# DIRECTORATE OF DISTANCE EDUCATION
# UNIVERSITY OF NORTH BENGAL

## MASTER OF SCIENCES- MATHEMATICS
## SEMESTER –III

## ELEMENTARY NUMBER THEORY
## DEMATH3OLEC5

# BLOCK-1

**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-1 ELEMENTARY NUMBER THEORY

**Introduction to Block**

The branch of number theory that investigates properties of the integers by elementary methods. These methods include the use of divisibility properties, various forms of the axiom of induction and combinatorial arguments. Sometimes the notion of elementary methods is extended by bringing in the simplest elements of mathematical analysis. Traditionally, proofs are deemed to be non-elementary if they involve complex numbers.

Usually, one refers to elementary number theory the problems that arise in branches of number theory such as the theory of divisibility, of congruences, of arithmetic functions, of indefinite equations, of partitions, of additive representations, of the approximation by rational numbers, and of continued fractions. Quite often, the solution of such problems leads to the need to go beyond the framework of elementary methods. Occasionally, following the discovery of a non-elementary solution of some problem, one also finds an elementary solution of it.

# UNIT 1: DIVISIBILITY THEORY I

**STRUCTURE**



## 1.0 OBJECTIVES

- What is a Divisibility?
- Whatis divison?
- What are greatest common divisor?

- What is prime?

# 1.1 INTRODUCTION

All numbers are integers, unless specified otherwise. Thus in the following definition, *d*, *n*, and *k* are integers.

## 1.1.1 Definition

The number d divides the number n if there is a k such thatn = dk. (Alternate terms are: d is a divisor of n, or d is a factor of n, or n isa multiple of d.) This relationship between d and n is symbolized d | n. Thesymbol d ∤n means that d does not divide n.Note that the symbol d | n is different from the fraction symbol d/n. Itis also different from n/d because d | n is either true or false, while n/d is arational number.

## 1.1.2 Divisibility Properties

For all numbers n, m, and d,

(1) $d \mid 0$

(2) $0 \mid n \Longrightarrow n = 0$

(3) $1 \mid n$

(4) (Reflexivity property) $n \mid n$

(5) $n \mid 1 \Longrightarrow n = 1$ or $n = -1$

(6) (Transitivity property) $d \mid n$ and $n \mid m \Longrightarrow d \mid m$

(7) (Multiplication property) $d \mid n \Longrightarrow ad \mid an$

(8) (Cancellation property) $ad \mid an$ and $a \neq 0 \Longrightarrow d \mid n$

(9) (Linearity property) $d \mid n$ and $d \mid m \Longrightarrow d \mid an + bm$ for all a and b

(10) (Comparison property) If d and n are positive and $d \mid n$ then $d \leq n$

**Proof:**For the first item, take k = 0.

For the second, if 0 | n then n = 0·k = 0.

The next item holds because we can take n as the k in the definition.

Reflexivity is similar: n = n · 1 shows that it holds.

The next property followsimmediately from Basic Axiom 3 for Z, from the first Appendix.

For Transitivity, assume the d | n and that n | m. Then $n = dk_1$ andm = $nk_2$ for some $k_1$, $k_2$∈Z. Substitute to get $m = nk_2 = (dk_1)k_2$.

By theAssociative Property of Multiplication, $(dk_1)k_2 = d(k_1k_2)$, which shows that ddivides m.

Multiplication also follows from associativity. Assume that d | n so thatn = dk. Then an = a(dk) = (ad)k shows that ad | ak.

For Cancellation, assume that a 6= 0 and that ad | an. Then there is a ksuch that an = (ad)k. We will show that n = dk. Assume first that a >0. Bythe Trichotomy Property from the first Appendix, either n > dk or n = dk orn < dk. If n > dk then we have that an > a(dk) = (ad)k, which contradicts thisparagraph's assumption that an = (ad)k. If n < dk then an < a(dk) = (ad)k, also contradicting the assumption. Therefore n = dk, and so d | n.

Theargument for the a <0 case is similar.

To verify Linearity, suppose that d | n and d | m so that n = dk1 andm = dk2 for k1, k2 ∈Z. Then an + bm = a(dk1) + b(dk2) = d(ak1 + bk2) showsthat d | (an + bm).

Finally, for Comparison, assume that d, n >0 and d | n. Then n = dkfor some k. Observe that k is positive because the other two are positive.

ByTrichotomy, either d < n or d = n or d > n. We will show that the d > n caseis not possible.

Assume that d > n. Then dk > nk follows by one of the firstAppendix's Properties of Inequalities. But that gives n > nk, which means thatn · 1 > n · k despite that fact that k is positive and so 1 ≤ k. This is impossiblebecause it violates the same Property of Inequalities.

## 1.1. 3 Definition

An integer n is even (or has even parity) if it is divisible by 2and is odd (or is of odd parity) otherwise.

## Lemma

Recall that $|a|$ equals $a$ if $a \geq 0$ and equals $-a$ if $a < 0$.

(1) If $d \mid a$ then $-d \mid a$ and $d \mid -a$.

(2) If $d \mid a$ then $d \mid |a|$

(3) The largest positive integer that divides a nonzero number $a$ is $|a|$.

Proof. For (1), if $d \mid a$ then $a = dk$ for some $k$. It follows that $a = (-d)(-k)$and since $-d$ and $-k$ are also integers, this shows that $-d \mid a$. It also followsthat $-a = (-k)d$, and so $d \mid -a$.

For (2), suppose first that $a$ is nonnegative. Then $|a| = a$ and so if $d \mid a$then $d \mid |a|$. Next suppose that $a$ is negative. Since $|a| = -a$ for negative $a$, andsince (1) shows that $d \mid -a$, and $d$ therefore divides $|a|$.

For (3), first note that $|a|$ actually divides $a$: in the $a \geq 0$ case $|a| \mid a$ becausein this case $|a| = a$ and we know that $a \mid a$, while in the $a < 0$ case we have that$a = |a|(-1)$, so that $|a|$ is indeed a factor of $a$. We finish by showing that $|a|$is maximal among the divisors of $a$. Suppose that $d$ is a positive number thatdivides $a$. Then $a = dk$ for some $k$, and also $-a = d(-k)$. Thus $d \mid |a|$, whether$a$ is positive or negative. So by the Comparison property of Theorem 1.1.2, we
have that $d \leq |a|$.

# 1.2 DIVISION

## 1.2.1 Theorem

Where $a$ and $b > 0$ are integers, there are integers $q$ and $r$,called the *quotient* and the *remainder* on division of $a$ by $b$, satisfying these twoconditions.

$$a = bq + r \qquad 0 \leq r < b$$

Further, those integers are unique.

Note that this result has two parts. One part is that the theorem says thereexists a quotient and remainder satisfying the conditions. The second part isthat the quotient, remainder pair are unique: no other pair of numbers satisfiesthose conditions.

Proof. To verify that for any $a$ and $b > 0$ there exists an appropriate quotientand remainder we need only produce suitable numbers. Consider these.

$$q = \left\lfloor \frac{a}{b} \right\rfloor \qquad r = a - bq$$

Obviously $a = bq + r$, so these satisfy the first condition. To finish the existencehalf of this proof, we need only check that $0 \leq r < b$. The Floor Lemma fromthe Some Properties of $\mathbb{R}$appendix gives

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}$$

Multiply all of the terms of this inequality by $-b$. Since $b$ is positive, $-b$ isnegative, and so the direction of the inequality is reversed.

$$b - a > -b \left\lfloor \frac{a}{b} \right\rfloor \geq -a$$

Add $a$ to all three terms of the inequality and replace$\lfloor a/b \rfloor$by $q$ to get

$$b > a - bq \geq 0.$$

Since $r = a - bq$ this shows that $0 \leq r < b$.

We still must prove that $q$ and $r$ are unique. Assume that there are twoquotient, remainder pairs

$$a = bq_1 + r_1 \text{ with } 0 \leq r_1 < b$$

and

$$a = bq_2 + r_2 \text{ with } 0 \leq r_2 < b.$$

Subtracting

$$0 = a - a = (bq_1 + r_1) - (bq_2 + r_2) = b(q_1 - q_2) + (r_1 - r_2)$$

implies that

(1) $$r_2 - r_1 = b(q_1 - q_2).$$

We must show that the two pairs are equal, that $r_1 = r_2$ and $q_1 = q_2$. To obtaina contradiction, suppose otherwise. First suppose that $r_1 \neq r_2$. Then one mustbe larger than the other; without loss of generality assume that $r2 > r1$. Then

$$0 \leq r_1 < r_2 < b$$

and so $r_2 - r_1 < b$. But (1) shows that $b$ divides $r_2 - r_1$ and by the Comparisonproperty of Theorem 1.1. 2 this implies that $b \leq r_2 - r_1$. This is the desiredcontradiction and so we conclude that $r_1 = r_2$. With that, from equation (1) wehave $0 = b(q_1 - q_2)$. Since $b > 0$, this gives that $q_1 - q_2 = 0$ and so $q_1 = q_2$.

## Corollary

The number $d$ divides the number $n$ if and only if on divisionof $n$ by $d$ the remainder is 0.

Proof. If the remainder is 0 then $n = dq + 0 = dq$ shows that $d \mid n$. For theother half, if $d \mid n$ then for some $k$ we have

$$n = dk = dk + 0 \text{ (with } 0 \leq 0 < d)$$

and the fact that the quotient, remainder pair is uniqus shows that $k$ and 0must be the quotient and the remainder.

That corollary says that Theorem 1 generalizes the results on divisibility. For instance, fix $b = 3$. Then, given $a$, instead of only being able to say that$a$ is divisible or not, we can give a finer description: $a$ leaves a remainder of 0(this is the case where $b \mid a$), or 1, or 2.

## 1.2.3 Definition

For $b > 0$ define $a \bmod b = r$ where $r$ is the remainder when $a$is divided by $b$. For example: $23 \bmod 7 = 2$ since $23 = 7 \cdot 3 + 2$ and $-4 \bmod 5 = 1$ since$-4 = 5 \cdot (-1) + 1$.

The division algorithm also works in □[$x$], the set of polynomials with rational coefficients, and □[$x$], the set of all polynomials with real coefficients. For the sake of our study, we will onlyfocus on □[$x$]. If $a(x)$ and $b(x)$ are two polynomials, then we can find a unique quotient and remainder polynomial, $q(x)$, $r(x)$ $\in$□[$x$], such that

$$a(x) = b(x)q(x) + r(x), \qquad \deg(r) < \deg(b) \qquad \text{or} \qquad r(x) = 0.$$

**Example:** *Calculate $q(x)$ and $r(x)$ such that $a(x) = b(x)q(x) + r(x)$ for $a(x) = x^4 + 3x^3 + 10$ and $b(x) = x^2 - x$.*

***Solution:*** We begin by dividing the leading term of $a(x)$ by the leading term of $b(x)$: $\frac{x^4}{x^2} = x^2$. Therefore, we multiply $b(x)$ by $x^2$ and subtract the result from

$$a(x): x^4 + 3x^3 + 10 = (x^2 - x)(x^2) + (4x^3 + 10).$$

Now, in order to get rid of the $4x^3$ term in the remainder, we have to divide this bythe leading term of $b(x)$, $x^2$: $\frac{4x^3}{x^2}$= $4x$. We add this to the quotient and subtractthis multiplication from the remainder in order to get rid of the cubic term:

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2 + 4x) + (4x^2 + 10.)$$

One may be tempted to stop here, however, the remainder and $b(x)$ are bothquadratic and we need $\deg(r(x)) < \deg(b(x))$. Therefore, in order to remove thequadratic term from the remainder, we divide this term, $4x^2$, by the leading termof $b(x)$, $x^2$: $\frac{4x^2}{x^2}$= = 4. We then add this to thequotient, and subtract, in order toget

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2 + 4x + 4) + (4x + 10).$$

Therefore, $q(x) = x^2 + 4x + 4$and $r(x) = 4x+10$. We verify that indeed $\deg(r(x)) =1 <\deg(b(x)) =2$, therefore, we are finished.

*[Note:* The numbers will not always come out as nicely as they did in the aboveexpression, and we will occasionally have fractions.]

## 1.2.3 Theorem

For two polynomials, a(x), b(x) ∈Q[x], prove that thereexists a unique quotient andremainder polynomial, q(x) and r(x), such that

$$a(x) = b(x)q(x) + r(x), \deg(r) <\deg(b) \text{ or } r(x) = 0.$$

*Proof.* For any two polynomials $a(x)$ and $b(x)$, we can find $q(x)$ and $r(x)$ such that

$$a(x) = b(x)q(x) + r(x)$$

by repeating the procedure above.

