بسم الله الرحمن الرحيم

Sudan University of science and technology

Collage of sciences

Department of mathematic

A project submitted in partial fulfillment for the requirements of the degree (of bsc. (honor). In mathematic

(Number Theory)

By :

Maysaa Eltayeb Abd-elmjeed

Yusra Alzubir Mohamed Osman

Supervisor:

Dr. Balgiss Abd-alaziz

2014

قال تعالى:

بسم الله الرحمن الرحيم

﴿ربِ أوزعني أَن أشكُرَ نِعمَتَكَ التي أنعَمتَ عَليَ وَعَلي وَالِدَيَ وَأَن أَعمَلَ صالِحآ تَرضَاهُ وَأَدخِلني بِرَحمَتِكَ في عِبادِكَ الصَالِحينَ)

صدق الله العظيم

سورة النمل الآية (19)

DEDICATION

To the most wonderful parent s in the world my parents for their endless love, support and encouragement

To my brother and sisters

To my friends

I am trying to say thank you

ACKNOWLEDGMENTS

Firstly I would like to express my thanks to Allah who helped me to submit my research, thanks also extends to my supervisor, Dr. Balgiss Abd-alaziz

Countless thanks are offered to my mother, father and my friends for their help and support.

Abstract

We study the congruence moduli n, the arithmetic function and we study the basic properties of congruence , and we prove some theorems we study the Chinese remainder theorem and some of it’s application, we define the fermat number , Euler function and the relation between them we study multiplicative and we prove Euler theorem, Gauss theorem.

List of contents

CHAPTER ONE

The theory of congruence

Chapter (1)

The Theory of Congruences

In these Chapter we study the congruence moduli n, the arithmetic function , and study the basic properties of congruence , and we prove some theorems , we study the Chinese Remainder theorem and some of it's applications

Carl Friedrich Gauss:

Another approach to divisibility question is through the arithmetic of remainders, or the theory of congruences as it is now commonly known. The concept and the notation that makes it such a powerful tool, was first introduced by the German mathematician Carl Friedrich Gauss (1777-1855) in his Disquisitions Arithmetic ; this monumental work, which appeared in 1801 when Gauss was 24 years old, laid the foundations of modern number theory. Legend has a large part of the Disquisitions Arithmeticae had been submitted as memoir to the French Academy the previous year and had been rejected in a manner that, even if the work had been as worthless as the referees believed, would have been inexcusable.

Gauss was one of those remarkable infant prodigies whose natural aptitude for mathematics soon becomes apparent. As a child of age three, according to a well-authenticated story, he corrected an error in his father’s payroll calculations. His arithmetical powers so overwhelmed his

schoolmasters that, by the time Gauss was 7 years old, they admitted that there was nothing more they could teach the boy. It is said that in his first arithmetic class Gauss astonished his teacher by

instantly solving what was intended to be a "busy work" problem: Find the sum of all the numbers from 1 to 100. The young Gauss later confessed to recognized the pattern

$$1 + 100 = 101, \qquad 2 + 99 = 101, \qquad 3 + 98 = 101, \ldots, 50 + 51 = 101$$

Because there are 50 pairs of numbers, each of which adds up to 101, the sum of all the numbers be $50 \cdot 101 = 5050$. This technique provides another way of deriving the formula

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for the sum of the first n positive integers. One need only display the consecutive integers 1 through n in two rows as follows:

$$\begin{array}{cccccc} 1 & 2 & 3 & \ldots & n-1 & n \\ n & n-1 & n-2 & \ldots & 2 & 1 \end{array}$$

Addition of the vertical columns produces n terms, each of which is equal to $n + 1$: when these terms are added, we get the value $n(n + 1)$. Because the sum is obtained on adding the two rows horizontally, what occurs is the formula $n(n + 1) = 2(1 + 2 + 3 + \cdots + n)$.

Gauss went to a succession of triumphs, each new discovery following on the heels of a previous one. The problem of constructing regular polygons with only "Euclidean tools", that is to say, with ruler and compass alone, had long been laid aside in the belief that the ancients had

exhausted all the possible constructions. In 1796, Gauss showed that the 17-sides regular polygon is so constructible, the first advance in this area since Euclid's time. Gauss's doctoral thesis of 1799 provided a rigorous proof of the Fundamental Theorem of Algebra, which had been started first by Girard in 1629 and then proved imperfectly by d'Alembert (1746), and later by Euler (1749). The theorem (it asserts that a polynomial equation of degree n has exactly n complex roots) was always a favorite of Gauss's, and he gave, in all, four distinct demonstrations of it. The publication of Disquisitions Arithmetic in 1801 at once placed Gauss in the front rank of mathematicians.

The most extraordinary achievement of Gauss was more in the realm of theoretical astronomy than of mathematics. On the opening night of the 19th century, January 1, 1801, the Italian astronomer Piazzi discovered the first of the so-called miner planets (planets or asteroids), later called Ceres. But after the course of this newly found body – visible only by telescope – passed the sum, neither Piazzi nor any other astronomer could locate it again. Piazzi's observations extended over a period of 41 days, during which the orbit swept out an angle of only nine degrees. From the scanty data available, Gauss was able to calculate the orbit of Ceres with amazing accuracy, and the elusive planet was rediscovered at the end of the year in almost exactly the position he had forecasted. The success brought Gauss worldwide fame, and led to his appointment as director of Gottingen Observatory.

By the middle of the 1th century, mathematics had grown into an enormous and unwieldy structure, divided into a large number of fields in which only the specialist knew his way. Gauss was the last complete mathematician, and it is no exaggeration to say that he was in some degree

connected with nearly every aspect of the subject. His contemporaries regarded him as Princeps Mathematicorum (Prince of Mathematicians), on a par with Archimedes and Isaac Newton. This is revealed in a small incident: On being asked who was the greatest mathematician in Germany, Laplace answered, "Why Pfaff." When the questioner indicated that he would have thought Gauss was, Laplace replied, "Pfaff is by far the greatest in Germany, but Gauss is the greatest in all Europe".

Although Gauss adorned every branch of mathematics, he always held number theory in high esteem and affection. He insisted that, "Mathematics is the Queen of the Sciences, and the theory of numbers is the Queen of Mathematics".

Basic Properties of Congruence:

In the first chapter of Disquisitions Arithmeticae, Gauss introduces the concept of congruence and the notation that makes it such a powerful technique (he explains that he was induced to adopt the symbol ≡because of the close analogy with algebraic equality). According to Gauss, "if a number n measures the difference between two numbers a and b, then a and b are said to be congruent with respect to n; if not, incongruent". Putting this into the form of a definition, we have Definition (1.1).

Definition (1.1):

Let n be a fixed positive integer. Two integers a and b are said to be congruent moduli n, symbolized by

$$a \equiv b \pmod{n}$$

if n divides difference $a-b$: that is, provides that $a-b=kn$ for some integer k. To fix the idea, consider $n=7$. It is routing to check that

$$3 \equiv 4(\text{mod } 7) \qquad -31 \equiv 11(\text{mod } 7) \qquad -15 \equiv -64(\text{mod } 7)$$

because $3-24=(-3)7,\ -31-11=(-6)7,$ and $-15-(-64)=7\cdot 7.$ When $n \nmid (a-b)$, we say that a is incongruent to b moduli n, and this case we write $a \not\equiv b(\text{mod } n)$. For example: $25 \not\equiv 12\ (\text{mod } 7)$, because 7 fails to divide $25-12=13$.

It is to be noted that any two integers are congruent moduli 1, whereas two integers are congruent moduli 2 when they are both even or both odd. Inasmuch as congruence moduli 1 is not particularly interesting, the usual practices is to assume that $n>1$.

Given an integer a, let q and r be its quotient and remainder upon division by n, so that

$$a=qn+r \qquad 0 \leq r < n$$

Then by definition of congruence, $a \equiv r(\text{mod } n)$. Because there are n choices for r, we see that every integer is congruent moduli n to exactly one of the values $0,1,2,\dots,n-1$; in particular, $a \equiv 0(\text{mod } n)$ if and only if $n|a$. The set of n integers $0,1,2,\dots,n-1$ is called the set of least nonnegative residues moduli n.

In general, a collection of n integers $a_1, a_2, \dots, a_n$ is said to form a complete set of residues (or a complete system of residues) moduli n if every integers is congruent moduli n to one and only one of the a_k. To put it

another way $a_1, a_2, \dots, a_n$ are congruent moduli n to $0,1,2, \dots, n-1$, taken in some order. For instance,

$$-12, -4, 11, 13, 22, 82, 91$$

constitute a complete set of residues moduli 7; here we have

$$-12 \equiv 2 \quad -4 \equiv 3 \quad 11 \equiv 4 \quad 13 \equiv 6 \quad 22 \equiv 1 \quad 82 \equiv 5 \quad 91 \equiv 0$$

all moduli 7. An observation of some importance is that any n integers form a complete set of residues moduli n if and only if no two of the integers are congruent moduli n. We shall need this fact later.

