end{cases}$$

Eliminating u_{n+1} from this system, we obtain

$p_n^2 - dq_n^2 = v_{n+1}(p_nq_{n-1} - q_n p_{n-1}) = (-1)^{n-1} v_{n+1}$,

(ii) The convergents p_n/q_n are $> \sqrt{d}$ if n is odd and $< \sqrt{d}$ if n is even. Therefore, $p_n^2 - dq_n^2$ has the same sign as $(-1)n-1$, so it follows from (i) that v_{n+1} is positive for every $n \geq -1$.

(iii) Since $\xi = \sqrt{d}$ has period length r, $\xi_{kr+1} = \xi_1$ for all positive integers k. It follows that

$$\xi_{kr} - a_{kr} = \frac{1}{\xi_{kr+1}} = \frac{1}{\xi_1} = \xi_0 - a_0 = -a_0 + \sqrt{d},$$

that is $\xi_{kr} = a_{kr} - a_0 + \sqrt{d}$ Hence, $_{vkr} = 1$ (and $u_{kr} = a_{kr} - a_0$). Conversely, assume $v_n = 1$; then $\xi_n = u_n + \sqrt{d}$ so

$$a_n = [\xi_n] = u_n + [\sqrt{d}\ ] = u_n + a_0$$

and

$$\xi_n - a_n = \sqrt{d} - a_0 = \xi_0 - a_0,$$

that is $\xi_{n+1} = 1/(\xi_n - a_n) = 1/(\xi_0 - a_0) = \xi_1$.

It follows from this that n is a multiple of the period length r. The reader may have noted in the few examples of continued fraction expansion of √d that we have given, that the numbers appearing in the period of $\sqrt{d}$ were all less than or equal to a0 except for the last one, which equals $2a_0$. This holds in general.

14.3.3 Proposition

Let $\sqrt{d} = \langle a_0, a_1, \ldots, a_{r-1}, 2a_0 \rangle$, i. Then $a_n \leq a_0$ for $1 \leq n \leq r - 1$.

Proof. With $\xi = \xi_0 = \sqrt{d}$,let $\xi_n = (u_n + \sqrt{d})/v_n$ be as in Theorem14.1.10 and suppose $1 \leq n \leq r - 1$. Then $v_n \geq 2$ by the previous theorem, and using Lemma 14.1.11 we conclude that $\xi_n' = (u_n - \sqrt{d})/v_n < 0$, because $\xi_0' = -\sqrt{d} < 0$.
It follows that $u_n - \sqrt{d} < 0$, that is $u_n < \sqrt{d}$ and hence $\xi_n < 2\sqrt{d}/v_n \leq \sqrt{d}$.
Finally, $a_n = [\xi_n] \leq [\sqrt{d}] = a_0$.

14.4 Pell's Equation

The equation $x^2 - dy^2 = N$, with given non-zero integers d and N, is called Pell's equation. If d is negative, Pell's equation can have only a finite number of solutions in integers, since $x^2 \leq N$ and $y^2 \leq -N/d$. If $d = a^2$ is a perfect square, then we have $(x + ay)(x - ay) = N$, and again there is only a finite number of integral solutions to Pell's equation, since there is only a finite number of ways to factor N.
We will therefore suppose that d is a positive integer that is not a perfect square. We will show that in that case there is either no solution at all or infinitely many solutions in integers. When $N = \pm 1$, we will give a complete description of the set of solutions.

If (u, v) is an integral solution of Pell's equation $x^2 - dy^2 = N$, then (±u, ±v) is also a solution for every combination of the signs. Thus, in order to find all integral solutions it suffices to find all positive solutions, that is all solutions (u, v) with $u > 0$ and $v > 0$. If N is a perfect square, there will of course be two additional trivial solutions $(\pm\sqrt{N}, 0)$, and if $-N/d$ happens to be an integer that is a perfect square, $(0, \pm \sqrt{-N/d})$ are two trivial solutions of Pell's equation.

If (x_1, y_1) and (x_2, y_2) are two positive solutions of $x^2 - dy^2 = N$, then $x_1^2 - x_2^2 = d(y_1^2 - y_2^2)$, and hence $x_1 < x_2$ if and only if $y_1 < y_2$. Thus, if we order the positive solutions according to increasing x-value or according to increasing y-value we will get the same result. If there is a positive

solution in integers of Pell's equation, then there is obviously a positive solution (x_1, y_1) with a least positive x-value. This solution has also the least y-value among all positive solutions. Since it plays a special role we introduce the following definition.

14.4.1 Definition

Suppose Pell's equation $x^2 - dy^2 = N$ has positive integral solutions. The fundamental solution, or least positive solution, is the positive solution (x_1, y_1) such that $x_1 < u$ and $y_1 < v$ for every other positive solution (u, v). The following theorem gives a connection between Pell's equation and continued fractions.