The main idea is to eliminate the leading term of $r(x)$ repeatedly, until $\deg(r(x)) <\deg(b(x))$.

•Divide the leading term of $a(x)$ by the leading term of $b(x)$ in order to obtainthe polynomial $q1(x)$. In the example above, we found $q1(x) = \frac{x^4}{x^2} = x^2$and

$r1(x) = 4x3 + 10$. Then, $a(x) = b(x)\, q1(x) + r1(x)$.

• Divide the leading term of $r1(x)$ by the leading term of $b(x)$ in order to obtainthe polynomial $q2(x)$. In the example above, we found $q2(x) =\frac{4x^3}{x^2}= 4x$.

Then, add this quotient to $q1(x)$ and subtract in order to find $r2(x)$:

$$a(x) = b(x)\, (q1(x) + q2(x)) + r2(x).$$

In the example above, $r2(x) = 4x^2 + 10$.

Repeat the above step of dividing the leading term of $rj(x)$ by the leadingterm of $b(x)$ and adding this quotient to the previous quotients. So long asdeg($rj(x)$) ≥ deg($b(x)$), this will decrease the degree of the remainder polynomial by eliminating its leading term.

Stop once deg($rj(x)$) <deg($b(x)$),at which point

$$\sum_{i=1}^{j}(q_i(x)) \text{ and } r(x) = r_j(x).$$

For the uniqueness part, note that if there exists distinct quotients $q1(x)$,$q2(x)$ and remainders $r1(x)$, $r2(x)$ with deg($r1(x)$) <deg($b(x)$) and deg($r2(x)$) <deg($b(x)$) found through the division algorithm, we willarrive at a contradiction:

$a(x) = b(x)q1(x) + r1(x)$

$a(x) = b(x)q2(x) + r2(x)$

$b(x)(q1(x) - q2(x)) = r2(x) - r1(x)$.

However, assuming that $q1(x)$ and $q2(x)$ are distinct, we havedeg $[b(x)(q1(x) - q2(x)] \geq$ deg($b(x)$).

On the other hand, since deg($r1(x)$) <deg($b(x)$) and deg($r2(x)$) <deg($b(x)$), weknow that

$$\deg(r2(x) - r1(x)) < \deg(b(x)).$$

Therefore, it is impossible for the left hand side of the equation above to equalthe right hand side since the degrees of the polynomials are different.

**Example**: Show that the expression $a\ (a2 + 2)/3$ is an integer forall $a$ :=: 1.

**Solution:** According to the Division Algorithm, every $a$ is of the form $3q$, $3q + 1$, or$3q + 2$. Assume the first of these cases. Then

$$\frac{a(a^2 + 2)}{3} = q(9q^2 + 2)$$

which clearly is an integer. Similarly, if $a = 3q + 1$, then

$$\frac{(3q + 1)((3q + 1)^2 + 2)}{3} = (3q + 1)(3q^2 + 2q + 1)$$

and $a(a^2 + 2)/3$ is an integer in this instance also. Finally, for $a = 3q + 2$, we obtain

$$\frac{(3q + 2)((3q + 2)^2 + 2)}{3} = (3q + 2)(3q^2 + 4q + 2)$$

an integer once more. Therefore, this result is established in all cases.

**Example:** Prove that for every positive integer $n$ the number $3(1^5+2^5+ \ldots +n^5)$ is divisible by $1^3+2^3+ \ldots +n^3$•

For positive integer $n$, we have

$$1^3+2^3+\ldots+n^3 = \frac{n^2(n+1)^2}{4}$$

(which follows by induction). By induction, we obtain also the identity

$$1^5+2^5+\ldots+n^5 = \frac{1}{12}n^2(n+1)^2(2n^2+2n-1)$$

for all positive integer $n$. It follows from these formulas that

$$3(1^5+2^5+\ldots+n^5)/(1^3+2^3+\ldots+n^3) = 2n^2+2n-1,$$

which proves the desired property.

**Example:** For positive integer $n$, find which of the two numbers $a_n = 2^{2n+1} - 2^{n+1}+1$ and $b_n = 2^{2n+1}+2^{n+1}+1$ is divisible by 5 and which is not.

**Solutions:** Consider four cases:

(a) $n = 4k$, where $k$ is a positive integer. Then

$a_n = 2^{8k+1} - 2^{4k+1} + 1 \equiv 2 - 2 + 1 \equiv 0 \pmod 5$

$b_n = 2^{8k+1} + 2^{4k+1} + 1 \equiv 2 + 2 + 1 \equiv 0 \pmod 5$

(since $2^4 \equiv 1 \pmod 5$, which implies $2^{4k} \equiv 2^{8k} \equiv 1 \pmod 5$).

(b) n = $4k+1$, $k = 0, 1, 2, ....$ Then

$a_n = 2^{8k+3} - 2^{4k+2} + 1 \equiv 8 - 4 + 1 \equiv 0 \pmod 5$

$b_n = 2^{8k+3} + 2^{4k+2} + 1 \equiv 8 + 4 + 1 \equiv 3 \pmod 5$

(c) $n = 4k+2$, $k = 0, 1, 2, ....$ Then

$a_n = 2^{8k+5} - 2^{4k+3} + 1 \equiv 2 - 8 + 1 \equiv 0 \pmod 5$

$b_n = 2^{8k+5} + 2^{4k+3} + 1 \equiv 2 + 8 + 1 \equiv 0 \pmod 5$

(d) $n = 4k+3$, $k = 0, 1, 2, ....$ Then

$a_n = 2^{8k+7} - 2^{4k+4} + 1 \equiv 2 - 8 + 1 \equiv 0 \pmod 5$

$b_n = 2^{8k+7} + 2^{4k+4} + 1 \equiv 2 + 8 + 1 \equiv 0 \pmod 5$

Thus, the numbers *an* are divisible by 5 only for $n \equiv 1$ or 2 (mod 4), whilethe numbers $b_n$are divisible by 5 only for $n \equiv 0$ or 3 (mod 4). Thus one andonly one of the numbers $a_n$and $b_n$is divisible by 5.

# 1.3 GREATEST COMMON DIVISOR

## 1.3.1 Definition

An integer is a *common divisor* of two others if it divides bothof them.
We write $C(a, b)$ for the set of numbers that are common divisors of $a$ and $b$.

## 1.3.2 Definition

The *greatest common divisor* of two nonzero integers $a$ and $b$,gcd($a$, $b$), is the largest integer that divides both, except that gcd(0, 0) = 0.
The exception is there because every number divides zero, and so we

speciallydefine gcd(0, 0) to be a convienent value.

**Example** The set of common divisors of 18 and 30 is$C(18, 30) = \{-1, 1, -2, 2, -3, 3, -6, 6\}$.

So, gcd(18, 30) = 6.

## Lemma

Gcd $(a, b)$ = gcd $(b, a)$.

Proof. Clearly the two sets $C(a, b)$ and $C(b, a)$ are equal. It follows that theirlargest elements are equal, that is, that gcd $(a, b)$ = gcd$(b, a)$.

## Lemma

Gcd $(a, b)$ = gcd $(|a|, |b|)$.

Proof. If $a = 0$ and $b = 0$ then $|a| = a$ and $|b| = b$, and so in this casegcd$(a, b)$ = gcd$(|a|, |b|)$. Suppose that one of $a$ or $b$ is not 0. Lemma1.1.4 showsthat $d \mid a \Leftrightarrow d \mid |a|$. It follows that the two sets $C(a, b)$ and $C(|a|, |b|)$ are thesame set. So the largest member of that set, the greatestcommon divisor of $a$and $b$, is also the greatest common divisor of $|a|$ and $|b|$.

## Lemma

If $a \neq 0$ or $b \neq 0$, then gcd $(a, b)$ exists and satisfies$0 <$gcd$(a, b) \leq \min\{|a|, |b|\}$.

**Proof**. Note that gcd$(a, b)$ is the largest integer in the set $C(a, b)$. Since $1 \mid a$and $1 \mid b$ we know that $1 \in C(a, b)$. So the greatest common divisor must be atleast 1, and is therefore positive. On the other hand, if $d \in C(a, b)$ then $d \mid |a|$and $d \mid |b|$, so $d$ is no larger than $|a|$ and no larger than $|b|$.

Thus, $d$ is at mostthe minimum of $|a|$ and $|b|$. qed

**Example** The above results give thatgcd (48, 732) = gcd(−48, 732) = gcd(−48, −732) = gcd(48, −732).

We also know that 0 <gcd(48, 732) ≤ 48. Since if $d$ = gcd(48, 732) then $d \mid$

48,to find *d* we need check only for positive divisors of 48 that also divide 732.

**Remark** Observe that the first two lemmas, which draw conclusions aboutthe properties of the gcd operator, preceed Lemma 1.3.5, which shows that thegcd exists.If two numbers have a greatest common divisor of 1 then they have nonontivial common factors.

## 1.3.3 Theorem

For integers a, b, c, the following hold:

(a) a|0, 1|a, a|a.

(b) a|1 if and only if a= ±1.

(c) If a|b and c|d, then ac|bd.

(d) If a|b and b|c, then a|c

(e) a|b and b|a if and only if a = ±b.

(f) If a|b and b ≠0, then |a| ≤ |b|

(g) If a | band a | c, then a |(bx + cy) for arbitrary integers x andy.

**Proof**. We shall prove assertions (f) and (g), leaving the other parts as an exercise. Ifa|b, then there exists an integer c such that b = ac; also, b ¥= 0 implies that c ≠0.

Upon taking absolute values, we get |b|= |ac| = |a||c|. Because c ≠0, it followsthat |c| ≥1, whence |b|= |a||c|≥ |a|.

As regards (g), the relations a|band a|censure that b = ar and c = as forsuitable integers r and s. But then whatever the choice of x and y,

$$bx + cy = arx + asy = a(rx + sy)$$

Because *rx* + *sy* is an integer, this says that *a* |*(bx* + *cy),* as desired.

It is worth pointing out that property (g) of Theorem 2.2 extends by inductionto sums of more than two terms. That is, if $a|b_k$fork = 1, 2, .., *n,* then

$$a \mid (b_1x_1 + b_2x_2 + \cdots + b_nx_n)$$

for all integers $x_1, x_2, \ldots, x_n$.

If *a* and *b* are arbitrary integers, then an integer *d* is said to be a *commondivisor* of *a* and *b* if both *d* I*a* and *d* I*b.* Because 1 is a divisor of every integer1 is a common divisor of *a* and *b;* hence, their set of positive common divisors isnonempty.

Now every integer divides zero, so that if *a*= *b* = 0, then every integerserves as a commondivisor of *a* and *b.* In this instance, the set of positive commondivisors of *a* and *b* is infinite. However, when at least one of *a* or *b* is different fromzero, there are only a finite number of positive common divisors. Among these, thereis a largest one, called the greatest common divisor of *a* and *b.*

## 1.3.4 Definition

Let *a* and *b* be given integers, with at least one of them different fromzero. The *greatest common divisor* of *a* and *b,* denoted by gcd(a, *b),* is the positiveinteger *d* satisfying the following:

(a) $d|a$ and $d|b$.

(b) If $c|a$ and $c|b$, then $c \leq d$.

**Example :** The positive divisors of -12 are 1, 2, 3, 4, 6, 12, whereas those of 30are 1, 2, 3, 5,6, 10, 15, 30; hence, the positive common divisors of -12 and 30 are 1,2, 3, 6.

Because 6 is the largest of these integers, it follows that

$$\text{Gcd}(-12, 30) = 6.$$

Inthe same way, we can show that

gcd(-5, 5) = 5      gcd(8 , 17) = 1      gcd (-8, -36) = 4

Notes

## 1.3.5 Theorem

Given integers $a$ and $b$, not both of which are zero, there exist integers $x$ and $y$ such that

$$\text{Gcd}(a, b) = ax + by$$

*Proof.* Consider the setS of all positive linear combinations of $a$ and $b$:

$$S = \{au + bv \mid au + bv > 0;\ u, v \text{ integers}\}$$

Notice first that Sis not empty. For example, if $a \neq 0$, then the integer $|a| = au + b \cdot 0$ lies inS, where we choose $u = 1$ or $u = -1$ according as $a$ is positive or negative.By virtue of the Well-Ordering Principle, $S$ must contain a smallest element $d$. Thus,from the very definition of $S$, there exist integers $x$ andy for which $d = ax + by$. Weclaim that $d = \gcd(a, b)$.