Our first theorem provides a useful characterization of congruence moduli n in terms of remainders upon division by n.

Theorem (1.2):

For arbitrary integers a and b, $a \equiv b (\mathrm{mod}\, n)$ if and only if a and b leave the same nonnegative remainder when divided by n.

Proof:

First take $a \equiv b (mod\, n)$, so that $a = b + kn$ for some integer k. Upon division by n, b leaves a certain remainder$r$; that is, $b = qn + r$, where $0 \leq r < n$. Therefore,

$$a = b + kn = (qn + r) + kn = (q + k)n + r$$

which indicates that a has the same remainder as b.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder $r (0 \leq r < n)$. Then

$$a - b - (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$$

whence $n|a - b$. In the language of congruences, we have $a \equiv b (\mathrm{mod}\, n)$.

Congruence may be viewed as a generalized form of equality, in the sense that its behavior with respect to addition and multiplication is reminiscent of ordinary equality. Some of the elementary properties of equality that carry over to congruences appear in the next theorem.

Theorem (1.3):

Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

a) $a \equiv a \pmod{n}$.
b) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
c) If $a \equiv b \pmod{n}$ and $b \equiv c$, then $a \equiv c \pmod{n}$.
d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
e) If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$.
f) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$, for any positive integer k.

Proof:

For any integer a, we have $a - a = 0$, so that $a \equiv a \pmod{n}$. Now if $a \equiv b \pmod{n}$, then $a - b = kn$ for some integer k. Hence, $b - a = -(kn) = (-k)n$ and because $-k$ is an integer, this yields property (b).

Property (c) is slightly less obvious. Suppose that $a \equiv b \pmod{n}$ and also $b \equiv c \pmod{n}$. Then there exist integers h and k satisfying $a - b = kn$ and $b - c = kn$. It follows that

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n$$

which is $a \equiv c \pmod{n}$ in congruence notation.

In the same vein, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then we are assured that $a - b = k_1 n$ and $c - d = k_2 n$ for some choice of k_1 and k_2. Adding these equations, we obtain

$$(a + c) - (b + d) = (a - b) + (c - d)$$

$$= k_1 n + k_2 n + (k_1 + k_2)n$$

or, as congruence statement, $a + c \equiv b + d \pmod{n}$. As regards the second assertion of property (d), note that

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2)n$$

Because $bk_2 + dk_1 + k_1 k_2 n$ is an integer, this say that $ac - bd$ is divisible by n, whence $ac \equiv bd \pmod{n}$.

The proof of property (e) is covered by (d) and the fact that $c \equiv c \pmod{n}$. Finally, we obtain property (f) by making an induction argument. The statement certainly holds for $k = 1$, and we will assume it is true for some fixed k. From (d), we know that $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$ together imply that $aa^k \equiv bb^k \pmod{n}$, or equivalently $a^{k+1} \equiv b^{k+1} \pmod{n}$. This is the form the statements should take for $k + 1$, and so the induction step is complete.

Before going further, we should illustrate that congruences can be great help in carrying out certain types of computations.

In theorem (1.2) we saw that if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$ for any integer c. The converse, however, fails to hold. As an example, perhaps as simple as any note that $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, whereas $4 \not\equiv 1 \pmod{6}$. In brief: One cannot unrestrictedly cancel a common factor in the arithmetic of congruences.

With suitable precautions, cancellation can be allowed; one step in this direction, and an important one, is provided by the following theorem.

Theorem (1.4):

If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof:

By hypothesis, we can write

$$c(a - b) = ca - cb = kn$$

for some integer k. Knowing that $\gcd(c, n) = d$ there exist relatively prime integers r and s satisfying $c = dr,\ n = ds$. When these values are substituted in the displayed equation and the common factor d canceled, the net result is

$$r(a - b) = ks$$

Hence, $s | r(a - b)$ and $\gcd(r, s) = 1$. Euclid's lemma yields $s | a - b$, which may be recast as $a \equiv b \pmod{s}$; in other words, $a \equiv b \pmod{n/d}$.

Theorem (1.4) gets its maximum force when the requirement that $\gcd(c,n)=1$ is added, for then the cancellation may be accomplished without a change in modulus.

Corollary (1.5):

If $ca \equiv cb \pmod{n}$ and $\gcd(c,n)=1$, then $a \equiv b \pmod{n}$.

We take a moment to record a special case of Corollary (1.5) that we shall have frequent occasion to use, namely, Corollary (1. 6).

Corollary (1.6):

If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is a prime number, then $a \equiv b \pmod{p}$.

Proof:

The conditions $p \nmid c$ and p a prime imply that $\gcd(c,p)=1$.

Binary and Decimal Representations of Integers:

One of the more interesting applications of congruence theory involves finding special criteria under which a given integer is divisible by another integer. At their heart, these divisibility testes depend on the notational system used to assign "names" to integers and, more particularly, to the fact that 10 is taken as the base for our number system. let us, therefore, start by showing that given by an integer $b>1$, any positive integer N can be written uniquely in terms of powers of b as

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

where the coefficients a_k can take on the b different values $0, 1, 2, \ldots, b-1$. For the Division Algorithm yields integers q_1 and a_0 satisfying

$$N = q_1 b + a_0 \quad 0 \leq a_0 < b$$

If $q_1 \geq b$, we can divide once more, obtaining

$$q_1 = q_2 b + a_1 \quad 0 \leq a_1 < b$$

Now substitute for q_1 in the earlier equation to get

$$N = (q_2 b + a_1)b + a_0 = q_2 b^2 + a_1 b + a_0$$

As long as $q_2 \geq b$, we can continue in the same fashion. Going one more step: $q_2 = q_3 b + a_2$, where $0 \leq a_2 < b$, hence

$$N = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

Because $N > q_1 > q_2 > \cdots \geq 0$ is a strictly decreasing sequence of integers, this process must eventually terminate, say, at the $(n-1)$th stage, where

$$q_{m-1} = q_m b + a_{m-1} \quad 0 \leq a_{m-1} < b$$

and $0 \leq q_m < b$. Setting $a_m = q_m$, we reach the representation

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

which was our aim.

To show uniqueness, let us suppose that N has two distinct representations, say,

$$N = a_m b^m + \cdots + a_1 b + a_0 = c_m b^m + \cdots + c_1 b + c_0$$

with $0 \leq a_i < b$ for each i and $0 \leq c_j < b$ for each j (we can use the same m by simply adding terms with coefficients $a_i = 0$ or $c_j = 0$, if necessary). Subtracting the second representation from the first gives the equation

$$0 = d_m b^m + \cdots + d_1 b + d_0$$

where $d_i = a_i - c_i$ for $i = 0, 1, \ldots, m$. Because the two representations for N are assured to be different, we must have $d_i \neq 0$ for some value of i. Take k to be the smallest subscript for which $d_k \neq 0$. Then

$$0 = d_m b^m + \cdots + d_{k+1} b^{k+1} + d_k b^k$$

and so, after dividing by b^k,

$$d_k = -b(d_m b^{m-k-1} + \cdots + d_{k+1})$$

This tell us that $b | d_k$. Now the inequalities $0 \leq a_k < b$ and $0 \leq c_k < b$ lead us to $-b < a_k - c_k < b$, or $|d_k| < b$. The only way of recording the conditions $b | d_k$ and $|d_k| < b$ is to have $d_k = 0$, which is impossible. From this contradiction, we conclude that the representation of N is unique.

The essential feature in all of this is that the integer N is completely determined by the ordered array $a_m, a_{m-1}, \ldots, a_1, a_0$ of coefficients, with the plus signs and the powers of b being superfluous. Thus, the number

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_0$$

may be replaced by the simpler symbol

$$N = (a_m a_{m-1} \ldots a_2 a_1 a_0)_b$$

(the right-hand side is not to be interpreted as a product, but only as an abbreviation for N). We call this the base b place-value notation for N.

Small values of b give rise to lengthy representation of numbers, but have the advantage of requiring fewer choices for coefficients. The simplest case occurs when the base $b = 2$, and the resulting system of enumeration is called the binary number system (from the Latin binaries, two). The fact that when a number is written in the binary system only the integers 0 and 1 can appear as coefficients means that every positive integer is expressible in exactly one way as a sum of distinct powers of 2. For example, the 105 can be written as

$$105 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1$$

$$= 2^6 + 2^5 + 2^3 + 1$$

or, in abbreviated form

$$105 = (1101001)_2$$

In the other direction, $(1001111)_2$ translates into

$$1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 79$$

The binary system is most convenient for use in modern electronic computing machines, because binary numbers are represented by strings of zeros and ones; 0 and 1 can be expressed in the machine by a switch (or a similar electronic device) being either on or off.