14.4.2 Theorem

Let d be a positive integer that is not a perfect square, and suppose $|N| < \sqrt{d}$. If (u, v) is a positive solution in integers of $x^2 - dy^2 = N$,then there is a convergent (pn, qn) of the simple continued fraction expansion of $\sqrt{d}$ such that $u/v = p_n/q_n$.

Remark. The numbers u and v need not be relatively prime, but if c is their greatest common divisor, then obviously $c^2 \mid N$. Hence, if N is square-free, and in particular if $N = \pm 1$, then u and v are necessarily relatively prime. That means that there is an index n such that $u = p_n$ and $v = q_n$.

Proof. We will consider a more general situation. Let d and N be any positive real numbers, not necessarily integers, such that $\sqrt{d}$ is irrational and $N < \sqrt{d}$ and assume that u and v are positive integers satisfying $u^2 - dv^2 = N$.

Since

$$\left(\frac{u}{v} - \sqrt{d}\right)\left(\frac{u}{v} + \sqrt{d}\right) = \frac{u^2 - dv^2}{v^2} = \frac{N}{v^2}$$

and the second factor of the left hand side is positive, we first conclude that $u/v - \sqrt{d} > 0$, and consequently $u/v + \sqrt{d} > 2\sqrt{d}$. Hence

$$0 < \frac{u}{v} - \sqrt{d} = \frac{N}{v^2(u/v + \sqrt{d})} < \frac{\sqrt{d}}{2v^2\sqrt{d}} = \frac{1}{2v^2}.$$

u/v is a convergent of $\sqrt{d}$. Let now d and N be as in the statement of the theorem. The case N > 0 is a special case of what we have just proved. If N < 0, we rewrite the equation as $y^2 - (1/d)x^2 = -N/d$. Since $0 < -N/d < \sqrt{d}/d = p1/d$, we can apply the general case above, and we conclude that v/u is a convergent of $1/\sqrt{d}$. Suppose $\sqrt{d}$ has the continued fraction expansion ha0, a1, a2, . . . i. Then $1/\sqrt{d} = h0, \sqrt{d_i} = \langle a_0, a_1, a_2 \ldots, \rangle$.Hence, there is an n such that

u/v = $\langle a_0, a_1, a_2 \ldots, \rangle$is a convergent of $\sqrt{d}$

$$\frac{v}{u} = \langle 0, a_0, a_1, \ldots, a_n \rangle = \frac{1}{\langle a_0, a_1, \ldots, a_n \rangle},$$

By combining the theorem above with Theorem 14.2.2, we get a complete description of the solution set of Pell's equation in the case N = ±1

14.4.3 Theorem

Suppose d is a positive integer that is not a perfect square, let r be the period length of the simple continued fraction expansion of $\sqrt{d}$, and let $(p_n, q_n)_{n=0}^{\infty}$be the corresponding sequence of convergents.

(i) Suppose r is even. Then

(a) $x^2 - dy^2 = -1$ has no solutions in integers;

(b) all positive integral solutions of $x^2 - dy^2 = 1$ are given by $x = p_{kr-1}, y = q_{kr-1}$ for k = 1, 2, 3, . . . , with $x = p_{r-1}$ and $y = q_{r-1}$ as the fundamental solution.

(ii) Suppose r is odd Then

(a) all positive integral solutions of $x^2 - dy^2 = -1$ are given by $x = p_{kr-1}, y = q_{kr-1}$ for k = 1, 3, 5, . . . , with $x = p_{r-1}$ and $y = q_{r-1}$ as the fundamental solution;

(b) all positive integral solutions of x2 − dy2 = 1 are given by x = p_{kr-1}, y = q_{kr-1} for k = 2, 4, 6, . . . , with x = p_{2r-1} and y = q_{2r-1} as the fundamental solution.

Proof. By the previous theorem, the positive integral solutions of $x^2-dy^2 = \pm 1$ are to be found among the convergents (pn, qn). Furthermore, $a_0 = [\sqrt{d}] \geq 1$, so the sequence $(p_n)_{n=0}^{\infty}$ is strictly increasing. Therefore, the first solution that appears in the sequence (p_n, q_n) will be the fundamental solution.