Taking stock of the Division Algorithm, we can obtain integers $q$ and $r$ such that

$a = qd + r$, where 0 ::S $r < d$. Then $r$ can be written in the form

$$r = a - qd = a - q(ax + by)$$
$$= a(l - qx) + b(-qy)$$

If $r$ were positive, then this representation would imply that $r$ is a member of $S$,contradicting the fact that $d$ is the least integer in $S$ (recall that $r < d$). Therefore,$r = 0$, and so $a = qd$, orequivalently $d|a$. By similar reasoning, $d|b$, the effect ofwhich is to make $d$ a common divisor of $a$ and $b$.

Now if cis an arbitrary positive common divisor of the integers $a$ and $b$, then part(g) of Theorem 1.3.5 allows us to conclude that $c \mid (ax + by)$; that is, $c \mid d$. By part (f) ofthe sametheorem, $c = |c| \leq |d| = d$, so that $d$ is greater than every positive commondivisor of $a$ and $b$. Piecing the bits of information together, we see that $d = \gcd(a, b)$.

A perusal of the proof of Theorem 1.3.7 reveals that the greatest common divisorof $a$ and $b$ may be described as the smallest positive integer of the form $ax + by$.

Consider the case in which $a = 6$ and $b = 15$. Here, the setS becomes

$s = \{6(–2) + 15 \cdot 1, 6(–1) + 15 \cdot 1, 6 \cdot 1 + 15 \cdot 0, 0\ 0 \ldots.\}$

$= \{3, 9, 6, \ldots.\}$

We observe that 3 is the smallest integer inS, where 3 = gcd(6, 15).

The nature of the members of *S* appearing in this illustration suggests anotherresult, which we give in the next corollary.

## Lemma

If *a* and *b* are given integers, not both zero, then the set$T = \{ax + by \mid x, y$ *are* integers} is precisely the set of all multiples of *d* = gcd(a, *b)*.

*Proof*. Because $d \mid a$ and $d \mid b$, we know that $d \mid (ax + by)$ for all integers *x, y*. Thus,every member *ofT* is a multiple of *d*. Conversely, *d* may be written as $d = ax_0 + by_0$for suitable integers $x_0$and $y_0$ , so that any multiple *nd* of *dis* of the form

$$nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0)$$

Hence, *nd* is a linear combination of *a* and *b,* and, by definition, lies in *T*.It may happen that 1 and -1 are the only common divisors of a given pair ofintegers *a* and *b,* whence gcd (a, *b)*= 1.

**For example:**

$$\gcd(2, 5) = \gcd(–9, 16) = \gcd(–27, –35) = 1$$

This situation occurs often enough to prompt a definition

## 1.3.6 Definition

Two numbers are *relatively prime* if they have a greatest common divisor of 1.Although the relatively prime relationship is symmetric — if gcd(*a*, *b*) = 1then gcd(*b*, *a*) = 1 — we sometimes state it as “*a* is relatively prime to *b*.”

## 1.3.7 Theorem

Let a and b be integers, not both zero. Then a and b are relatively primeif and only if there exist integers x and y such that 1 = ax + by.

**Proof**. If a and bare relatively prime so that gcd(a, b)= 1, then Theorem 1.3.8 guarantees the existence of integers x and y satisfying 1 = ax + by. As for the converse,suppose that 1 =ax+ by forsomechoiceofx andy, and thatd = gcd(a, b). Becaused | a and d | b, Theorem 1.3.6 yields d|(ax+ by), or d |1. Inasmuch as dis a positiveinteger, this last divisibility condition forces d to equal1 (part (b) of Theorem 1.3.6 playsa role here), and the desired conclusion follows.

This result leads to an observation that is useful in certain situations; namely,

## Lemma

If $g$ = gcd ($a$, $b$) then gcd($a/g$, $b/g$) = 1.

**Proof.**The greatest common divisor of $a/g$ and $b/g$ must exist, by the priorresult. Let gcd($a/g$, $b/g$) = $k$. Then $k$ is a divisor of both $a/g$ and $b/g$ so thereare numbers $ja$ and $jb$ such that $jak = a/g$ and $jbk = b/g$.

Therefore $ja(kg) = a$and $jb(kg) = b$, and so $kg$ is a common divisor of $a$ and $b$. If $k > 1$ this would be a contradiction, because then $kg > g$ but $g$ is the greatest common divisor. Therefore $k = 1$.

Let us observe that gcd (-12, 30) = 6andgcd (-12/6, 30/6) = gcd(-2, 5) = 1as it should be.It is not true, without adding an extra condition, that $a \mid c$ and $b \mid c$ together give$ab \mid c$.

For instance, 6 | 24 and 8 | 24, but $6 \cdot 8 \nmid 24$. If 6 and 8 were relatively prime, of course, this situation would not arise. This brings us to next Lemma as follows.

## Lemma

If $a \mid c$ and $b \mid c$, with gcd (a, $b$)= 1, then $ab \mid c$.

***Proof.***Inasmuch as $a \mid c$ and $b \mid c$, integers *rands* can be found such that $c = ar = bs$.

Now the relation gcd (a, $b$)= 1 allows us to write $1 = ax + by$ for some choice ofintegers $x$ andy. Multiplying the last equation by c, it appears that

$$c = c \cdot 1 = c(ax + by) = acx + bey$$

If the appropriate substitutions are now made on the right-hand side, then

$$c = a(bs)x + b(ar)y = ab(sx + ry)$$

or, as a divisibility statement, $ab \mid c$.

## 1.3.7 Theorem

Euclid's lemma. If $a \mid be$, with gcd(a, $b$)= 1, then $a \mid c$.

***Proof.***We start again from Theorem 1.3.8, writing $1 = ax + by$, where $x$ and $y$ areintegers. Multiplication of this equation by $c$ produces

$$c = 1 \cdot c = (ax + by)c = acx + bey$$

Because $a \mid ac$ and $a \mid be$, it follows that $a \mid (acx + bey)$, which can be recast as $a \mid c$.If $a$ and $b$ are not relatively prime, then the conclusion of Euclid's lemma mayfail to hold.

For example: $12 \mid 9 \cdot 8$, but $12 \nmid 9$ and $12 \nmid 8$.

The subsequent theorem often serves as a definition of*gcd(a , b).* The advantageof using it as a definition is that order relationship is not involved. Thus, it may beused in algebraic systemshaving no order relation.

## 1.3.8 Theorem

Let $a$, $b$ be integers, not both zero. For a positive integer $d$,

$d$ = gcd(a, $b$) if and only if

(a) $d \mid a$ and $d \mid b$.

(b) Whenever cIa and $c \mid b$, then $c \mid d$.

***Proof.*** To begin, suppose that $d$ = gcd(a, $b$). Certainly, $d$ I$a$ and $d$ I$b$, so that (a)holds. In light of Theorem 2.3, $d$ is expressible as $d = ax + by$ for some integers $x, y$.Thus, if $c$ 1$a$ and $c$ I$b$, then $c$ I$(ax+ by)$, or rather $c$ I$d$. In short, condition (b) holds.

Conversely, let $d$ be any positive integer satisfying the stated conditions. Given anycommon divisor $c$ of $a$ and $b$, we have $c \mid d$ from hypothesis (b). The implication isthat $d \geq c$, andconsequently dis the greatest common divisor of $a$ and $b$.

**Example:** Prove that if $a$ and $b$ are different integers, then there exist infinitelymany positive integers $n$ such that $a+n$ and $b+n$ are relatively prime.

Solutions: Let $a$ , and $b$ be two different integers. Assume for instance $a < b$ ,and let

$$n = (b-a)k + I-a.$$

For $k$ sufficiently large, $n$ will be positive integer.

We have

$$a+n = (b-a)k+l,\ b+n = (b-a)(k+1)+1,$$

hence $a+n$ and $b+n$will be positive integers.

If we had $d|a+n$ and $d|b+n$, we would have$d|a-b$, and, in view of $d|a+n$, also d|l, which implies that $d$ = 1. Thus,

$$(a+n, b+n) = 1.$$

**Example:** Prove that every integer> 6 can be represented as a sum of twointegers > 1 which are relatively prime.

**Solutions:** If $n$ is odd and> 6, then $n = 2+(n-2)$, where $n-2$ is odd and> 1, and we have $(2, n-2)$ =1.

The following proof for the case of even $n > 6$ is due to A. Makowski.If $n = 4k$, where $k$ is aninteger > 1 (since $n > 6$), then

$$n = (2k-1)+ +(2k+1),\ \text{and}\ 2k+1>2k-1> 1\ (\text{since}\ k>1).$$

The numbers $2k-1$ and $2k+1$, as consecutive odd numbers, are relatively prime.

If $n = 4k+2$, where $k$ is an integer > 1 (since $n > 6$), we have

$$n = (2k+3)+(2k-1), \text{ where } 2k+3 > 2k-1 > 1 \text{ (since } k > 1).$$

Thenumbers $2k+3$ and $2k-1$are relatively prime since if $0 < d \mid 2k+3$ and $d \mid 2k-1$, then $d \mid (2k+3)-(2k-1)$ or $d \mid 4$. Now, $d$ as a divisor of an oddnumber must be odd, hence $d = 1$, and $(2k+3, 2k-1) = 1$.

**Check Your Progress**

1. State and explain the division properties

2. What do you understand by Relatively prime?

3. Define Greatest common divisor and highlight its two properties.

# 1 .4 SUMMARY

The Division Algorithm, acts as the foundation stone in the integers.

# 1.5 KEYWORDS

1. **Prime** - A prime number is a whole number greater than 1 whose only factors are 1 and itself.
2. **Division** - The division is a method of distributing a group of things into equal parts.

3. **Divisor** – Divisor is a number or an integer which divides any other number to give the result
4. **Hypothesis** – A statement that might be true, which might then be tested.
5. **Implication** - the conclusion that can be drawn from something although it is not explicitly stated.

## 1 .6 QUESTIONS FOR REVIEW

1. Find all integers $x \neq 3$ such that $x-3 | x^3-3$.
2. Prove that there exists infinitely many positive integers $n$ such that $4n^2+1$ is divisible both by 5 and 13.
3. Find all integers n > 1 such that $1^n+2^n+ \ldots +(n-l)^n$ is divisible by n.
4. Given integers *a, b, c, d,* verify the following:
   (a) If $a | b$, then $a | be$.
   (b) If $a |$ band $a | c$, then $a^2 | be$.
   (c) $a | b$ if and only if $ac | be$, where $c \neq 0$.
   (d) If $a$ Iband $c$ I$d$, then $ac | bd$.
5. Prove or disprove: If $a | (b +c)$, then either $a |$ *bora* | c

## 1.7 SUGGESTED READING


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.

# 1.8 ANSWERS TO CHECK YOUR PROGRESS

**1.** **[**(1) $d \mid 0$

(2) $0 \mid n \Longrightarrow n = 0$

(3) $1 \mid n$

(4) *(Reflexivity property)* $n \mid n$

(5) $n \mid 1 \Longrightarrow n = 1$ or $n = -1$

(6) *(Transitivity property)* $d \mid n$ and $n \mid m \Longrightarrow d \mid m$

(7) *(Multiplication property)* $d \mid n \Longrightarrow ad \mid an$

(8) *(Cancellation property)* $ad \mid an$ and $a \neq 0 \Longrightarrow d \mid n$

(9) *(Linearity property)* $d \mid n$ and $d \mid m \Longrightarrow d \mid an + bm$ for all $a$ and $b$

(10) *(Comparison property)* If $d$ and $n$ are positive and $d \mid n$ then $d \leq n$. *Provide the proofs –1.1.2***]**

**2.** **[**Two numbers are *relatively prime* if they have a greatest common divisor of 1.Although the relatively prime relationship is symmetric — if gcd($a$, $b$) = 1then gcd($b$, $a$) = 1 — we sometimes state it as "$a$ is relatively prime to $b$."Hint – Provide the theorem and proof –1.3.10 and 1.3.11**]**

**3.** **[**The *greatest common divisor* of $a$ and $b$, denoted by gcd(a, $b$), is the positiveinteger $d$ satisfying the following:

(a) $d|a$ and $d|b$.

(b) If $c|a$ and $c|b$, then $c \leq d$.*—1.3.7***]**

# UNIT 2: DIVISIBILITY THEORY -II

## STRUCTURE



## 2.0 OBJECTIVE

- Understand the The Euclidean Algorithm
- What is THE DIOPHANTINE EQUATION?

## 2.1 THE EUCLIDEAN ALGORITHM

Euclidean algorithm is a method for efficiently finding the greatest common divisor of two numbers. The GCD of two integers X and Y is the largest number that divides both of X and Y.