We shall frequently wish to calculate the value of $a^k \pmod n$ when k is large. Is there a more efficient way of obtaining the least positive residue than multiplying a by itself k times before reducing moduli n? One such procedure, called the binary exponential algorithm, relies on successive squaring, with a reduction moduli n after each squaring. More specially, the

exponent k is written in binary form, as $k = (a_m a_{m-1} \dots a_2 a_1 a_0)$, and the values $a^{2^j} \pmod{n}$ are calculated for the powers of 2, which correspond to the 1's in the binary representation. These partial results are then multiplied together to give the final answer.

An illustration should make this process clear.

We ordinary record numbers in the decimal system of notation, where $b = 10$, omitting the 10-subscript that specifies the base. For instance, the symbol 1492 stands for the awkward expression

$$1 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10 + 2$$

The integers $1, 4, 9$, and 2 are called the digits of the given number, 1 being the thousands digit, 4 the hundred digit, 9 the tens digit, and 2 the units digit. In technical language we refer to the representation of the positive integers as sums of powers of 10, with coefficients at most 9, as their decimal representation (from the Latin decem, ten).

We are about ready to derive criteria for determining whether an integer is divisible by 9 or 11, without performing the actual division. For this, we need a result having to do with congruences involving polynomials with integral coefficients.

Theorem (1.7):

Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficient c_k. If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$.

Proof:

Because $a \equiv b \pmod{n}$, part (f) of theorem (1.3) can be applied to give $a^k \equiv b^k \pmod{n}$ for $k = 0, 1, \ldots, m$. Therefore,

$$c_k a^k \equiv c_k b^k \pmod{n}$$

for all such k. Adding these $m + 1$ congruences, we conclude that

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}$$

or in different notation, $P(a) \equiv P(b) \pmod{n}$.

If $P(x)$ is a polynomial with integral coefficients, we say that a is a solution of the congruence $P(x) \equiv 0 \pmod{n}$ if $P(a) \equiv 0 \pmod{n}$.

Corollary (1.8):

If a is a solution of $P(x) \equiv 0 \pmod{n}$ and $a \equiv b \pmod{n}$, then b also is a solution.

Proof:

From the last theorem, it is known that $P(a) \equiv P(b) \pmod{n}$. Hence, if a is a solution of $P(x) \equiv 0 \pmod{n}$, then $P(b) \equiv P(a) \pmod{n}$, making b a solution.

One divisibility test that we have in mind is this. A positive integer is divisible by 9 if and only if the sum of the digits in its decimal representation is divisible by 9.

Theorem (1.9):

Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $S = a_0 + a_1 + \cdots + a_m$. Then $9|N$ if and only if $9|S$.

Proof:

Consider $P(x) = \sum_{k=0}^{m} a_k x^k$, a polynomial with integral coefficients. The key observation is that $10 \equiv 1 \pmod 9$, whence by theorem (1.7), $P(10) \equiv P(1) \pmod 9$. But $P(10) = N$ and $P(1) = a_0 + a_1 + \cdots + a_m = S$, so that $N = S \pmod 9$. It follows that $N \equiv 0 \pmod 9$ if and only if $S \equiv 0 \pmod 9$, which is what we wanted to prove.

Theorem (1.7) also serves as the basis for a well-known test for divisibility by 1: an integer is divisible by 11 if and only if the altering sum of its digits is divisible by 11. We state this more precisely by theorem (1.10).

Theorem (1.10):

Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11|N$ if and only if $11|T$.

Proof:

As in the proof of theorem (1.9), put $P(x) = \sum_{k=0}^{m} a_k x^k$. Because $10 \equiv -1 \pmod{11}$, we get $P(10) \equiv P(-1) \pmod{11}$. But $P(10) = N$, whereas $P(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m = T$, so that $N = T \pmod{11}$. The implication is that either both N and T are divisible by 11 or neither is divisible by 11.

Congruence theory is frequently used to append an extra check digit to identification numbers, in order to recognize transmission errors or forgeries. Personal identification numbers of some kind appear on passports, credit cards, bank accounts, and a variety of other settings.

Some banks use an eight-digit identification number $a_1 a_2 \ldots a_8$ together with a final check digit a_9. The check digit is usually obtained by multiplying the digits $a_i (1 \leq i \leq 8)$ by certain "weights" and calculating the sum of the weighted products moduli 10. For instance, the check digit might be chosen to satisfy

$$a_9 \equiv 7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 \pmod{10}$$

The identification number 81504216 would then have check digit

$$\begin{aligned} a_9 &\equiv 7 \cdot 8 + 3 \cdot 1 + 9 \cdot 5 + 7 \cdot 0 + 3 \cdot 4 + 9 \cdot 2 + 7 \cdot 1 + 3 \cdot 6 \\ &\equiv 9 \pmod{10} \end{aligned}$$

so that 815042169 would be printed on the check.

This weighted scheme for assigning check digits detects any single-digit error in the identification number. For suppose that the digit a_i is replaced by a different a_i'. By the manner in which the check digit is calculated, the difference between the correct a_9 and the new a_9' is

$$a_9 - a_9' \equiv k(a_i - a_i') \pmod{10}$$

where k is 7, 3, or 9 depending to the position of a_i'. Because $k(a_i - a_i') \not\equiv 0\ (mod\ 10)$, it follows that $a_9 \neq a_9'$ and the error is apparent. Thus, it is the valid number 81504216 were incorrectly entered as 81504316 into a computer programmed to calculate check digits, an 8 would come up rather than the expected 9.

The moduli 10 approach is not entirely effective, for it does not always detect the common error of transporting distinct adjacent entries a and b within the string of digits. To illustrate the identification numbers 81504216 and 80504261 have the same check digit 9 when our example weights are used: (The problem occurs when $|a - b| = 5$). More sophisticated methods are available, with larger moduli and different weights, that would prevent this possible error.

Linear Congruences and the Chinese Remainder Theorem:

This is a convenient in our development of number theory at which to investigate the theory of linear congruences: An equation of the form $ax \equiv b \pmod{n}$ is called a linear congruence, and by a solution of such an equation we mean an integer x_0 for which $ax_0 \equiv b \pmod{n}$. By definition, $ax_0 \equiv b \pmod{n}$ if and only if $n|ax_0 - b$ or, what amounts to the same thing, if and only if $ax_0 - b = ny_0$ for some integer y_0. Thus, the problem of finding all integers that will satisfy the linear congruence $ax \equiv b \pmod{n}$ is identical with that for obtaining all solutions of the linear Diophantine equation $ax - ny = b$.

It is convenient to treat two solutions of $ax \equiv b \pmod{n}$ that are congruent moduli n as being "equal" even though they are not equal in the usual sense. For instance, $x = 3$ and $x = -9$ both satisfy the congruence $3x \equiv 9 \pmod{12}$; because $3 \equiv -9 \pmod{12}$, they are not counted as different solutions. In short: When we refer to the number of solutions of $ax \equiv b \pmod{n}$, we mean the number of incongruent integers satisfying this congruence.

With these remarks in mind, the principal result is easy to state.

Theorem (1.11):

The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$, where $d = \gcd(a, n)$. If $d|b$, then it has d mutually incongruent solutions moduli n.

Proof:

We already have observed that the given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. It is known that the latter equation can be solved if and only if $d|b$; moreover, if it is solvable and x_0, y_0 is one specific solution, then any other solution has the form

$$x = x_0 + \frac{n}{d}t \quad y = y_0 + \frac{a}{d}t$$

For some choice of t.

Among the various integers satisfying the first of these formulas, consider those that occur when t takes on the successive values $t = 0, 1, 2, \ldots, d - 1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

We claim that these integers are incongruent moduli n and all other such integers x are congruent to some one of them. If it happened that

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}$$

where $0 \leq t_1 < t_2 \leq d-1$, then we would have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}$$

Now $\gcd(n/d, n) = n/d$, and therefore by theorem (1.4) the factor n/d could be canceled to arrive at the congruence

$$t_1 \equiv t_2 \pmod{n}$$

which is to say that $d|t_2 - t_1$. But this is impossible in view of the equality $0 < t_2 - t_1 < d$.

It remains to argue that any other solution $x_0 + (n/d)$ is congruent moduli n to one of the d integers listed above. The Division Algorithm permits us to write t as $t = qd + r$, where $0 \leq r \leq d-1$. Hence

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r)$$

$$= x_0 + nq + \frac{n}{d}r$$

$$\equiv x_0 + \frac{n}{d}r \pmod{n}$$

With $x_0 + (n/d)r$ being one of our d selected solutions. This ends the proof.