According to Theorem 14.2.2, $p_n^2 - dq_n^2 = (-1)^{n-1} v_{n+1}$, where $v_n \geq 1$ for all n and $v_n = 1$ if and only if r | n. Thus, $|p_n^2 - dq_n^2| \geq 2$ except when n = kr – 1 for some non-negative integer k, in which case

$$p_n^2 - dq_n^2 = (-1)^k r.$$

If r is even, then $(-1)^{kr} = 1$ for all k, and hence (p_{kr-1}, q_{kr-1}) is a solution of $x^2 - dy^2 = 1$ for all k, whereas the equation $x^2 - dy^2 = -1$ has no positive solution, and of course no solution at all in integers. This proves part (i). If the period length r is odd, then $(-1)^{kr} = 1$ for k even, and = −1 for k odd, and this proves part (ii).

Example: We shall use Theorem 14.3.3 to find the fundamental solution of the equation $x^2 - 19y^2 = 1$.

The continued fraction expansion $\sqrt{19} = \langle 4, 2, 1, 3, 1, 2, 8 \rangle$ was found in the previous section. Since the period length is 6, the fundamental solution is (x, y) = (p_5, q_5). The convergents are computed in the following table:

n	−2	−1	0	1	2	3	4	5
a_n			4	2	1	3	1	2
p_n	0	1	4	9	13	48	61	170
q_n	1	0	1	2	3	11	14	39

Thus, the fundamental solution is (x, y) = (170, 39).

14.4.4 Lemma

Let (x1, y1) be an arbitrary integral solution of $x^2 - dy^2 = M$ and (x_2, y_2) an arbitrary integral solution of $x^2 - dy^2 = N$, and define the integers u and v by

$$(x_1 + y_1\sqrt{d})\ (x_2 + y_2\sqrt{d})) = u + v\sqrt{d})$$

that is $u = x_1x_2 + y_1y_2d$, $v = x_1y_2 + x_2y_1$. Then (u, v) is a solution of $x^2 - dy^2 = MN$. If (x_1, y_1) and (x_2, y_2) are positive solutions, then (u, v) is also positive.

Proof. By taking conjugates we have $(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = u - v\sqrt{d}$ and hence

$$u^2 - dv^2 = (u + v\sqrt{d})(u - v\sqrt{d})$$

$$= (x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d})$$

$$= (\quad x_1^2 - \quad d \quad y_1^2)(\quad x_2^2 - d \quad y_2^2) = MN.$$

The solution (u, v) will obviously be positive if the original ones are positive.

14.4.5 Corollary

If the equation $x^2 - dy^2 = N$ has an integral solution, then it has infinitely many integral solutions.

Proof. Suppose the equation $x^2 - dy^2 = N$ has at least one integral solution. This solution multiplied by any solution of $x^2 - dy^2 = 1$ yields another solution of $x^2 - dy^2 = N$. Since the equation $x^2 - dy^2 = 1$ has infinitely many integral solutions, there will also be infinitely many integral solutions of $x^2 - dy^2 = N$.

14.4.6 Theorem

Let (x_1, y_1) be the fundamental solution of $x^2 - dy^2 = 1$. Then all positive integral solutions are given by (x_n, y_n), $n \geq 1$, where the integers x_n and yn are recursively defined by

$$x_{n+1} = x_1x_n + y_1y_nd,\ y_{n+1} = x_1y_n + y_1x_n.$$

Proof. Note that $x_{n+1} + y_{n+1}\sqrt{d} = (x_1 + y_1\sqrt{d})(x_n + y_n\sqrt{d}) = (x_1 + y_1\sqrt{d})^{n+1}$.

Hence by Lemma 14.3.4 with M = N = 1, if (x_n, y_n) is a positive solution of Pell's equation $x^2 - dy^2 = 1$, then (x_{n+1}, y_{n+1}) will also be a positive solution. It therefore follows by induction, that (x_n, y_n) is a solution for all n. It remains to show that every positive integral solution is obtained in this way. Suppose there is a positive solution (u, v) that is not of the form (x_n, y_n).

Since x

n forms an increasing sequence, there must be some integer m such that $x_m \leq u < x_{m+1}$. It follows that $y_m \leq v < y_{m+1}$, because we get the same result if positive solutions are ordered according to their x-value or y-value. We cannot have equality, because u = xm would imply v = ym. Now $(x_m, -y_m)$ is of course also a (non-positive) solution of $x^2 - dy^2 = 1$, so by Lemma 14.3.4 we

will obtain another solution (s, t) by defining

$$s + t\sqrt{d} = (u + v\sqrt{d})(x_m - y_m\sqrt{d}) = \frac{u + v\sqrt{d}}{x_m + y_m\sqrt{d}}.$$

Since $x_m + y_m\sqrt{d} < u + v\sqrt{d} < x_{m+1} + y_{m+1}\sqrt{d}$, we have

$$1 < s + t\sqrt{d} < \frac{x_{m+1} + y_{m+1}\sqrt{d}}{x_m + y_m\sqrt{d}} = x_1 + y_1\sqrt{d}.$$