We can efficiently compute the greatest common divisor of two numbers.We first reduce the problem. Since gcd($a$, $b$) = gcd($|a|$, $|b|$) (and gcd(0, 0) =0), we need only give a method to compute gcd($a$, $b$) where $a$ and $b$ are nonnegative. And, since gcd($a$, $b$) = gcd($b$, $a$), it is enough for us to give a method for $a \geq b \geq 0$.

Euclidean algorithm concept can be illustrated as :

Let $a$ and $b$ be two integers whose greatest common divisor is desired.

Because gcd($|a|$, $|b|$) = gcd(a , $b$),there is no harm in assuming that $a \geq b > 0$.

The first step is to apply the Division

Algorithm to $a$ and $b$ to get

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

If it happens that $r_1 = 0$, then $b \mid a$ and gcd(a, $b$) = $b$. When $r_1 \neq 0$, divide $b$ by $r_1$ to produce integers $q_2$ and $r_2$ satisfying

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears, say, at the(n + l)th stage where $r_{n-1}$ is divided by $r_n$(a zero remainder occurs sooner orlater because the decreasingsequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain morethan $b$ integers).

The result is the following system of equations:

$$\begin{array}{ll} a = q_1 b + r_1 & 0 < r_1 < b \\ b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ \vdots & \\ r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n + 0 & \end{array}$$

We argue that $r_n$, the last nonzero remainder that appears in this manner, is equal togcd(a , $b$). Our proof is based on the lemma below.

## Lemma

If $a > 0$ then $\gcd(a, 0) = a$.

**Proof.**Since every integer divides 0, $C(a, 0)$ is just the set of divisors of $a$. Thelargest divisor of $a$ is $|a|$. Since $a$ is positive, $|a| = a$, and so $\gcd(a, 0) = a$.

The prior lemma reduces the problem of computing $\gcd(a, b)$ to the casewhere $a \geq b > 0$.

## Lemma

If $a > 0$ then gcd $(a, a) = a$.

**Proof**. Obviously, $a$ is a common divisor. By Lemma 1.3.5, $\gcd(a, a) \leq |a|$ andsince $a$ is positive, $|a| = a$. So $a$ is the greatest common divisor.

We have now reduced the problem to the case $a > b > 0$. The central resultis next.

## Lemma

Let $a > b > 0$. If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

**Proof**. It suffices to show that the two sets $C(a, b)$ and $C(b, r)$ are equal, becausethen they must have the same greatest member. To show that the sets are equalwe will show that they have the same members.

First, suppose that $d \in C(a, b)$, so that $d \mid a$ and $d \mid b$. Note that $r = a - bq$.

By Theorem 1.1.2(3) we have that $d \mid r$. Thus $d \mid b$ and $d \mid r$, and so $d \in C(b, r)$.

We have shown that any member of $C(a, b)$ is a member of $C(b, r)$, that is, that$C(a, b) \subseteq C(b, r)$.

For the other containment, assume that $d \in C(b, r)$ so that $d \mid b$ and $d \mid r$.Since $a = bq + r$, Theorem 1.1.2(3) applies again to shows that $d \mid a$. So $d \mid a$ and$d \mid b$, and therefore $d \in C(a, b)$.

The *Euclidean Algorithm* uses Lemma 2.1.3 to compute the greatest commondivisor of two numbers. Rather introduce a computer language in which to givealgorithm, we will illustrate it with an example.

**Example** Compute gcd(803, 154).

gcd(803, 154) = gcd(154, 33) since 803 = 154 · 5 + 33

gcd(154, 33) = gcd(33, 22) since 154 = 33 · 4 + 22

gcd(33, 22) = gcd(22, 11) since 33 = 22 · 1 + 11

gcd(22, 11) = gcd(11, 0) since 22 = 11 · 1 + 0

gcd(11, 0) = 11

Hence gcd(803, 154) = 11.

**Remark** This method is much faster than finding $C(a, b)$ and can findgcd's of quite large numbers.

Recall that Bezout's Lemma asserts that given $a$ and $b$ there exists twonumbers $s$ and $t$ such that gcd$(a, b) = s{\cdot}a+t{\cdot}b$. We can use Euclid's Algorithmto find $s$ and $t$ by tracing through the steps, in reverse.

**Example** Express gcd(803, 154) as a linear combination of 803 and 154.

11 = 33 + 22 · (−1)

= 33 + (154 − 33 · 4) · (−1) = 154 · (−1) + 33 · 5

= 154 · (−1) + (803 − 154 · 5) · 5 = 803 · 5 + 154 · (−26)

## Lemma

If $a = qb + r$, then gcd (a, $b$)= gcd(b, $r$).

***Proof.*** If $d = gcd\ (a, b)$, then the relations $d\ |a$ and $d\ |b$ together imply that $d\ |(a - qb)$, or $d \mid r$. Thus, $d$ is a common divisor of both $b$ and $r$. On the otherhand, if c is an arbitrary commondivisor of $b$ and $r$, then c $|(qb + r)$, wherec|a. This makes c , a common divisor of $a$ and $b$, so that c $\leq d$. It now follows fromthe definition of $gcd\ (b, r)$ that $d = gcd(b, r)$.

**Example:** Let us see how the Euclidean Algorithm works in a concrete caseby calculating, say, gcd (12378, 3054). The appropriate applications of the DivisionAlgorithm produce the equations

$$12378 = 4.\ 3054 + 162$$

$$3054 = 18\ .\ 162 + 138$$

$$162 = 1\ .\ 138 + 24$$

$$138 = 5.\ 24 + 18$$

$$24 = 1.\ 18 + 6$$

$$18 = 3.\ 6+0$$

The integer 6, is the greatest common divisor of 12378 and 3054:

$$6 = \gcd(12378, 3054)$$

To represent 6 as a linear combination of the integers 12378 and 3054, we start withthe next-to-last of the displayed equations and successively eliminate the remainders18, 24, 138, and 162:

Thus, we have

$$6 = 24-18$$

$$= 24- (138- 5\ .\ 24)$$

$$= 6.\ 24- 138$$

$$= 6(162- 138) - 138$$

$$= 6.\ 162 - 7.\ 138$$

$$= 6.\ 162- 7(3054- 18.\ 162)$$

$$= 132.\ 162- 7.\ 3054$$

$$= 132(12378 - 4.\ 3054)- 7.\ 3054$$

$$= 132.\ 12378 + (-535)3054$$

$$6 = \gcd(12378, 3054) = 12378x + 3054y$$

where $x = 132$ and$y = -535$. Note that this is not the only way to express the integer6 as a linear combination of 12378 and 3054; among other possibilities, we could addand subtract 3054 · 12378 to get

$$6 = (132 + 3054)12378 + (-535- 12378)3054= 3186.\ 12378 + (-12913)3054$$

## 2.1.1 Theorem

If $k > 0$, then $gcd(ka, kb) = k \gcd(a, b)$.

***Proof***. If each of the equations appearing in the Euclidean Algorithm for *a* and *b* is multiplied by *k*, we obtain

$ak = q_1(bk) + r_1k \qquad 0 < r_1k < bk$

$bk = q2(r_1k) + r_2k \qquad 0 < r_2k < r1k$

$\vdots$

$r_{n-2}k = q_n(r_{n-1}k) + r_nk \qquad 0 < r_nk < rn\text{-}Ik$

$r_{n-1}k = q_n + I(r_nk) + 0$

We have applied the Euclidean Algorithm to the integers *ak* and *bk*, so thattheir greatest common divisor is the last nonzero remainder $r_nk$; that is,

$$\gcd(ka, kb) = r_nk = k \gcd(a, b)$$

as stated in the theorem.

## Corollary

For any integer $k \neq 0$, $\gcd(ka, kb) = |k| \gcd(a, b)$.

***Proof.***It suffices to consider the case in which $k < 0$. Then $-k = |k| > 0$ and, byTheorem 2.1.5,

$\gcd(ak, bk) = \gcd(-ak, -bk)$

$= \gcd(a|k|, b|k|)$

$= |k| \gcd(a,b)$

**Definition.** The *least common multiple* of two nonzero integers *a* and *b*, denotedby *l*cm (a, *b)*, is the positive integer *m* satisfying the following:

(a) $a|m$ and $b\ |m$.

(b) If $a\ |c$ and $b\ |c$, with $c > 0$, then $m \leq c$.

As an example, the positive common multiples of the integers -12 and 30 are60, 120, 180, ... ; hence, *l*cm(-12, 30) = 60.

It implies that: Given nonzero integers *a*and *b*, *l*cm(a, *b)* always exists and $\text{lcm}(a, b) \leq |ab|$.

## 2.1.2 Theorem

For positive integers *a* and *b*gcd(a, *b)* lcm(a, *b)*= *ab*

***Proof.*** To begin, put $d$ = gcd(a, $b$) and write $a = dr$, $b = ds$ for integers $r$ and $s$. If $m = abjd$, then $m = as = rb$, the effect of which is to make $m$ a (positive) commonmultiple of $a$ and $b$.

Now let $c$ be any positive integer that is a common multiple of $a$ and $b$; say,for definiteness,

$c = au = bv$.

There exist integers $x$ and $y$ satisfying $d = ax + by$.

It results as

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx + uy$$

From above equation, we can states that $m|c$, i.e. $m \leq c$. According to the definition of $l$cm, $m$ = lcm(a, $b$); i.e.

$$lcm\ (a, b) = \frac{ab}{d} = \frac{ab}{\gcd(a, b)}$$

hence, proved

## 2.1.8 Corollary

For any choice of positive integers $a$ and $b$, $l$cm(a, $b$) = $ab$ if and only if gcd(a, $b$)= 1.

In thecase ofthree integers, $a$, $b$, $c$, not all zero, $gcd(a, b, c)$ is defined to be the positive

integer $d$ having the following properties:

(a) $d$ is a divisor of each of $a$, $b$, $c$.

(b) If $e$ divides the integers $a$, $b$, $c$, then $e \leq d$.

**Example:** *Find the greatest common divisor of* $x^4 + x^3 - 4x^2 + x + 5$ *and* $x^3 + x^2 - 9x - 9$.

***Solution***. Using polynomial division, we find that

$$x^4 + x^3 - 4x^2 + x + 5 = (x^3 + x^2 - 9x - 9)x + 5x^2 + 10x + 5 .$$

Next, we have to divide $x^3 + x^2 - 9x - 9$ by $5x^2 + 10x + 5$. We find that

$$x^3 + x^2 - 9x - 9 = (5x^2 + 10x + 5)\left(\frac{x}{5} - \frac{1}{5}\right) + (-8x - 8).$$

Finally, we divide $5x^2 + 10x + 5$ by $-8x - 8$ and find that

$$5x^2 + 10x + 5 = (-8x - 8)\left[-\frac{5}{8}(x + 1)\right]$$

This is the final non-zero remainder. However, remembering that the greatestcommon divisor of two polynomials must be monic, we get rid of the − 85 term anddetermine that

$$\text{Gcd}\,(x^4 + x^3 - 4x^2 + x + 5, x^3 + x^2 - 9x - 9) = x + 1$$

**Example:** *What is the largest positive integer n suchthat* $n^3 + 100$ *is divisible by* $n + 10$*?*

***Solution***. Let$n^3 + 100 = (n + 10)\, n^2 + an + b + c$

$$= n^3 + n^2(10 + a) + n\,(b + 10a) + 10b + c.$$

Equating coefficients yields

$$10 + a = 0$$

$$b + 10a = 0$$

$$10b + c = 100.$$

Solving this system yields $a = -10$, $b = 100$, and $c = -900$. Therefore, by theEuclidean Algorithm, we get

$$n + 10 = \gcd\,(n3 + 100, n + 10) = \gcd(-900, n + 10) =$$

$\gcd(900, n + 10)$

The maximum value for $n$ is hence $n = 890$ .

**Example:** *The numbers in the sequence 101, 104, 109,116, . . . are of the form* $a_n = 100 + n^2$*, where n* = 1*,2, 3, . . . . For each n, let dn be the greatest common divisor of an and an*+1*. Find the maximum valueof dn as n ranges through the positive integers.*

*Solution.* Since $dn = \gcd\,(100 + n^2, 100 + (n + 1)^2)$, $dn$ must divide the differencebetween these two, or

$dn \mid (100 + (n + 1)^2) - (100 + n^2) = 2n + 1.$

Therefore

$$dn = \gcd(100 + n^2, 100 + (n + 1)^2) = \gcd(n^2 + 100, 2n + 1).$$

Since $2n + 1$ will always be odd, 2 will never be a common factor, hence we canmultiply $n^2 + 100$ by 4 without affecting the greatest common divisor:

$$dn = \gcd(4n^2 + 400, 2n + 1) = \gcd\ 4n^2 + 400 - (2n + 1)(2n - 1), 2n + 1$$

$$= \gcd(401, 2n + 1).$$

Therefore, in order to maximize the value of $dn$, we set $n = 200$ to give a greatest common divisor of 401.