The argument that we gave in theorem (1.11) brings out a point worth stating explicitly: If x_0 is any solution of $ax \equiv b \pmod{n}$, then the $d = \gcd(a, n)$ incongruent solutions are given by

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\left(\frac{n}{d}\right), \dots, x_0 + (d-1)\left(\frac{n}{d}\right)$$

For the reader's convenience, let us also record the form theorem (1.11) takes in the special case in which a and n are assumed to be relatively prime.

Corollary (1.12):

if $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has a unique solution moduli n.

Given relatively prime integers a and n, the congruence $ax \equiv 1 \pmod{n}$ has a unique solution. This solution is sometimes called the (multiplicative) inverse of aa moduli n.

Having considered a single linear congruence, it is natural to turn to the problem of solving a system of simultaneous linear congruences:

$$a_1 x \equiv b_1 \pmod{m_1}\ a_2 \equiv b_2 \pmod{m_2}, \dots, a_r x \equiv b_r \pmod{m_r}$$

We shall assume that the moduli m_k are relatively prime in pairs. Evidently, the system will admit no solution unless each individual congruence is solvable; that is, unless $d_k | b_k$ for each k, where $d_k = \gcd(a_k, m_k)$. When these conditions are satisfied, the factor d_k can be

canceled in the kth congruence to produce a new system having the same set of solution as the original one:

$$a_1' \equiv b_1' \pmod{n_1}, a_2'x \equiv b_2' \pmod{n_2}, \dots, a_r'x \equiv b_r' \pmod{n_r}$$

where $n_k = m_k/d_k$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$; in addition, $\gcd(a_i', n_i) = 1$. The solution of the individual congruences assume the form

$$x \equiv c_1 \pmod{n_1}, x \equiv c_2 \pmod{n_2}, \dots, x \equiv c_r \pmod{n_r}$$

Thus, the problem is reduces to one of finding a simultaneous solution of a system of congruences of this simpler type.

The kind of problem that can be solved by simultaneous congruence has a long history, appearing in the Chinese literature as early as the 1st century A.D. Sun-Tsu asked : Find a number that leaves the remainders 2, 3, 2 when divided by 3, 5, 7, respectively. (Such mathematical puzzles are by no means confined to a single cultural sphere, indeed, the same problem occurs in the Introduction Arthemeticae of the Greek mathematician Nicomachus, circa 100 A.D.). In honor of their early contribution, the rule for obtaining a solution usually goes by the name of the Chinese Remainder Theorem.

Theorem (1.13): Chinese Remainder Theorem

Let $n_1, n_2, \dots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

has a simultaneous solution, which is unique moduli the integer $n_1 n_2 \ldots n_r$.

Proof:

We start by forming the product $n = n_1 n_2 \ldots n_r$. For each $k = 1,2, \ldots, r$ let

$$N_k = \frac{n}{n_k} = n_1 \ldots n_{k-1} n_{k+1} \ldots n_r$$

In words, N_k is the product of all the integers n_i with the factor omitted. By hypothesis, the n_i are relatively prime in pairs, so that $\gcd(N_k, n_k) = 1$. According to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 \pmod{n_k}$; call the unique solution x_k. Our aim is to prove that the integer

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

is a simultaneous solution of the given system.

first, observe that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, because $n_k | N_i$ in this case. The result is

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 \pmod{n_k}$, which forces

$$\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}$$

This shows that a solution to the given congruences exists.

As for the uniqueness assertion, suppose that x' is any other integer that satisfies these congruences. Then

$$\bar{x} \equiv a_k \equiv x' (\text{mod } n_k) \quad k = 1, 2, , \dots, r$$

and so n_k|x-x' for each value of k. Because $\gcd(n_i, n_j) = 1$. Corollary (1. 6) supplies us with the crucial point that $n_1 n_2 \dots n_r | \bar{x} - x'$; hence $\bar{x} \equiv x' (\text{mod } n)$. With this, the Chinese Remainder Theorem is proven.

In analogy with theorem (1.11), such a congruence has a solution if and only if $\gcd(a, b, n)$ divides c. The condition for solvability holds if either $\gcd(a, n) = 1$ or $\gcd(b, n) = 1$. Say $\gcd(a, n) = 1$. When the congruence is expressed as

$$ax \equiv c - by \ (\text{mod } n)$$

the corollary to theorem (1.11) guarantees a unique solution x for each of the n incongruent values of y. Take as a simple illustration $7x + 4y \equiv 5 \ (\text{mod } 12)$, that would be treated as $7x \equiv 5 - 4y \ (\text{mod } 12)$. Substitution of $y \equiv 5 \ (\text{mod } 12)$ gives $7x \equiv -15 \ (\text{mod } 12)$; but is equivalent to $-5x \equiv -15 \ (\text{mod } 12)$ so that $x \equiv 3 \ (\text{mod } 12)$. It follows that $x \equiv 3 \ (\text{mod } 12)$, $y \equiv 5 \ (\text{mod } 12)$ is one of the 12 incongruent solutions of $7x + 4y \equiv 5 \ (\text{mod } 12)$. Another solution having the same value of x is $x \equiv 3 (\text{mod } 12), y \equiv 8 \ (\text{mod } 12)$.

The focus of our concern here is how to solve a system of two linear congruences, in two variables with the same modulus. The proof of the

coming theorem adopts the familiar procedure of eliminating one of the unknowns.

Theorem (1.14):

The system of linear congruences

$$ax + by \equiv r \pmod{n}$$

$$cx + dy \equiv s \pmod{n}$$

has a unique solution moduli n whenever $\gcd(ad - bc, n) = 1$.

Proof:

Let us multiply the first congruence of the system by d in the second congruence by b, and subtracting the lower result from the upper. These calculations yield

$$(ad - bc)x \equiv dr - bs \pmod{n} \qquad (1)$$

The assumption $\gcd(ad - bc, n) = 1$ensures that the congruence

$$(ad - bc)z \equiv 1 \pmod{n}$$

possesses a unique solution; denote the solution by: When congruence (1) is multiplied by t, we obtain

$$x \equiv t(dr - bs) \pmod{n}$$

A value for y is found by a similar eliminate process. That is, multiply the first congruence of the system by c, the second one by a, and subtract to end up with

$$(ad - bc)y \equiv y\ as - cr\ \equiv (\mathrm{mod}\ n) \qquad (2)$$

Multiplication of this congruence by t leads to

$$y \equiv t(as - cr)\ (\mathrm{mod}\ n)$$

A solution of the system is now established.

CHAPTER TWO

Euler's Generalization of Fermat's Theorem

Chapter (two)

Euler's function and Fermat's Theorem

In this chapter we define the Fermat number Euler function and the Relation between them , we study the multiplicative and prove some theorem ,we prove Euler theorem , Gauss theorem .

Euler's Generalization of Fermat's Theorem

The importance of Fermat work resides not so much in any contribution to the mathematics of this own day, but rather in its animating effect on later generations of mathematicians. Perhaps the greatest disappointment of Fermat's career was his inability to interest others in his new number theory. A century was to pass before a first-class mathematician, Leonhard-Euler (1707-1783), either understood or appreciated its significance. Many of the theorems announced without proof by Fermat yielded to Euler's skill, and it is likely that the arguments devised by Euler were not substantially different from those that Fermat said he possessed.

The key figure in 18th century mathematics, Euler was the son of a Lutheran pastor who lived in the vicinity of Basel, Switzerland. Euler's father earnestly wished him to enter the ministry and sent his son, at the age of 13, to the University of Basel to study theology.

Where the 17th century had been an age of great amateur mathematicians, the 18th century was almost exclusively an era of professionals- university professors and members of scientific academies. Many of the reigning monarchs delighted in regarding themselves as patrons of learning, and the academies served

as the intellectual crown jewels of the royal courts. Although the motives of these rulers may not have been entirely philanthropic, the fact remains that the learned societies constituted agencies for the promotion of science. They provided salaries for distinguished scholars, published journals of research papers on a regular basis, and offered monetary prizes for scientific discoveries. Euler was at different times associated with two of the newly formed academies, the Imperial Academy at St. Petersburg (1727-1741; 1766-1783) and the Royal Academy in Berlin (1741-1766). In 1725, Pater the Great founded the Academy of St. Petersburg and attracted a number of leading mathematicians to Russia, including Nicolaus and Daniel Bernoulli. On their recommendation, an appointment was secured of Euler. Because of his youth, he had recently been denied a professorship in physics at the University of Basel and was only too accept the invitation of the Academy. In St. Petersburg, he soon came into contact with the versatile scholar Christian Goldbach (of the famous conjecture), a man who subsequently rose from professor of mathematics to Russian Minister of Foreign Affairs. Given his interests, it seems likely that Goldbach was the one who first drew Euler's attention to the work of Fermat on theory of numbers.