But $s - t\sqrt{d} = 1/(s + t\sqrt{d})$ and hence $0 < s - t\sqrt{d} < 1$. It now follows that

$$s = \tfrac{1}{2}(s + t\sqrt{d}) + \tfrac{1}{2}(s - t\sqrt{d}) > \tfrac{1}{2} + 0 > 0$$
$$t\sqrt{d} = \tfrac{1}{2}(s + t\sqrt{d}) - \tfrac{1}{2}(s - t\sqrt{d}) > \tfrac{1}{2} - \tfrac{1}{2} = 0,$$

so (s, t) is a positive solution. Therefore, $s > x_1$ and $t > y_1$, but this contradicts $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. This contradiction shows that every integral solution (u, v) must be of the form (x_n, y_n).

Example : In above Example, we showed that the fundamental solution of $x^2 - 19y^2 = 1$ is $(x_1, y_1) = (170, 39)$.

Using the recursion formulas

$xn = x_1x_n + 19y_1y_n$, $y_n = x_1y_n + y_1x_n$,

we can compute the next positive solutions. They are

$(x_2, y_2) = (57\ 799, 13\ 260)$

$(x_3, y_3) = (19\ 651\ 490, 4\ 508\ 361)$

$(x_4, y_4) = (6\ 681\ 448\ 801, 1\ 532\ 829\ 480)$

Just as in the case of $x^2 - dy^2 = 1$, further solutions of the equation $x^2 - dy^2 = -1$ can be found from its fundamental solution.

14.4.7 Theorem

Suppose that $x^2 - dy^2 = -1$ has an integral solution, and let (x_1, y_1) denote the fundamental solution. For $n \geq 1$, define positive integers x_n and y_n recursively as in Theorem 25.6, i.e. $(x_n + y_n\sqrt{d}) = (x_1 + y_1\sqrt{d})_n$. Then all positive integral solutions of $x^2 - dy^2 = -1$ are given by (x_n, y_n) with n odd, and all positive integral solutions of $x^2 - dy^2 = 1$ are given by (xn, yn) with n even. In particular, (x_2, y_2) is the fundamental solution of $x^2 - dy^2 = 1$

Check Your Progress 2

3. What is Pell's Equation? Explain 'If the equation $x^2 - dy^2 = N$ has an integral solution, then it has infinitely many integral solutions.'

4. What do you understand by continued expansion fraction of $\sqrt{d}$

14.5 SUMMARY

The property characterizes the periodic simple continued fractions, that is an irrational number has a periodic continued fraction expansion if and only if it satifies a quadratic equation with integer coefficients.

14.6 KEYWORDS

1.**Sequence** : a **sequence** is an enumerated collection of objects in which repetitions are allowed.

2.**Irrational Number**. An **irrational number** is a **number** that cannot be expressed as a fraction for any integers. **Irrational numbers** have decimal expansions that neither terminate nor become periodic

3.Conjugate - A **math conjugate** is formed by changing the sign between two terms in a binomial. For instance, the **conjugate** of x + y is x - y.

4.Index - **Indices** are a **mathematical** concept for expressing very large numbers. They are also known as powers or exponents.

5. **Integral solution** : is a **solution** such that all the unknown variables take only **integer** values.

14.7 QUESTIONS FOR REVIEW

1. If x_0 , y_0 is a positive solution of the equation $x^2 – dy^2 = 1$, prove that $x_0 > y_0$.

2. By the technique of successively substituting y = 1, 2, 3, ... into dy 2 + 1, determine the smallest positive solution of $x^2 - dy^2 = 1$ when d is 7

3. Find all positive solutions of the following equations for which y < 250: $x^2 - 2y^2 = 1$.

4. If d is divisible by a prime p =3 (mod 4), show that the equation $x^2 - dy^2 = -1$ has no solution.

14.8 SUGGESTED READINGS

1.David M. Burton, Elementary Number Theory, University of New Hampshire.

2.G.H. Hardy, and , E.M. Wrigh,. An Introduction to the Theory of Numbers (6th ed, Oxford University Press, (2008).

3.W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.

4.A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.

5.I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.

6.T.M. Apostol, Introduction to Analytic number theory, UTM, Springer, (1976).

7.J. W. S Cassel, A. Frolich, Algebraic number theory, Cambridge.

8.M Ram Murty, Problems in analytic number theory, springer.

M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer

14.9 ANSWERS TO CHECK YOUR PROGRESS

1. [HINT: Provide the definition with example 14.1.3 & 14.1.16]
2. [HINT: Provide the proof of above statement 14.1.14]
3. [HINT: Provide the definition of Pell equation 14.3.1and proof of the statement14.3.5]
4. [HINT: Provide the theorem and proof of 14.3.2]