**Check Your Progress 1**

1. Explain Euclidean Algorithm?

2. Define GCD & LCM.

# 2.2 THE DIOPHANTINE EQUATION

## 2.2.1 Definition

Let P(x, y, ...) is a polynomial with integer coefficients in one or more variables. A Diophantine equation is an algebraic equation

$$P(x, y, z, ...) = 0$$

for which integer solutions are sought.

For example

$$2x + 3y = 11$$

$$7x^2 - 5y^2 + 2x + 4y - 11 = 0$$

$$y^3 + x^3 = z^3$$

The problem to be solved is to determine whether or not a given Diophantine equation has solutions in the domain of integer numbers.

## 2.2.2 Linear Diophantine Equations (LDE):

**Definition.** A linear Diophantine equation (in two variables x and y) is an equation

$$ax + by = c$$

with integer coefficients a, b, c ∈∃ to which we seek integer solutions. It is not obvious that all such equations solvable. For example, the equation

$$2x + 2y = 1$$

Some linear Diophantine equations have finite number of solutions, for example

$$2x = 4$$

and some have infinite number of solutions.

## 2.2.3 Thereom

The linear equation a, b, c ∈∃

$$ax + by = c$$

has an integer solution in x and y ∈∃⇔gcd (a, b) |c

Proof:

$$\gcd(a, b) \mid a \wedge \gcd(a, b) \mid b \Rightarrow$$

$$\gcd(a, b) \mid (xa + yb) \Rightarrow \gcd(a, b) \mid c$$

Given

Notes

$$\gcd(a, b) \mid c \Rightarrow \exists\ z \in \exists,\ \ c = \gcd(a, b) * z$$

On the other hand

$$\exists\ x_1, y_1 \in \exists, \qquad \gcd(a, b) = x_1 a + y_1 b$$

Multiply this by z:

$$z * \gcd(a, b) = a * x_1 * z + b * y_1 * z$$

$$c = a * x_1 * z + b * y_1 * z$$

Then the pair $x_1 * z$ and $y_1 * z$ is the solution

## 2.2. 4 How Do You Find A Particular Solution?

$$ax + by = c$$

By extended Euclidean algorithm we find gcd and such n and m that

$$a * n + b * m = \gcd(a, b)$$

Multiply this by c

$$a * n * c + b * m * c = \gcd(a, b) * c$$

Divide it by gcd

$$a \frac{n * c}{\gcd(a, b)} + b \frac{m * c}{\gcd(a, b)} = c$$

Compare this with the original equation

$$ax + by = c$$

It follows that a particular solution is

$$x_0 = \frac{n * c}{\gcd(a, b)}\ ; y_0 = \frac{m * c}{\gcd(a, b)}$$

Example: Find a particular solution of

$$56\,x + 72\,y = 40$$

Solution. Run the EEA to find GCD, n and m

GCD ( 56, 72) = 8 = 4∗ 56 + (-3)∗ 72

Then one of the solutions is

$$x_0 = \frac{4 * 40}{8}\;;\; y_0 = \frac{(-3) * 40}{8}$$

$$x_0 = 20;\; y_0 = -15$$

## 2.2.5 How Do You Find All Solutions?

$$ax + by = c$$

By the extended Euclidean algorithm we find gcd and such n and m that

$$\gcd(a, b) = a*n + b*m$$

$$\gcd(a, b)*c = a*n*c + b*m*c$$

Next we add and subtract a∗b∗k where $\forall k \in \exists$

$$\gcd(a, b)*c = a*n*c + b*m*c + a*b*k - a*b*k$$

Collect terms with respect a and b

$$a*(n\,c + b\,k) + b*(m\,c - a\,k) = \gcd(a, b)*c$$

Divide this by gcd$a$, $b$

$$a * \frac{(n\,c + b\,k)}{\gcd(a, b)} + b * \frac{(m\,c - a\,k)}{\gcd(a, b)} = c$$

$$c = a * \left( \frac{n\,c}{\gcd(a,\,b)} + \frac{b\,k}{\gcd(a,\,b)} \right) + b * \left( \frac{m\,c}{\gcd(a,\,b)} - \frac{a\,k}{\gcd(a,\,b)} \right)$$

$$c = a * \left( x_0 + \frac{b * k}{\gcd(a,\,b)} \right) + b * \left( y_0 - \frac{a * k}{\gcd(a,\,b)} \right)$$

$$k = 0,\ \pm 1,\ \pm 2,\ \ldots$$

It can be rewritten as

since $x_0$, $y_0$ is a particular solution.

Therefore, all integers solutions are in the form

$$x = x_0 + \frac{bk}{\gcd(a,b)}\ ; y = y_0 - \frac{ak}{\gcd(a,b)}$$

**Example:** Find all integer solutions of

$$56\,x + 72\,y = 40$$

Run the EEA to find GCD, n and m

GCD( 56, 72) = 8 = 4∗ 56 + (-3)∗ 72

All solutions are in the form

$$x = \frac{n\,c}{\gcd(a,\,b)} + \frac{b\,k}{\gcd(a,\,b)}$$

$$y = \frac{m\,c}{\gcd(a,\,b)} - \frac{a\,k}{\gcd(a,\,b)}$$

$$y = \frac{-3 * 40}{8} - \frac{56\,k}{8} = -15 - 7 * k$$

## 2.2.6 Positive Solutions Of LDE:

In some applications it might required to find all positive solutions *x*, *y* .

We take a general solution

$$x = \frac{nc}{\gcd(a,b)} + \frac{bk}{\gcd(a,b)}$$

$$y = \frac{mc}{\gcd(a,b)} - \frac{ak}{\gcd(a,b)}$$

from which we get two inequalities

$$nc + bk > 0$$

$$mc - ak > 0$$

To find out how many positive solutions a given equation has let us consider two cases

a. ax + by = c, gcd (a, b) = 1, a, b > 0
b. ax – by = c, gcd (a, b) = 1, a, b > 0
c.

It follows that in the first case, the equation has a finite number of solutions

$$-\frac{nc}{|b|} < k < \frac{mc}{|a|}$$

In the second case, there is an infinite number of solutions

$$nc - |b|\,k > 0$$

$$mc - |a|\,k > 0$$

**Example:** Determine the number of solutions in positive integers

$$4x + 7y = 117$$

***Solution*:** GCD (4, 7) =1 = 2∗ 4 + ( -1)∗7

The number of solutions in positive integers can be determined from the system

$$nc + bk > 0$$

$$mc - bk > 0$$

Which for our equation transforms to

$$2 * 117 + 7 * k > 0$$

$$(-1) * 117 - 4 * k > 0$$

This gives

$$-\frac{2 * 117}{7} < k < -\frac{117}{4}$$

There 4 such $k$, namely $k$ = – 33, –32, –31, –30.

## 2.2.7 Ldes With Three Variables

Consider

$$3x + 6y + 5z = 7$$

$$\text{GCD}(3, 6)(x+2y) + 5z = 7$$

Let $w = x + 2y$

The equation becomes

$$3w + 5z = 7$$

Its general solution is

$$w = 2 * 7 + 5k$$

$$z = (-1)*7 - 3k$$

since

GCD (3, 5) =1 = 2 ∗ 3 + (–1) ∗ 5

Next we find $x$ and $y$

$x + 2y = 14 + 5k$

Since GCD (1, 2)| (14 +5$k$), the equation is solvable and the solution is

$$x = 1*(14 + 5k) + 2*l$$

$y = 0*(14 + 5k) - 1*l$

where $l \in \exists$ is another parameter. Here are all triple-solutions

$$x = 5k + 2l + 14$$

$$y = -l$$

$$z = -7 - 3k$$

where $k, l = 0, \pm 1, \pm 2, \ldots$

**Check Your Progress 2**

1. What is Diophantine equation?

2. Explain Linear Diophantine equation with steps of finding a particular solution.

## 2.3 SUMMARY

Diophantine equations can be reduced modulo primes, and then occur in coding theory and cryprography. For example elliptic curve cryptography is based on doing calculations in finite field (also called Galois fields) for a diophantine equation of degree 3 in two variables.

In mathematics diophantine equations are central objects in number theory as they express natural questions such as the ways to write a number as a sum of cubes, but they naturally come up in all questions that can be reduced to questions involving discrete objects, e.g. in algebraic topology.

## 2.4 KEYWORDS

1. **Algorithm:**a process or set of rules to be followed in calculations or other problem-solving operations

2. **Linear Combination:** is an expression constructed from a set of terms by multiplying each term by a constant and adding the results

Notes

3. **Variables:**A variable is a quantity that may change within the context of a mathematical problem or experiment.

4. **Equations**: a statement that the values of two mathematical expressions are equal (indicated by the sign =).

5. **Algebraic equation** - statement of the equality of two expressions formulated by applying to a set of variables the algebraic operations, namely, addition, subtraction, multiplication, division, raising to a power, and extraction of a root.

## 2.5 QUESTIONS FOR REVIEW

1. Use the Euclidean Algorithm to obtain integers $x$ andy satisfying the following:
   gcd(56, 72) = $56x + 72y$.
2. Assuming that gcd(a, $b$)= 1, prove the following:
   gcd(a + $b$, $a$- $b$)= 1 or 2
3. Find all integer solutions of$16x+35y = 50$
4. Find a particular solution of 25 x + 30 y = 70
5. Find gcd(143, 227), gcd(306, 657), and gcd(272, 1479).

## 2.6 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.

## 2.7 ANSWERS TO CHECK YOUR PROGRESS

1. Write the Concept of Euclidean algorithm and supporting 3 Lemma's ---2.1, 2.1.1,2.1.2,2.1.3
2. Provide respective definition and conditions ---below 2.1.6
3. [Provide definition with example 2.2.1]
4. [Hint: Define Linear Diophantine equation and write the steps to find particular solution and all solution 2.2.2,  2.2.4 ]

# UNIT 3: PRIMES

## STRUCTURE



## 3.0 OBJECTIVE

Understand the concept of Prime numbers and the fundamental theorem.

## 3.1 PRIME NUMBERS

### 3.1.1 Definition

An integer $p \geq 2$ is *prime* if it has no positive divisors other than 1 and itself. An integer greater than or equal to 2 that is not prime is *composite*.Note that 1 is neither prime nor composite.

Or

An integer $p > 1$ is called a *prime number,* or simply a *prime,* if itsonly positive divisors are 1 and $p$. An integer greater than 1 that is not a prime is termed*composite.*

## 3.1.2 Theorem

If *p*is a prime and pI *ab,* then $p|a$ or $p \mid b$.

*Proof.* If $p|a$, then we need go no further, so let us assume that $p \nmid a$.

Becausethe only positive divisors of $p$ are 1 and $p$ itself, this implies that gcd(p , *a)* = 1.

(Ingeneral, gcd(p, *a)*= *p* or gcd(p, *a)*= 1 according asp I*a* or *p l a.)*

Hence, citingEuclid's lemma, we get $p \mid b$.

## Corollary

If $p$ is a prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some $k$, where $1 \le k \le n$.

***Proof***. Let's proceed by induction on $n$, the number of factors. When $n = 1$, the statedconclusion obviously holds; whereas when $n = 2$, the result is the content of Theorem3.1.2. Assume, as the induction hypothesis, that $n > 2$ and that whenever $p$ divides aproduct ofless than $n$ factors, it divides at least one ofthe factors. Now let $p \mid a_1 a_2 \cdots a_n$.

From Theorem 3.1.2, either $p|a_n$ or $p| a_1 a_2 \cdots a_{n-1}$. If $p|a_n$, then we are through. Asregards the case where $p \mid a_1 a_2 \cdots a_{n-1}$, the induction hypothesis ensures that $p \mid a_k$ for some choice of $k$, with $1 \le k \le n - 1$. In any event, $p$ divides one of the integers$a_1, a_2, \ldots, a_n$.

## Corollary

If $p, q_1, q_2, \ldots, q_n$ are all primes and $p|q_1 q_2 \cdots q_n$, then $p = q_k$ forsome $k$, where $1 \le k \le n$.

***Proof***. By virtue ofCorollary 1, we know that $p \mid q_k$ for some $k$, with $1 \le k \le$

$n$. Beinga prime, $q_k$is not divisible by any positive integer other than 1 or $q_k$itself. Because$p > 1$, we are forced to conclude that $p = q_k$.