Euler eventually tried of the political repression in Russia and accepted the call of Frederick the Great to become a member of the Berlin

Academy. The story is told that, during a reception at Court, he was kindly received by the Queen Mother who inquired why so distinguished a scholar be so timid and reticent; he replied, "Madame, it is because I have just come from a country where, when one speaks, one is hanged." However, flattered by the warmth of the Russian feeling toward him and unendurably offended by the contrasting coolness of Frederick his court, and unendurably offended by the contrasting of Frederick and his court, Euler returned to St. Petersburg in 1766 to spend his remaining days. Within two or three years of his return, Euler became totally blind.

However, Euler did permit blindness to retard his scientific work; aided by a phenomenal memory his writings grew to such enormous proportions as to be virtually unmanageable. Without a doubt, Euler was the most prolific written in the entire history of mathematics. He wrote or dictated over 700 books and papers in his lifetime, and left so much unpublished material that the St. Petersburg Academy did not finish printing all his manuscripts unit 47 years after his death. The publication of Euler's collected works was begun by the Swiss Society of Natural Sciences in 1911 and it is estimated that more than 75 large volumes will ultimately be required for the completion of his monumental project. The best testament to the quality of these papers may be the fact on 12 occasions they won the coveted biennial prize of the French Academy in Paris.

During his stay in Berlin, Euler acquired the habit of writing memoir after memoir, placing each when finished at the top of a manuscripts. Whenever material was needed to fill the Academy's journal, the printers helped themselves to a few papers from the top of the stack. As the height of the pile increased more rapidly than the demands made upon it, memoirs at

the bottom tended to remain in place a long time. This explains how it happened that various papers of Euler were published, when extensions and improvements of the material in them had previously appeared in print under his name. we might also add that the manner in which Euler made his work public contrasts sharply with the secrecy customary in Fermat's time.

This chapter deals with that part of the theory arising out of the result known a Euler's Generalization of Fermat's Theorem. In a nutshell, Euler extended Fermat's theorem, which concerns congruences with prime moduli, to arbitrary moduli . while doing so, he introduced an important number-theoretic, described in Definition (2.1).

Definition (2.1):

For $n \geq 1$, let $\emptyset(n)$ denoted the number of the number of positive integers not exceeding n that relatively prime to n.

As an illustration of the definition, we find that $\emptyset(30) = 8$; for, among the positive integers that do not exceed 30, specifically,

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

Similarly, for the first few positive integers, the reader may check that

$$\emptyset(1) = 1, \emptyset(2) = 1, \emptyset(3) = 2, \emptyset(4) = 2, \emptyset(5) = 4, \emptyset(6) = 2, \emptyset(7) = 6, \ldots$$

Notice that $\emptyset(1) = 1$, because $\gcd(1.1) = 1$. In the even $n > 1$, then $\gcd(n.n) = n \neq 1$, so that $\emptyset(n)$ can be characterized as the number of integers less than n and relatively prime to it. The function $\emptyset$ is usually called the Euler phi function (sometimes, the indicator or totient) after its originator, the functional notation $\emptyset(n)$, however is credited to Gauss.

If n is a prime number, then every integer less than n is relatively prime to it; whence, $\emptyset(n) = n - 1$. One the other hand, if $n > 1$ is composite, then n has a divisor d such that $1 < d < n$. It follows that there are at least two integers among $1,2,3, \dots, n$ that are not relatively prime to n, namely, d and n itself. As a result, $\emptyset(n) \leq n - 2$. This proves that for $n > 1$,

$$\emptyset(n) = n - 1 \quad \text{if and ony if } n \text{ is prime}$$

The first item on the agenda is to derive a formula that will allow us to calculate the value of $\emptyset(n)$ directly from the prime-power factorization of n. A large step in this direction stems from Theorem (2.2).

Theorem (2.2):

If p is a prime and $k > 0$, then

$$\emptyset(P^k) = P^k - P^{k-1} = P^k\left(1 - \frac{1}{P}\right)$$

Proof:

Clearly, $\gcd(n, P^k) = 1$ if and only if $P \nmid n$. there are P^{k-1} integers between 1 and P^k divisible by P, namely,

$$P, 2P, 3P, \dots, (P^{k-1})P$$

Thus, the set $\{1,2, \dots, P^k\}$ contains exactly $P^k - P^{k-1}$ integers that are relatively prime to P^k, and so by the definition of the phi-function, $\emptyset(P^k) = P^k - P^{k-1}$.

For an example, we have

$$\emptyset(9) = \emptyset(3^2) = 3^2 - 3 = 6$$

the six integers less than and relatively prime to 9 being 1,2,4,5,7,8. To give a second illustration, there are 8 integers that are less than 16 and relatively prime to it; they are 1,3,5,7,9,11,13,15. Theorem (2. 2) yields the same count:

$$\emptyset(16) = \emptyset(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$

We now know how to evaluate the phi-function for prime powers, and our aim is not obtain a formula for $\emptyset(n)$ based on the factorization of n as a product of primes. The missing link in the chain is obvious: Show that $\emptyset$ is a multiplicative function. We pave the way with an easy lemma.

Lemma (2.3):

Give 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 pur $d = \gcd(a, b)$. Then $d\backslash a$ and $d\backslash b$, whence $d\backslash a$ and $d\backslash bc$. This implies that $\gcd(a, bc) \geq d$, 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 $d_1\backslash bc$, it follows that $P\backslash bc$; in consequence, $P\backslash b$ or $P\backslash c$. If $P\backslash b$, then (by virtue of the fact $P\backslash a$) we have $\gcd(a, b) \geq P, a$ contradiction. In the same way, the condition $P\backslash c$ leads to the equally false conclusion that $\gcd(a, c) \geq P$. Thus, $d_1 = 1$ and the lemma is proven.

Theorem (2.4):

The function $\emptyset$ is a multiplicative function.

Proof:

It is required to show that $\emptyset(mn) = \emptyset(m)\emptyset(n)$, wherever m and n have no common factor. Because $\emptyset(1) = 1$, the result obviously holds if either m or n equals 1. Thus, we may assume that $m > 1$ and $n > 1$. Arrange the integers from 1 to mn in m columns of n integers each, as follows:

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

We know that $\emptyset(mn)$ is equal to the number of entries in this array that are relatively prime to mn; by virtue of the lemma, this is the same as the number of integers that are relatively prime to both m and n.

Before embarking on the details, it worth commenting on the tactics to be adopted: Because $\gcd(qm + r, m) = \gcd(r, m)$, the numbers in the rth column are relatively prime to m if and only if r itself is relatively prime to m. Therefore, only $\emptyset(m)$ columns contain integers relatively prime to m, and every entry in the column will be relatively prime to m. The problem is one of showing that in each of these $\emptyset(m)$ columns there are exactly $\emptyset(n)$ integers that are relatively prime to n; for then altogether there would be $\emptyset(m)\emptyset(n)$ numbers in the table that are relatively prime to both m and n.

Now the entries in the rth column (where it is assumed that $\gcd(r, m) = 1$) are

$$r, m + 2m + r, \dots, (n-1)m + r$$

There are n integers in this sequence and no two are congruent moduli n. indeed, if

$$km + r \equiv jm + r (\mathrm{mod}\, n)$$

with $0 \leq k < j < n$, it would follow that $km \equiv jm (\mathrm{mod}\, n)$. Because $\gcd(m, n) = 1$, we would cancel m from both sides of this congruence to arrive at contradiction that $k \equiv j (\mathrm{mod}\, n)$. Thus, the numbers in the rth column are congruent moduli n to $0,1,2, \dots, n-1$, in some order. But if $s \equiv t (\mathrm{mod}\, n)$, then $\gcd(s, n) = 1$ if and only if $\gcd(t, n) = 1$. The implication is that the rth column contains as many integers that are relatively prime to n as does the set $\{0,1,2, \dots, n-1\}$, namely, $\emptyset(n)$ integers. Therefore, the total number of entries in the array that relatively prime to both m and n is $\emptyset(m)\emptyset(n)$. This completes the proof of the theorem.

With these preliminaries in hand, we now can prove Theorem (2. 5).