## Lemma

An integer $n \geq 2$ is composite if and only if it has factors $a$ and$b$ such that $1 < a < n$ and $1 < b < n$.

**Proof.** Let $n \geq 2$. The 'if' direction is obvious. For 'only if', assume that $n$ iscomposite. Then it has a positive integer factor $a$ such that $a \neq 1$, $a \neq n$. Thismeans that there is a $b$ with $n = ab$. Since $n$ and $a$ are positive, so is $b$. Hence$1 \leq a$ and $1 \leq b$.

As, $a \leq n$ and $b \leq n$. Since $a \neq 1$ and $a \neq n$ wehave $1 < a < n$. If $b = 1$ then $a = n$, which is not possible, so $b \neq 1$. If $b = n$then $a = 1$, which is also not possible.

So $1 < b < n$,finishing this half of theargument.

## Lemma

If $n > 1$ then there is a prime $p$ such that $p \mid n$.

**Proof:**Let $S$ denote the set of all integers greater than 1 that have no primedivisor. We must show that $S$ is empty.If $S$ is not empty then by the Well-Ordering Property it has a smallest member; call it $m$. Now $m > 1$ and has no prime divisor. Then $m$ cannot beprime (as every number is a divisor of itself). Hence $m$ is composite.

Therefore, $m = ab$ where $1 < a < m$ and $1 < b < m$. Since $1 < a < m$, thefactor $a$ is not a member of $S$. So $a$ must have a prime divisor $p$. Then $p \mid a$and $a \mid m$, so by Theorem 1.1. 2, $p \mid m$. This contradicts the assumption that $m$has no prime divisor. So the set $S$ must be empty.

## 3.1.3 Theorem (Euclid's Theorem)

There are infinitely many primes.

**Proof**. Assume, to get a contradiction, that there are only a finitely manyprimes $p_1 = 2$, $p_2 = 3, \ldots, p_n$. Consider the number $N = p_1 p_2 \cdots p_{n+1}$. Since $p_1 \geq 2$, clearly $N \geq 2$. So by Lemma 1.4.3, $N$ has a prime divisor$p$. That prime must be one of $p_1, \ldots, p_n$ since that list was assumed to beexhaustive. However, observe that the equation

$$N = p_i(p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n) + 1$$

along with $0 \leq 1 < pi$ shows by Lemma 1.2.2 that $n$ is not divisible by $p_i$. This isa contradiction; it follows that the assumption that there are only finitely manyprimes is not true.

**Remark** Eucild's Theorem, and its proof, is often cited as an example ofthe beauty ofMathematics.

## 3.1.4 Theorem

If $n > 1$ is composite then $n$ has a prime divisor $p \leq \sqrt{n}$.

Proof. Let $n > 1$ be composite. Then $n = ab$ where $1 < a < n$ and $1 < b < n$. We claim that at least one of $a$ or $b$ is less than or equal to$\sqrt{n}$.. For if not then$a > \sqrt{n}$.and $b > \sqrt{n}$., and hence $n = ab > \sqrt{n}.\cdot\sqrt{n}.= n$, which is impossible.

Suppose, without loss of generality, that $a \leq \sqrt{n}$. Since $1 < a$, by Lemma 1.4.3there is a prime $p$ such that $p \mid a$. Hence, by Transitivity in Theorem 1.1.2, since$a \mid n$ we have $p \mid n$. By Comparison in Theorem 1.1.2, since $p \mid a$ we have$p \leq a \leq \sqrt{n}$.

We can use Theorem 1.4.5 to help compute whether an integer is prime. Given$n > 1$, we need only try to divide it by all primes $p \leq \sqrt{n}$. If none of thesedivides $n$ then $n$ must be prime.

**Example** Consider the number 97. Note that $\sqrt{97} < \sqrt{100} = 10$. Theprimes less than 10 are 2, 3, 5, and 7. None of these divides 97, and so 97 isprime.

**Examples:**

1.Find all positive integers *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 $n+1 \mid n^2+1$, then $n+1 \mid n-1$ which for positive integer *n* is possible only if $n-1 = 0$, hence if $n = 1$.

2.Prove that for positive integer *n* we have $169 \mid 3^{3n+3} - 26n - 27$.

**Solution:** We shall prove the assertion by induction.

We have

$$169 \mid 3^6 - 26 - 27 = 676 = 4 \cdot 169.$$

Next, we have

$$3^{3(n+1)} - 26(n+1) - 27 - (3^{3n+3} - 26n - 27) = 26(3^{3n+3} - 1)$$

However, $13 \mid 3^3-1$, hence $13 \mid 13^{3(n+1)}$, and $169 \mid 26(3^{3n+3}-1)$.

The proof by induction follows immediately.

**Check Your Progress 1**

1. Define Prime & state two examples

---

---

2. Explain your understanding of , ‘There are infinite primes’.

---

---

# 3.2 THE FUNDAMENTAL THEOREM

## 3.2.1 Theorem (Fundamental Theorem of Arithmetic)

Every numbergreater than 1 factors into a product of primes $n = p_1p_2 \cdots p_s$. Further, writing the primes in ascending order $p_1 \leq p_2 \leq \cdots \leq p_s$ makes the factorizationunique.

Some of the primes in the product may be equal. For instance, $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$. So the Fundamental Theorem is sometimes stated as: every number greaterthan 1 can be factored uniquely as a product of powers of primes.

**Example** 600 = 2 · 2 · 2 · 3 · 5 · 5 = 23 · 3 · 52

We will break the proof of the Fundamental Theorem into a sequence ofLemmas.

## 3.2.2 Lemma (Euclid's Lemma)

If $p$ is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

**Proof.** Assume that $p \mid ab$. If $p \mid a$ then we are done, so suppose that it doesnot.

Let $d = \gcd(p, a)$. Note that $d > 0$, and that $d \mid p$ and $d \mid a$.

Since $d \mid p$ we have that $d = 1$ or $d = p$. If $d = p$ then $p \mid a$, which we assumed was not

true. So we must have $d = 1$. Hence $\gcd(p, a) = 1$ and $p \mid ab$.

So by Bezout's Lemma, $p \mid b$.

## Lemma

Let $p$ be prime. Let $a_1, a_2, \ldots, a_n$, $n \geq 1$, be integers. If $p \mid a_1a_2 \cdots a_n$, then $p \mid ai$ for at least one $i \in \{1, 2, \ldots, n\}$.

**Proof.** We use induction on $n$. For the $n = 1$ base case the result is clear.

For the inductive step, assume the inductive hypothesis: that the lemmaholds for $n$ such that $1 \leq n \leq k$. We must show that it holds for $n = k + 1$.

Assume that $p$ is prime and that $p \mid a_1a_2 \cdots a_ka_{k+1}$. Write $a_1a_2 \cdots a_k$ as $a$, and $a_{k+1}$ as $b$. Then $p \mid a$ or $p \mid b$ by Lemma 3.2.2. If $p \mid a = a_1 \cdots a_k$ then by theinduction hypothesis, $p \mid ai$ for some $i \in \{1, \ldots, k\}$. If $p \mid b$ then $p \mid a_{k+1}$.

Notes

Sowe can say that $p \mid ai$ for some $i \in \{1, 2, \dots, k + 1\}$. This verifies the lemma for$n = k + 1$. Hence by mathematical induction, it holds for all $n \geq 1$.

## 3.2.3 Lemma (Fundamental Theorem, Existence)

If $n > 1$ then there existprimes $p_1, \dots, p_s$, where $s \geq 1$, such that $n = p_1 p_2 \cdots p_s$ and $p_1 \leq p_2 \leq \cdots \leq p_s$.

**Proof.**We will use induction on $n$. The base step is $n = 2$: in this case, since2 is prime we can take $s = 1$ and $p_1 = 2$.

For the inductive step, assume the hypothesis that the lemma holds for$2 \leq n \leq k$; we will show that it holds for $n = k + 1$. If $k + 1$ is prime then $s = 1$and $p_1 = k + 1$. If $k + 1$ is composite then write $k + 1 = ab$ where $1 < a < k + 1$and $1 < b < k + 1$.

By the induction hypothesis there are primes $p_1, \dots, p_u$and$q_1, \dots, q_v$such that $a = p_1 \cdots p_u$and $b = q_1 \cdots q_v$. This gives that $k + 1$ is aproduct of primes

$$k + 1 = ab = p_1 p_2 \cdots p_u q_1 q_2 \cdots q_v,$$

where $s = u + v$. Reorder the primes into ascending order, if necessary.

The base step and the inductive step together give us that the statement istrue for all $n > 1$.

## 3.2.4 Lemma (Fundamental Theorem, Uniqueness)

If $n = p_1 p_2 \cdots p_s$for$s \geq 1$ with $p_1 \leq p_2 \leq \cdots \leq p_s$, and also $n = q_1 q_2 \cdots q_t$for $t \geq 1$ with$q_1 \leq q_2 \leq \cdots \leq q_t$, then $t = s$, and $p_i = q_i$for all $I$ between 1 and $s$.

**Proof.**The proof is by induction on $s$. In the $s = 1$ base case, $n = p_1$ is primeand we have $p_1 = q_1 q_2 \cdots q_t$. Now, $t$ must be 1 or else this is a factorization ofthe prime $p1$, and therefore $p1 = q1$.

Now assume the inductive hypothesis that the result holds for all $s$ with$1 \leq s \leq k$. We must show that the result then holds for $s = k + 1$.

Assume that $n = p_1 p_2 \cdots p_k p_{k+1}$ where $p_1 \leq p_2 \leq \cdots \leq p_{k+1}$, and also $n = q_1 q_2 \cdots q_t$ where

$q_1 \leq q_2 \leq \cdots \leq q_t$.

Clearly $p_{k+1} \mid n$, so $p_{k+1} \mid q_1 \cdots qt$. Euclid's Lemma thengives that $p_{k+1}$ divides some $q_i$. That implies that $p_{k+1} = q_i$, or else $p_{k+1}$ wouldbe a non-1 divisor of the prime $qi$, which is impossible. Hence $p_{k+1} = q_i \leq qt$.

A similar argument shows that $qt = pj \leq pk+1$. Therefore $pk+1 = qt$.

To finish, cancel $p_{k+1} = qt$ from the two sides of this equation.

$$p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_{t-1} q_t$$

Now the induction hypothesis applies: $k = t - 1$ and $p_i = q_i$ for $i = 1, \ldots, t - 1$.

So the lemma holds also in the $s = k + 1$ case, and so by mathematicalinduction it holds for all $s \geq 1$.

**Remark** Unique factorization gives an alternative, conceptually simpler,way to find the greatest common divisor of two numbers.

For example: 600 =23 · 31 · 52 · 70 and 252 = 22 · 32 · 50 · 7.

Now, 23 divides both number. So does31, but 32 does not divide both. Also, the highest power of 5 dividing bothnumbers is 50, and similarly the highest power of 7 that works for both is 70.

So gcd(600, 252) = 22 · 31 · 50 · 70 = 24.

In general, we can find the greatestcommon divisor of two numbers factoring, then taking the minimum power of2, times the minimum power of 3, etc.

**Example:** Given the polynomialwith integer coefficients

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n$$

with integer coefficients $a_1, a_2, \ldots, a_n$ and given that there exist four distinct integers a,b,c and $d$ such thatf(a) = f(b) = f(c) = f(d) = 5, show that there is no integer k for which f(k)=8

**Solution:** Let $g(x) = f(x) - 5$

Then we must have

$$g(x) = k(x-a)(x-b)(x-c)(x-d)h(x)$$

for some h(x) ∊ {ℤ }[x]. Let *k* be such that *f*(*k*)=8, Then *g*(*k*)=3 and we get

$$3=k(x-a)(x-b)(x-c)(x-d)h(x).$$

By the fundamental theorem of arithmetic, we can express 3 as a product of at most three different integers (−1,−3,1).

Since, (*x*−*a*),(*x*−*b*),(*x*−*c*) and *x*−*d*) are all distinct, this is an obvious contradiction.

**Check Your Progress 2**

1. Explain Fundamental Theorem Uniqueness

2. Explain Fundamental Theorem Existence

# 3.3 EXAMPLES

1. Prove that for every integer *k* the numbers 2k+l and *9k+4* are relatively prime, and for numbers *2k-1*and'*9k+4* find their greatest common divisor as a function of *k.*

***Solution:*** Numbers *2k+l* and *9k+4* are relatively prime since *9(2k+1)--2(9k+4)* = I.

Since

$$9k+4 = 4(2k-1)+(k+8),$$

while

$$2k\text{-}1 = 2(k+8)\text{-}17,$$

we have

$$(9k+4, 2k\text{-}1) = (2k\text{-}l, k+8) = (k+8, 17).$$

If $k$ =9

(mod 17), then $(k+8, 17)$ =17;

in the contrary case, we have 17 | k+8,

hence

$$(k+8, 17) = 1.$$

Thus, $(9k+4, 2k\text{-}1) = 17$ if $k \equiv 9 \pmod{17}$

and

$$(9k+4, 2k\text{-}1) = 1 \quad \text{if } k \not\equiv 9 \pmod{17}.$$

2. Prove that if $a$ and $b$ are different integers, then there exist infinitely many positive integers $n$ such that $a+n$ and $b+n$ are relatively prime.