Theorem (2.5):

If the integer $n > 1$ has the prime factorization $n = P_1^{k_1} P_2^{k_2} \dots P_r^{k_r}$, then

$$\emptyset(n) = \left(P_1^{k_1} - P_1^{k_1 - 1}\right)\left(P_2^{k_2} - P_2^{k_2 - 1}\right) \dots \left(P_r^{k_r} - P_r^{k_r - 1}\right)$$

$$= n\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\ldots\left(1-\frac{1}{P_r}\right)$$

Proof:

We intend to use induction on r, the number of distinct prime factors of n. By Theorem (2.2), the result is true for $r = 1$. Suppose that it holds for $r = i$. because

$$\gcd\left(P_1^{k_1}P_2^{k_2}\ldots P_i^{k_i}, P_{i+1}^{k_{i+1}}\right) = 1$$

the definition of multiplicative function gives

$$\emptyset\left(\left(P_1^{k_1}\ldots P_i^{k_i}\right)P_{i+1}^{k_{i+1}}\right) = \emptyset\left(P_1^{k_1}\ldots P_i^{k_i}\right)\emptyset\left(P_{i+1}^{k_{i+1}}\right)$$

$$= \emptyset\left(P_1^{k_1}\ldots P_i^{k_i}\right)\left(P_{i+1}^{k_{i+1}} - P_{i+1}^{k_{i+1}-1}\right)$$

Invoking the induction assumption, the first factor on the right-hand side becomes

$$\emptyset\left(P_1^{k_1}P_2^{k_2}\ldots P_i^{k_i}\right) = \left(P_1^{k_1} - P_1^{k_1-1}\right)\left(P_2^{k_2} - P_2^{k_2-1}\right)\ldots\left(P_i^{k_i} - P_i^{k_i-1}\right)$$

and this serves to complete the induction step, and the proof.

Theorem (2.6):

For $n > 2, \emptyset(n)$ is an even integer.

Proof:

First, assume that n is a power of 2, let us say that $n = 2^k$, with $k \geq 2$. By Theorem (2. 5),

$$\emptyset(n) = \emptyset(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1}$$

an even integer. If n does not happen to be a power of 2, then it is divisible by an odd prime P; we therefore may write n as $n = P^k m$, where $k \geq 1$ and $\gcd(P^k, m) = 1$. Exploiting the multiplication nature of the phi-function, we obtain

$$\emptyset(n) = \emptyset(P^k)\emptyset(m) = P^{k-1}(P-1)\emptyset(m)$$

which again is even because $2 \backslash P - 1$.

We can establish Euclid's theorem on the finitude of prime in the following new way. As before, assume that there are only a finite number of primes. Call them $P_1, P_2, \ldots, P_r$ and consider the integer $n = P_1 P_2 \ldots P_r$. We argue that if $1 < a \leq n$, then $\gcd(a, n) \neq 1$. For the Fundamental Theorem of Arithmetic tell us that a has a prime divisor q. Because $P_1, P_2, \ldots, P_r$ are the only primes, q must be one of these P_i, whence $q \backslash n$; in other words, $\gcd(a, n) \geq q$. The implication of all this is that $\emptyset(n) = 1$, which clearly is impossible by Theorem (2. 6).

As remarked earlier, the first published proof of Fermat's theorem (namely that $a^{P-1} \equiv 1 (\text{mod } P)$ if $P \nmid a$) was given by Euler in 1736. Somewhat later, in 1760, he succeeded in generalizing Fermat's theorem from the case of a prime P to an arbitrary positive integer n. This landmark result states: If $\gcd(a, n) = 1$, then $a^{\emptyset(n)} \equiv 1 (\text{mod } n)$.

For example, putting $n = 30$ and $a = 11$, we have

$$11^{\emptyset(30)} \equiv 11^8 \equiv (11^2)^4 \equiv (121)^4 \equiv 1^4 \equiv 1 (\text{mod } 30)$$

As a prelude to launching our proof of Euler's generalization of Fermat's theorem, we require a preliminary lemma.

Lemma (2.7):

Let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \dots, a_{\emptyset(n)}$ are the positive integers less than n and relatively prime to n, then

$$aa_1, aa_2, \dots, aa_{\emptyset(n)}$$

are congruent moduli n to $a_1, a_2, \dots, a_{\emptyset(n)}$ n some order.

Proof:

Observe that no two of the integers $aa_1, aa_2, \dots, aa_{\emptyset(n)}$ are congruent moduli n. For if $aa_i \equiv aa_j (\mathrm{mod}\, n)$, with $1 \leq i < j \leq \emptyset(n)$, then the cancellation law yields $a_i \equiv a_j (\mathrm{mod}\, n)$, and thus $a_i = a_j$, a contradiction. Furthermore, because $\gcd(a_j, n) = 1$ for all i and $\gcd(a, n) = 1$, the lemma preceding Theorem (2. 4) guarantees that each of the aa_i is relatively prime to n.

Fixing on a particular aa_i, there exists a unique integer b, where $0 \leq b < n$, for which $aa_i \equiv b (\mathrm{mod}\, n)$. Because

$$\gcd(b, n) = \gcd(aa_i, n) = 1$$

b must be one of the integers $a_1, a_2, \dots, a_{\emptyset(n)}$. All told, this proves that the numbers $aa_1, aa_2, \dots, aa_{\emptyset(n)}$ and the numbers $a_1, a_2, \dots, a_{\emptyset(n)}$ are identical (moduli n) in a certain order.

Theorem (2.8): Euler Theorem

If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\emptyset(n)} \equiv 1 (\text{mod } n)$.

Proof:

There is no harm in taking $n > 1$. Let $a_1, a_2, \ldots, a_{\emptyset(n)}$ be the positive integers less than n that are relatively prime to n. Because $\gcd(a, n) = 1$, it follows from the lemma that $aa_1, aa_2, \ldots, aa_{\emptyset(n)}$ are congruent, not necessarily in order of appearance, to $a_1, a_2, \ldots, a_{\emptyset(n)}$. Then

$$\begin{aligned} aa_1 &\equiv a_1' (\text{mod } n) \\ aa_2 &\equiv a_2' (\text{mod } n) \\ \vdots \qquad & \qquad \vdots \\ aa_{\emptyset(n)} &\equiv a_{\emptyset(n)}' (\text{mod } n) \end{aligned}$$

where $a_1', a_2', \ldots, a_{\emptyset(n)}'$ are the integers $a_1; a_2, \ldots, a_{\emptyset(n)}$ in some order. On taking the product of these $\emptyset(n)$ congruences, we get

$$\begin{aligned} (aa_1)(aa_2) \ldots \left(aa_{\emptyset(n)}\right) &\equiv a_1' a_2' \ldots a_{\emptyset(n)}' (\text{mod } n) \\ &\equiv a_1 a_2 \ldots a_{\emptyset(n)} (\text{mod } n) \end{aligned}$$

and so

$$a^{\emptyset(n)}\left(a_1 a_2 \ldots a_{\emptyset(n)}\right) \equiv a_1 a_2 \ldots a_{\emptyset(n)} \ (\text{mod } n)$$

Because $\gcd(a_i, n) = 1$ for each i, the lemma preceding Theorem (2. 4) implies that $\gcd\left(a_1 a_2 \ldots a_{\emptyset(n)}\right) = 1$. Therefore, we may divide both sides of the foregoing congruence by the common factor $a_1 a_2 \ldots a_{\emptyset(n)}$, leaving us with

$$a^{\emptyset(n)} \equiv 1 (\text{mod } n)$$

This proof can best be illustrated by carrying it out with some specific numbers. Let $n = 9$, for instance. The positive integers less than and relatively prime to 9 are

$$1,2,4,5,7,8$$

These play the role of the integers $a_1, a_2, \ldots, a_{\emptyset(n)}$ in the proof of Theorem (2. 8). If $a = -4$, then the integers aa_i are

$$-4, -8, -16, -20, -28, -32$$

where, moduli 9,

$$-4 \equiv 5 \quad -8 \equiv 1 \quad -16 \equiv 2 \quad -20 \equiv 7 \quad -28 \equiv 8 \quad -32 \equiv 4$$

When the above congruences are all multiplied together, we obtain

$$(-4)(-8)(-16)(-20)(-28)(-32) \equiv 5 \cdot 1 \cdot 2 \cdot 7 \cdot 8 \cdot 4 \pmod 9$$

which becomes

$$(1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8)(-4)^6 \equiv (1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8) \pmod 9$$

Being relatively prime to 9, the six integers 1,2,4,5,7,8 may be canceled successively to give

$$(-4)^6 \equiv 1 \pmod 9$$

The validity of this last congruence is confirmed by the calculation

$$(-4)^6 \equiv 4^6 \equiv (64)^2 \equiv 1^2 \equiv 1 \pmod 9$$

Note that Theorem (2.1.8) does indeed generalize the one credited to Fermat, which we proved earlier. For if P is a prime, then $\emptyset(P) = p - 1$; hence, when $\gcd(a, p) = 1$, we get

$$a^{P-1} \equiv a^{\emptyset(P)} \equiv 1 (\text{mod } P)$$

and so we have the following corollary.

Corollary (2. 9): Fermat Theorem

If P is a prime and $P \nmid a$, then $a^{P-1} \equiv 1 (\text{mod } P)$.

There is another path to Euler's theorem, one which requires the use of Fermat's theorem.

Second proof of Euler's Theorem:

To start, we argue by induction that if $P \nmid a$ (P a prime), then

$$a^{\emptyset(P^k)} \equiv 1 (\text{mod } P^k) \quad k > 0 \qquad (1)$$

When $k = 1$, this assertion reduces to the statement of Fermat's theorem. Assuming the truth of Equation (1) for a fixed value of k, we wish to show that it is true with k replaced by $k + 1$.

Because Equation (1) is assumed to hold, we may write

$$\emptyset(P^{k+1}) = P^{k+1} - P^k = P(P^k - P^{k-1}) = P\emptyset(P^k)$$

Using these fact, along with the binomial theorem, we obtain

$$a^{\emptyset(P^{k+1})} = a^{P\emptyset(P^k)}$$

$$= \left(a^{\emptyset(P^k)}\right)^P$$

$$= (1 + qP^k)^P$$

$$= 1 + \binom{P}{1}(qP^k) + \binom{P}{2}(qP^k)^2 + \cdots + \binom{P}{P-1}(qP^k)^{P-1} + (qP^k)^P$$

$$\equiv 1 + \binom{P}{1}(qP^k) (\text{mod } P^{k+1})$$

But $P|\binom{P}{1}$, and so $P^{k+1}|\binom{P}{1}(qP^k)$. Thus, the last-written congruence becomes

$$a^{\emptyset(P^{k+1})} \equiv 1 (\text{mod } P^{k+1})$$

completing the induction sep.

Let $\gcd(a, n) = 1$ and n have the prime-power factorization $n = P_1^{k_1} P_2^{k_2} \ldots P_r^{k_r}$. In view of what already has been proven, each of the congruences

$$a^{\emptyset\left(P_i^{k_i}\right)} \equiv 1\left(\text{mod } P_i^{k_i}\right) \quad i = 1,2, \ldots, r \qquad (2)$$

holds. Noting that $\emptyset(n)$is divisible by $\emptyset\left(P_i^{k_i}\right)$, we may raise both side of Equation (2) to the power $\emptyset(n)/\emptyset\left(P_i^{k_i}\right)$ and arrive at

$$a^{\emptyset(n)} \equiv 1\left(\text{mod } P_i^{k_i}\right) \quad i = 1,2, \ldots, r$$

Inasmuch as the moduli are relatively prime, this us leads us to the relation

$$a^{\emptyset(n)} \equiv 1\left(\text{mod } P_1^{k_1} P_2^{k_2} \ldots P_r^{k_r}\right)$$

or $a^{\emptyset(n)} \equiv 1(\text{mod } n)$.

The usefulness of Euler's theorem in number theory would hard to exaggerate. It leads, for instance, to a different proof of the Chinese Remainder Theorem. In other words, we seek to establish that if $\gcd(n_i, n_j) = 1$ for $i \neq j$, then the system of linear congruences

$$x \equiv a_i (\text{mod } n_i) \quad i = 1,2, \dots, r$$

admits a simultaneous solution. Let $n = n_1 n_2 \dots n_r$, and put $N_i = n/n_i$ for $n = 1,2, \dots, r$. Then the integer

$$x = a_1 N_1^{\emptyset(n_1)} + a_2 N_2^{\emptyset(n_2)} + \cdots + a_r N_r^{\emptyset(n_r)}$$

fulfills our requirements. To see this, first note that $N_j \equiv 0 (\text{mod } n_i)$ whenever $i \neq j$; whence,

$$x \equiv a_i N_i^{\emptyset(n_i)} (\text{mod } n_i)$$

But because $\gcd(N_i, n_i) = 1$, we have

$$N_i^{\emptyset(n_i)} \equiv 1 (\text{mod } n_i)$$

and so $x \equiv a_i (\text{mod } n_i)$ for each i.

As a second application of Euler's theorem, let us show that if n is an odd integer that is not a multiple of 5, then n divides an integer all of whose digits are equal to 1 (for example, 7|111111). Because $\gcd(n, 10) = 1$ and $\gcd(9,10) = 1$, we have $\gcd(9n, 10) = 1$. Quoting Theorem (2. 8), again,

$$10^{\emptyset(9n)} \equiv 1 (\text{mod } 9n)$$

This says that $10^{\emptyset(9n)} - 1 = 9nk$ for some integer k or, what amounts to the same thing,

$$kn = \frac{10^{\emptyset(9n)} - 1}{9}$$

The right-hand side of this expression is an integer whose digits are all equal to 1, each digit of the numerator being clearly equal to 9.

The next theorem points out a curious feature of the phi-function; namely, that the sum of the values of $\emptyset(d)$, as d ranges over the positive divisors of n, is equal to n itself. This was first noticed by Gauss.

Theorem (2. 10): Gauss Theorem

For each positive integer $n \geq 1$,

$$n = \sum_{d|n} \emptyset(d)$$

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 S_d provided that $\gcd(m, n) = d$. Stated in symbols,

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

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 $\emptyset(n/d)$. Because each of the n integers in the set $\{1,2, \ldots, n\}$ lies in exactly one class S_d, we obtain the formula

$$n = \sum_{d|n} \emptyset\left(\frac{n}{d}\right).$$

But as d runs through all positive divisor of n, so does n/d; hence,

$$\sum_{d|n} \emptyset\left(\frac{n}{d}\right) = \sum_{d|n} \emptyset(d)$$

which proves the theorem.

It is instructive to give a second proof of theorem (2. 10), this one depending on the fact that $\emptyset$ is multiplicative. The details are as follows. If $n = 1$, then clearly

$$\sum_{d|n} \emptyset(d) = \sum_{d|1} \emptyset(d) = \emptyset(1) = 1 = n$$

Assuming that $n > 1$, let us consider the number-theoretic function

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

Because $\emptyset$ is known to be a multiplicative function, asserts that F is also multiplicative. Hence, if $n = P_1^{k_1} P_2^{k_2} \ldots P_r^{k_r}$ is the prime factorization of n, then

$$F(n) = F\left(P_1^{k_1}\right) F\left(P_2^{k_2}\right) \ldots F\left(P_r^{k_r}\right)$$

For each value of i,

$$F\left(P_i^{k_i}\right) = \sum_{d|P_i^{k_i}} \emptyset(d)$$

$$= \emptyset(1) + \emptyset(P_i) + \emptyset\left(P_i^2\right) + \emptyset\left(P_i^3\right) + \cdots + \emptyset\left(P_i^{k_i}\right)$$

$$= 1 + (P_i - 1) + \left(P_i^2 - P_i\right) + \left(P_i^3 - P_i^2\right) + \cdots + \left(P_i^{k_i} - P_i^{k_i - 1}\right)$$

$$= P_i^{k_i}$$

because the terms in the foregoing expression cancel each other, save for the term $P_i^{k_i}$. knowing this, we end up with

$$F(n) = P_1^{k_1} P_2^{k_2} \ldots P_r^{k_r} = n$$

and so

$$n = \sum_{d|n} \emptyset(d)$$

as desired.

We should mention in passing that there is another interesting identity that involves the phi-function.

Theorem (2.11):

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

Proof:

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

$$a_1 + a_2 + \cdots + a_{\emptyset(n)} = (n - a_1)(n - a_2) \ldots \left(n - a_{\emptyset(n)}\right)$$

$$= \emptyset(n)n - \left(a_1 + a_2 + \cdots + a_{\emptyset(n)}\right)$$

Hence,

$$2\left(a_1 + a_2 + \cdots + a_{\emptyset(n)}\right) = \emptyset(n)n$$

leading to the stated conclusion.

This is a good point at which o give an application of the Möbius inversion formula.