Solution: Let $a$ and $b$ be two different integers.

Assume for instance $a < b$, and let $n = (b\text{-}a)k + 1 - a$.

For $k$ sufficiently large, $n$ will be positive integer.

We have

$$a+n = (b-a)k+1, \qquad b+n = (b-a)(k+1)+1,$$

hence $a+n$ and $b+n$ will be positive integers.

If we had $d|a+n$ and $d|b+n$, we would have $d|a-b$, and, in view of $d|a+n$, also d|l, which implies that $d = 1$.

Thus,

$$(a+n, b+n) = 1.$$

3. Prove that the equation $p^2+q^2 = r^2+s^2+t^2$ has no solution with primes p, $q$, $r$, $s$, $t$.

**Notes**

Solutions: Note first thatifp, $q$,$r$, s, and $t$ are primes and

$$q^2+q^2 = r^2+s^2+t^2,$$

then each of the numbers $p$ and $q$ must be different from each of the numbers r, s, and $t$. In fact, if we had, for instance, $p$ = r then we would also have

$$q^2= s^2+t^2$$

which is impossible since this equation cannot have solutionin primes $q$, s, and $t$. Indeed, the numbers s and $t$ could not be both odd norcould they be both even (since in this case we would have $q$ = 2, which isimpossible in view of the fact that the right-hand side is > 4).

If we had s = 2, then the number 4 would be a difference of two squares of positive
integers which is impossible.
If $p^2+q^2 = r^2+s^2+t^2$, then it is not possible that all numbers $p$, $q$, r,s, $t$are odd.

If $p$ is even, then $p$ = 2, and the numbers $q$,$r$, s, $t$ are odd.
Sincethe square of an odd number gives the remainder 1 upon dividing by 8,the left-hand side would give the remainder 5, and the right-hand side wouldgive the remainder 3, which is impossible. If both $p$ and $q$ are odd, thenthe left-hand side gives the remainder 2 upon dividing by 8, while on theright-hand side one (and only one) of the numbers must be even, for instance
r = 2. Then, however, the right-hand side would give the remainder 6upon dividing by 8, which is impossible.

4. Find all prime solutions $p$, $q$, $r$ of the equation $p(p+l)+q(q+l) = r(r+l)$.

**Solution :** We present the solution found by A. Schinzel. There is only onesolution, namely

$$p = q = 2, r = 3.$$

To see that, we shall find all solutionsof the equation

$$p(p+1) + q(q+1) = n(n+1)$$

where *p* and *q* are primes and*n* is a positive integer.

Our equation yields

$$p(p+l) = n(n+1) - q(q+1) = (n-q)(n+q+1),$$

and we must have $n > q$.

Since *p* is a prime, we have either $p|n\text{-}q$ or$p|n+q+1$. If $p|n\text{-}q$, then we have $p \le n\text{-}q$, whichimplies $p(p+1) \le (n\text{-}q)(n\text{-}q+1)$, and therefore $n+q+l \le n\text{-}q+l$, which is impossible.

Thus we have $p|n+q+1$, which means that for some positive integer $kn+q+1= kp$, whichimplies $p+1= k(n\text{-}q)$.

(1)

If we had $k = 1$, then $n+q+1 = p$ and $p+1 = n\text{-}q$, which gives $p\text{-}q= n+1$ and $p+q = n+1$, which is impossible.

Thus, $k > 1$. From (1) weeasily obtain

$$2q = (n+q) - (n-q) = kp - 1 - (n-q)$$
$$= k[k(n-q) - 1] - 1 - (n-q) = (k+1)[(k-1)(n-q) - 1].$$

Since $k \ge 2$, we have $k+1 \ge 3$.

The last equality, whose left-hand side haspositive integer divisors 1, 2, *q*, and $2q$ only, implies that either $k+1 = q$or $k+1= 2q$. If $k+1= q$, then $(k-1)(n-q) = 3$, hence $(q-2)(n-q) = 3$.

This leads to either $q-2 = 1$, $n-q= 3$, that is $q = 3$, $n = 6$, $k = q-1 = 2$,and, in view of (1), $p = 5$, or else, $q-2 = 3$, $n-q = 1$, which gives $q = 5$,$n = 6$, $k = 4$, and in view of (I), $p = 3$.

On the other hand, if $k+l = 2q$, then $(k-1)(n-k) = 2$, hence$2(q-1)(n-q) = 2$. This leads to $q-1 = 1$ and $n-q = 1$, or $q = 2$, $n = 3$,and, in view of (I), $p =$

2. Thus, for positive integers$n$, we have thefollowing solutions in primes $p$ and $q$:

1) $p = q = 2$, $n = 3$;
2) $p = 5$,$q = 3$, $n = 6$, and
3) $p = 3$, $q = 5$, $n = 6$.

Only in the first solution allthree numbers are primes.

5. Find all primesp, $q$, and $r$ such that the numbers $p(p+l)$, $q(q+l)$, $r(r+1)$ form an increasingarithmetic progression.

**Solution:** Such numbers are, for instance, $p = 127$, $q = 3697$, r = 5527. Itis easy to check (for instance, in the tables of prime numbers) that thesenumbers are primes, and that the numbers $p(p+1)$, $q(q+1)$, and $r(r+1)$form an arithmetic progression.

We shall present a method of finding suchnumbers.
From the identity

$$n(n+1) + (41n+20)(41n+21) = 2(29n+14)(29n+15)$$

it follows that for a positive integer $n$, the numbers

$$n(n+1), (29n+14)(29n+15), \text{and} (41n+20)(41n+21)$$

form an arithmetic progression.
If for some positive integer $n$ the numbers$n$, 29n+14, and $41n+20$ were all primes, we would have found a solution.
Thus, we ought to take consecutive odd primes for $n$ and check whether thenumbers $29n+14$ and 41n+20 are primes.

The least such number is $n = 127$ which leads to the above solution.
We cannot claim, however, that in this manner we obtain all triplets ofprimes with the required properties.

6. Find all positive integers $n$ such that each of the numbers $n+1$, $n+3$, $n+7$, $n+9$, $n+13$, and$n+15$ is a prime.

Solutions: There is only one such positive integer, namely $n = 4$.

In fact, for$n = 1$, the number $n+3 = 4$ is composite;

for $n = 2$, the number $n+7 = 9$is composite;

for $n = 3$, the number n+l = 4 is composite;

and for $n > 4$,all our numbers exceed 5, and at least one of them is divisible by 5.

Thelast property follows from the fact that the numbers 1, 3, 7, 9, 13, and 15give upon dividing by 5 the remainders 1, 3, 2, 4, 3, and 0, hence all possibleremainders.

Thus, the numbers $n+1$, $n+3$, $n+7$, $n+9$, $n+13$, and $n+15$give also all possible remainders upon dividing by 5; therefore at least oneof them is divisible by 5, and as > 5, is composite. On the other hand,for $n = 4$ we get the prime numbers 5,7,11,13,17, and 19.

## 3.4 SUMMARY

Every number $a > 1$ is eithera prime or, by the Fundamental Theorem, can be broken down into unique primefactors and no further, the primes serve as the building blocks from which all other integers can be made. Accordingly, the prime numbers have intrigued mathematicians through the ages, and although a number of remarkable theorems relating totheir distribution in the sequence of positive integers have been proved, even moreremarkable is what remains unproved.

## 3.5 KEYWORDS

**Notes**

1. **Existence** – it is a theorem with a prenex normal form involving the existential quantifier.
2. **Unqueness-** indicate that exactly one object with a certain property exists.
3. **Fundamentals** of **Mathematics -** is a work text that covers the traditional study in a modern prealgebra course, as well as the topics of estimation, elementary analytic geometry, and introductory algebra
4. **Arithmetic** - is a branch of mathematics that consists of the study of numbers, especially the properties of the traditional operations on them—addition, subtraction, multiplication and division
5. **Composite -**A **composite number** is a positive integer which is not prime.

## 3.6 QUESTIONS FOR REVIEW

1. Given that $p$ is a prime and $p \mid a^n$, prove that $p^n|a^n$.
2. If $p \geq q \geq 5$ and $p$ and $q$ are both primes, prove that $24|p^2 - q^2$
3. Prove that every integer> 6 can be represented as a sum of two integers > 1 which are relatively prime.
4. Prove that for every positive integer *m* every even number *2k* can be represented as a difference of two positive integers relatively prime to m.

## 3.7 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.

## 3.8 ANSWERS TO CHECK YOUR PROGRESS

1. HINT: Provide definition of Prime and one theorem and discuss 1 small example 3.1.1
2. [HINT: Provide proof of this theorem statement—3.1.7]
3. [HINT: Provide the statement of theorem with proof -- ***3.2.4***]
4. [HINT: Provide the statement of theorem with proof-- **3.2.5**]

# UNIT 4: PRIME NUMBERS AND THEIR DISTRIBUTION -II

## STRUCTURE



## 4.0 OBJECTIVES

Encode the concept of distribution of primes

Understand the Wilson's and the Prime number Theorem

Comprehend the concept of Fermat Primes and Mersenne Primes

# 4.1 DISTRIBUTION OF PRIMES

The *Sieve of Eratosthenes* is an ancient method to find primes. To find theprimes less than *n*, list the numbers from 2 to $n-1$. The smallest number, 2, isprime. Cross off all proper multiples of 2 (that is, the even numbers greater than2). The smallest number remaining, 3, is prime. Cross off all proper multiples of3, that is, 6, 9, etc. (some of them have already been eliminated). The smallestremaining number, 5, is prime. Cross off all proper multiples of 5. Continue
this process until the list is exhausted.Here is what is left when the sieve filters out the nonprimes less than 100

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | | 2 | 3 | | 5 | | 7 | | |
| 10 | | 11 | | 13 | | | | 17 | | 19 |
| 20 | | | | 23 | | | | | | 29 |
| 30 | | 31 | | | | | | 37 | | |
| 40 | | 41 | | 43 | | | | 47 | | |
| 50 | | | | 53 | | | | | | 59 |
| 60 | | 61 | | | | | | 67 | | |
| 70 | | 71 | | 73 | | | | | | 79 |
| 80 | | | | 83 | | | | | | 89 |
| 90 | | | | | | | | 97 | | |

Obviously, the columns with even numbers and the columns with multiples of5 are empty (except for 2 and 5) but this is an artifact of the fact that the rowsof the table are $10 = 2 \cdot 5$ wide. Other than that, at first glance no pattern isapparent.

## 4.1.1 Theorem

If $P_n$is the *nth* prime number, then $P_n . \leq 2^{2^{n-1}}$

Notes

***Proof.*** Let us proceed by induction on $n$, the asserted inequality being clearly truewhen $n = 1$. As the hypothesis of the induction, we assume that $n > 1$ and that theresult holds for all integers*upton.* Then

$p_{n+1} \leq p_1 p_2 \ldots p_{n+1}$

$$\leq 2 .\, 2^2 \ldots 2^{2^{n-1}} + 1 = 2^{1+2+\cdots+2^{n-1}} + 1$$

Recalling the identity $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, we obtain

$$p_{n+1} \leq 2^{2^{n-1}} + 1$$

However, $1 \leq 2^{2^{n-1}}$ for all $n$; where

$p_{n+1} \leq 2^{2^{n-1}} + 2^{2^{n-1}}$

$= 2 . 2^{2^{n-1}} = 2^{2^n}$

completing the induction step, and the argument.

## 4.1.2 Corollary

For $n \geq 1$, there are at least $n + 1$ primes less than $2^{2^n}$

## Lemma

The product of two or more integers of the form $4n + 1$ is of the same form.

***Proof.*** It is sufficient to consider the product ofjust two integers. Let us take $k = 4n + 1$

and $k' = 4m + 1$. Multiplying these together, we obtain

$$kk' = (4n + 1)(4m + 1)$$

$$= 16nm + 4n + 4m + 1 = 4(4nm + n + ..m) + 1$$

which is of the desired form.

## 4.1.2 Theorem

There are an infinite number of primes of the form $4n + 3$.