Theorem (2.12):

For any positive integer n,

$$\emptyset(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

Proof:

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

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

the result is

$$\emptyset(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right)$$

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

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

$$10\sum_{n|d}\frac{\mu(d)}{d} = 10\left[(1) + \frac{\mu(2)}{2} + \frac{\mu(5)}{5} + \frac{\mu(10)}{10}\right]$$

$$= 10\left[1 + \frac{(-1)}{2} + \frac{(-1)}{5} + \frac{(-1)^2}{10}\right]$$

$$= 10\left[1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{10}\right] = 10 \cdot \frac{2}{5} = 4 = \emptyset(10)$$

Starting with Theorem (2. 12), it is an easy matter to determine the value of the phi-function for any positive integer n. 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

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

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

$$\frac{\mu(1)\mu\left(P_1^{a_1}\right)\mu\left(P_2^{a_2}\right)\ldots\mu\left(P_r^{a_r}\right)}{P_1^{a_1}P_2^{a_2}\ldots P_r^{a_r}} \quad 0 \le a_i \le k_i$$

or, because μ is known to be multiplicative,

$$\frac{\mu\left(P_1^{a_1}P_2^{a_2}\ldots P_r^{a_r}\right)}{P_1^{a_1}P_2^{a_2}\ldots P_r^{a_r}} = \frac{\mu(d)}{d}$$

where the summation is over the set of divisors $d = P_1^{a_1}P_2^{a_2}\ldots P_r^{a_r}$, of n. Hence, $P = \sum_{d|n}\mu(d)/d$. It follows from Theorem (2. 12) that

$$\emptyset(n) = n\sum_{d|n}\frac{\mu(d)}{d} = n\prod_{P_i|n}\left(\mu(1) + \frac{\mu(P_i)}{P_i} + \cdots + \frac{\mu\left(P_i^{k_i}\right)}{P_i^{k_i}}\right)$$

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

$$\emptyset(n) = n\prod_{P_i|n}\left(\mu(1) + \frac{\mu(P_i)}{P_i}\right) = n\prod_{P_i|n}\left(1 - \frac{1}{P_i}\right)$$

which agree with the formula established earlier by different reasoning. What is significant about this argument is that no assumption is made concerning the multiplication character of the phi-function, only of μ.

Number Theory Problems

1) Find the primes P for which $\frac{2^{p-1}-1}{p}$ is square.

Solution:

Suppose $\frac{2^{p-1}-1}{p} = n^2$ for some positive integer then $2^{p-1} = pn^2$

Clearly both p and n must be odd let p = 2k + 1 for some positive integer k then $2^{2^k} - 1 = pn^2$ that is $(2^k-1)(2^k+1) = pn^2$ since $2^k - 1$ and 2^k+1 must be a perfect square suppose 2^k-1 is a perfect square r^2

$2^k - 1 = r^2$

$2^k = r^2 + 1$

then is

$2^{p-1} = (r^2+1)^2$

Since r≥ 1 and is odd r = 2i+ 1 for some integer ≥0 then $2^k = (2i + 1)^2 = 2(2i^2+2i+1)$ this is possible if and only if i = 0 then r = 1 so $2^{p-1} = (1^2+1)^2 = 4$ and hence p=3

Suppose 2^k+1 is a perfect square s^2

$2^k + 1 = s^2$

$2^k = s^2 - 1$

That is $2^{p-1} = (s-1)^2(s+1)^2$ since s≥3 and is odd s= 2i +1 for some i≥I then $2^k=(2i+1)^2-1 = 4i(i+1)$

That is $2^{k-2} = i(i+1)$ this is possible if and only if is i= 1 then s=3 and hence $2^{p-1} = 2^2.4^2 = 2^6$ so p=7

Thus p must be 3 or 7

2) Find the remainder when 24^{1947} is divisible by 17.

Solution:

$24 \equiv 7 \pmod{17}$

There $24^{1947} \equiv 7^{1947} \pmod{17}$

But by fermat's little theorem

$7^{16} \equiv 1 \pmod{17}$ so

$7^{1947} \equiv 7^{16.121+11} \equiv (7^{16})^{121}. 7^{11}$

$\equiv 1^{121}.7^{11} \equiv 7^{11} \pmod{17}$

But $z^7 \equiv -2 \pmod{17}$

So $7^{11} \equiv (7^2)^5.7 \equiv (-2)^5. 7 \equiv -32-7$

$\equiv 2.7 \equiv 14 \pmod{17}$

Thus when 24^{1947} is divided by 17

The remainder is 14.

3) solve the congruence: $12x \equiv 48 \pmod{18}$

Solution:

Since (12,18) = 6 and 6/48 the congruence has six incongruent solutions modulo 6 6 they are given by $x = x_0 + (m/d)t = x_0 + (18/6)t = x_0 + 3t$

Where x_0 is a particular solution and $0 \leq t < 6$ by trial and error $x_0 = 1$ is a solution thus the six incongruent solution modulo 18 are $1 + 3t$ where $0 \leq t < 6$ that is 1,4,7, ,10,13 and 16.

4) find all positive integer n such that n^2+1 is divisible by n+1

Solution:

There is only one such positive integer n=1 in fact $n^2+1 = n(n+1) - (n-1)$ thus if $n+1/n^2+1$ then $n + 1/ n-1$ which for positive integer n is possible only if n-1 so hence if n=1.

5) Find all integers n >1 such that $1^n + 2^n + \ldots + (n-1)^n$ is divisible by n.

Solution:

For positive integer n we have

$1^3 + 2^3 + \ldots + n^3 = n^2 (n+1)^3/n$

By induction we obtain also the indentity.

$1^5 + 2^5 + \ldots n^5 = 1/12\, n^2 (n+1)^2 (2n+2n-1)$

For all positive integer n it follows from these formula that $3(1^5+ \ldots + n^5)/(1^3+2^3+\ldots+n^3) = 2n^2+ 2n+1$

Which prove the desired property.

6) solve the linear system

X ≡ 1 (mod 3), x ≡ 2(mod 4), and x ≡ 3(mod 5).

Solution:

Here m = 3.4.5=6, m_1=m/3 = 20, m_2=m/4=15 and m3 = m/5 = 12 the unique solutions of the congruences $m_1,y_1 \equiv 1(\text{mod}m_1)$, $m_2\ y_2 \equiv 1(\text{mod}m_2)$ and $m_3y_3 \equiv 1(\text{mod}m_3)$, that is 20y1 ≡ (mod3), $15y_2 \equiv 1(\text{mod}4)$, and $12y_3 \equiv 1(\text{mod}5)$ are 2,3 and 3, respectivelty thus by the CRT.

$$x \equiv \sum_{i=1}^{3} a_i m_i y_i (modm)$$

≡ 1.20.2 +2.15.3+3.12.3 (mod 60)

≡ 58(mod 60)

7) the largest integer the scientific calculator casio fx 330 A can handle is the eight – digit number 99, 999,999. Compute the exact value of 2^{31} using this calculator and the CRT.

Solution:

To compute the value of $x = 2^{31}$, we select k pairwise relatively prime numbers $m_1,m_2, \ldots,m_k$

Where m = $m_1, m_2, \ldots, m_k > x$, and then compute the least residue.

8)For any n ≥ 2 $\boldsymbol{T(n) \equiv \sum_{k=1}^{n} \left(\left[\frac{n}{k} \right] - \left[\frac{n-1}{k} \right] \right)}$

Solution:

Note that

$$\left[\frac{n}{k}\right] - \left[\frac{n-1}{k}\right] = \begin{cases} 1 & \text{if } \frac{k}{n} \\ 0 & \text{other wise} \end{cases}$$

Hence

$$\sum_{k=1}^{n} \left(\left[\frac{n}{k} \right] - \left[\frac{n-1}{k} \right] \right) = \sum 1 = T(n)$$

Remarks it is clear that is n aprime if and only if T(n) = 2 hence

$$\sum_{k=1}^{n} \left(\left[\frac{n}{k} \right] - \left[\frac{n-1}{k} \right] \right) = 2$$

If and only if n is prime

9) For any n≥ 2 $\boldsymbol{\frac{\sigma(n)}{T(n)} \geq \sqrt{n}}$

Solution:

Let $d_1, d_2, \ldots, d_{T(n)}$ nethe divisors of n they can be rewritten as $\frac{n}{d_1}, \frac{n}{d_2}, \ldots . \frac{n}{d_{r(n)}}$

Hence

$\sigma(n)^2 = n\left(d_1 + d_2 \ldots . + d_{T(n)}\right)\left(\frac{1}{d_1} + \frac{1}{d_2} + \cdots .. + \frac{1}{d_{r(n)}}\right) \geq$ nT $(n)^2$ and the conclusion follows.

10) Prove that there are infinitely many positive integers n such that. Ø(n) = n/3.

Solutions:

Let $n = 2.3^m$ where mis appositive integer then $Ø(n) = Ø\ (2.3^m) = Ø(2)$ $Ø(3^m) = 3^m - 3^{m-1} = 2.3^{m-1} = n/3$

For infinitely many values of n as desired.

References

1 -Elementary number theory - David m- Burton

2 -Elementary number theory with application - THOMAS KOSHY

3 - number theory structures/examples / and problems Titu Andreescu dorin Andrica

4 - 250 problems in elementary number Theory by W.SFRINSKI/ polish academy of sciences

5 - مدخل إلي نظريه الإعداد تشارلز فانون ايدين / ترجمه رمضان محمد جهيمه د.إبراهيم رياض

6 - نظريه الإعداد تأليف أسماء أكرم سلامه