***Proof***. In anticipation of a contradiction, let us assume that there exist only finitelymany primes of the form4n + 3; call them $q_1$, $q_2$ , … , $q_s$. Consider the positive integer

$$N = 4q_1,q_2 \cdots q_s - 1 = 4(q_1,q_2 \cdots q_s - 1) + 3$$

and let $N = r_1 r_2 \cdots r_t$ be its prime factorization. Because $N$ is an odd integer, we have $r_k \neq 2$ for all $k$, so that each $rk$ is either of the form $4n + 1$ or $4n + 3$.

By the lemma,the product of any number ofprimes of the form $4n + 1$ is again an integer of this type.

For $N$ to take the form $4n + 3$, as it clearly does, $N$ must contain at least one primefactor $r_i$ of the form $4n + 3$. But $r_i$ cannot be found among the listing $q_1$, $q_2$ , … , $q_s$ for this would lead to the contradiction that $ri \mid 1$. The only possible conclusion is thatthere are infinitely many primes of the form $4n + 3$.

## 4.1.3 Theorem Dirichlet

If $a$ and bare relatively prime positive integers, then the arithmetic progression$a$, $a + b$, $a + 2b$, $a + 3b$, ...contains infinitely many primes.

Dirichlet's theorem tells us, for instance, that there are infinitely many primenumbers ending in 999, such as 1999, 100999, 1000999, ... for these appear in thearithmetic progression determined by $1000n + 999$, where gcd(lOOO, 999) = 1. There is no arithmetic progression $a$, $a + b$, $a + 2b$, ... that consists solely ofprime numbers. To understand this,let $a + nb = p$, where $p$ is a prime.

If we put$n_k = n + kp$ fork= 1, 2, 3, ... then the $n_k th$ term in the progression is

$$a + n_k b = a + (n + kp)b = (a + nb) + kpb = p + kpb$$

Because each term on the right-hand side is divisible by $p$, so is $a + nkb$. In otherwords, the progression must contain infinitely many composite numbers.

Notes

### 4.1.4 Theorem

If all the $n > 2$ terms of the arithmetic progression

$$p, p + d, p + 2d, \dots, p + (n - l)d$$

are prime numbers, then the common differenced is divisible by every prime $q < n$.

***Proof.*** Consider a prime number $q < n$ and assume to the contrary that $q \mid d$. Weclaim that the first $q$ terms of the progression

$$p, p + d, p + 2d, \dots' p + (q - l)d \qquad (1)$$

will leave different remainders when divided by $q$.

Otherwise there exist integers $j$and $k$, with $0 \leq j < k \leq q-1$, such that the numbers $p + jd$ and $p + kd$ yield thesame remainder upon division by $q$. Then $q$ divides their difference $(k - j)d$. But$gcd(q, d) = 1$, and so Euclid's lemma leads to $q \mid k - j$, which is nonsense in light of the inequality $k - j \leq q - 1$.

Because the $q$ different remainders produced from Eq. (1) are drawn from the$q$ integers 0, 1, ... , $q-1$, one of these remainders must be zero. This means that$q \mid p + td$ for some $t$ satisfying $0 \leq t \leq q - 1$. Because of the inequality $q < n \leq p \leq p + td$, we are forced to conclude that $p + td$ is composite. (If $p$ were lessthan $n$, one of the terms of the progression would be $p + pd = p(1 + d)$.) With thiscontradiction, the proof that $q \mid d$ is complete.

## 4.2 WILSON'S THEOREM

### 4.2.1 Theorem (Wilson's Theorem)

There are arbitrarily long gaps betweenprimes: for any positive integer $n$ there is a sequence of $n$ consecutive compositeintegers.

**Proof.**Given $n \geq 1$, consider $a = (n + 1)! + 2$. We will show that all of thenumbers $a, a + 1, . . . , a + (n - 1)$ are composite.

Since $n+1 \geq 2$, clearly $2 \mid (n+1)!$.

Hence

$$2 \mid (n+1)!+2.$$

Since $(n+1)!+2 > 2$,we therefore have that $a = (n + 1)! + 2$ is composite.

We will finish by showingthat the $i$-th number in the sequence, $a + i$ where $0 \leq i \leq n - 1$, is composite.

Because $2 \leq i + 2 \leq n + 1$, we have that $(i + 2) \mid (n + 1)!$.

Hence

$$i + 2 \mid a + i =(n+1)!+(i+2).$$

Because $a+i > i + 2 > 1$, we have that $a+i$ is composite.

### 4.2.2 Definition

For any positive real number $x$, the number of primes less thanor equal to $x$ is $\pi(x)$.

For example, $\pi(10) = 4$.

## 4.3 THE PRIME NUMBER THEOREM

$$\lim_{x\to\infty} \frac{\pi(x)}{(x/\ln(x))} = 1.$$

Here is a table of values of $\pi(10^i)$ and $10^i/\ln(10^i)$ for $i = 2, . . . , 10$ (the second set of values have been rounded to the nearest integer)

| $x$ | $\pi(x)$ | round$(x/\ln(x))$ |
|---|---|---|
| $10^2$ | 25 | 22 |
| $10^3$ | 168 | 145 |
| $10^4$ | 1229 | 1086 |
| $10^5$ | 9592 | 8686 |
| $10^6$ | 78498 | 72382 |
| $10^7$ | 664579 | 620421 |
| $10^8$ | 5761455 | 5428681 |
| $10^9$ | 50847534 | 48254942 |
| $10^{10}$ | 455052511 | 434294482 |

Notes

This table has been continued up to 1021, but mathematicians are still workingon finding the value of $\pi(1022)$. Of course, computing the approximations areeasy, but finding the exact value of $\pi(1022)$ is hard.

## 4.4 FERMAT PRIMES AND MERSENNE PRIMES

A formula that produces the primes would be nice. Historically, lacking such a formula, mathematicians have looked for formulas that at least produce only primes. In 1640 Fermat noted that the numbers in this list

| $n$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $F_n = 2^{(2^n)} + 1$ | 3 | 5 | 17 | 257 | 65,537 |

are all prime. He conjectured that $F_n$is always prime. Numbers of the form$2^{2^n} + 1$ are called *Fermat numbers*.

### Lemma

Let $a$ >1 and $n$ >1. If $a^n$+ 1 is prime then $a$ is even and $n = 2k$ for some $k \geq$ 1.

**Proof.**We first show that $n$ is even. Suppose otherwise, and recall the wellknown factorization.

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$$

Replace $a$ by $-a$.

$$(-a)^n - 1 = (-a - 1)\ (-a)^{n-1} + (-a)^{n-2} + \cdots + (-a) + 1$$

If the exponent $n$ is odd then $n - 1$ is even, $n - 2$ is odd, etc. So we have

$$(-a)^n = -a^n,\ (-a)^{n-1} = a^{n-1},\ (-a)^{n-2} = -a^{n-2}, \text{ etc.,}$$

and the factorizationbecomes

$-(a^n + 1) = -(a + 1)\,(a^{n-1} - a^{n-2} + \cdots - a + 1)$

Then changing the sign of both sides gives

$$(a^n + 1) = (a + 1)(a^{n-1} - a^{n-2} + \cdots - a + 1).$$

But with $n \geq 2$, we have $1 < a + 1 < a^n + 1$. This shows that if $n$is odd and $a$ >1, then $a^n + 1$ is not prime.

So $n$ is even.

Write $n = 2s \cdot t$ where $t$ is odd. Then if $a^n + 1$ is prime wehave $(a^{2^s})^t + 1$ is prime.

But by what we just showed this cannot be prime if $t$is odd and $t \geq 2$.

So we must have $t = 1$ and therefore $n = 2s$.

Also, $an + 1$ prime implies that $a$ is even since if $a$ is odd then so is $an$,and in consequence $an + 1$ would be even. But the only even prime is 2, andwe are assuming that $a$ >1 and so we have $a \geq 2$, which implies that so$a^n + 1 \geq 3$

## 4.4.1 Defiition

A prime number of the form $Fn = 2(2n) + 1$, $n \geq 0$, is a *Fermatprime*.

Euler showed that Fermat number next on the table, $F5$ = 4, 294, 967, 297,is composite.

As $n$ increases, the $Fn$'s increase in size very rapidly, and are not easy tocheck for primality. We know that $Fn$ is composite for all $n$ such that $5 \leq n \leq 30$,and a large number of other values of $n$ including 382447 (the largest one thatI know).

Many researchers now conjecture that $Fn$ is composite for $n \geq 5$. SoFermat's original thought that $Fn$ is always prime is badly mistaken.

Mathematicians have also looked for formulas that produce many primes.That is, we can guess that numbers of various special forms are disproportionately prime. One form that has historically been of interest is are the *Mersennenumbers* $M_n = 2^n - 1$.

| $n$ | 2 | 3 | 5 | 7 | 13 |
|---|---|---|---|---|---|
| $f(n)$ | 3 | 7 | 31 | 127 | 8191 |

All of the numbers on the second row are prime. Note that $2^4 - 1$ is not prime, so this is not supposed to be a formula that gives only primes.

## Lemma

Let $a > 1$ and $n > 1$. If $a^n - 1$ is prime then $a = 2$ and $n$ is prime.

**Proof**. Consider again $a^n - 1 = (a - 1)(a^{n-1} + \cdots + a + 1)$ Note that if $a > 2$and $n > 1$ then $a - 1 > 1$ and $a^{n-1} + \cdots + a + 1 > a + 1 > 3$ so both factors aregreater then 1, and therefore $a^n - 1$ is not prime.
Hence if $a^n - 1$ is prime thenwe must have $a = 2$.

Now suppose $2^n - 1$ is prime. We claim that $n$ is prime. For, if not, then$n = st$ where $1 < s < n$ and $1 < t < n$. Then $2^n - 1 = 2^{st} - 1 = (2^s)^t - 1$ isprime. But we just showed that if $a^n - 1$ isprime then we must have $a = 2$. Sowe must have $2^s = 2$, and hence $s = 1$ and $t = n$.
Therefore $n$ is not composite,that is, $n$ is prime.

## Corollary

If $M_n$is prime, then $n$ is prime.

**Proof**. This is immediate from Lemma 4.4.3.
At first it was thought that $M_p = 2^p - 1$ is prime whenever $p$ is prime. Butin 1536, Hudalricus Regius showed that $M_{11} = 2^{11} - 1 = 2047$ is not prime:2047 $= 23 \cdot 89$.

## 4.4.2 Theorem: Fermat's Theorem

Let $p$ be a prime and suppose that $p \nmid a$. Then $a^{p-1} = 1 \pmod{p}$.

*Proof.* We begin by considering the first $p - 1$ positive multiples of $a$; that is, the integers

$$a, 2a, 3a, \ldots, (p-1)a$$

None of these numbers is congruent modulo $p$ to any other, nor is any congruent to zero. Indeed, if it happened that

$$ra \equiv sa \pmod{p} \quad 1 \leq r < s \leq p - 1$$

then $a$ could be canceled to give $r = s \pmod{p}$, which is impossible. Therefore, the previous set of integers must be congruent modulo $p$ to 1, 2, 3, ... , $p - 1$, taken in some order. Multiplying all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

where

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

Once $(p - 1)!$ is canceled from both sides of the preceding congruence (this is possible because since $p \nmid (p - 1)!$), our line of reasoning culminates in the statement that $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's theorem.

This result can be stated in a slightly more general way in which the requirement that $p \nmid a$ is dropped.

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

***Proof***. When $p \mid a$, the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, 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.. If $a = 1$, the assertion is that $1^p = 1 \pmod{p}$, which clearly is true, as is the case $a = 0$. Assuming that the result holds for $a$, we must confirm its validity for $a + 1$. With reference to 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 $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \le k \le p - 1$. 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 pI (f). But p | k! implies that p |*j* for some *j* satisfying$1 \le k \le p - 1$, an absurdity. Therefore, *p* I(f) or, converting to a congruence statement,

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

The point we wish to make is that

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

where the rightmost congruence uses our inductive assumption. Thus, the desiredconclusion holds for $a + 1$ and, in consequence, for all $a \ge 0$. If *a* happens to bea negative integer, there is no problem: because $a = r \pmod{p}$ for some *r*, where$0 \le r \le p - 1$, we get $a^p \equiv rP \equiv r = a \pmod{p}$.

**Lemma.** If *p* and *q* are distinct primes with $aP = a \pmod{q}$ and $aq = a \pmod{p}$,then $aPq = a \pmod{pq}$.

***Proof.***The last corollary tells us that $(a^q)^p \equiv a^q \pmod{p}$, whereas $a^q \equiv a \pmod{p}$holds byhypothesis. Combining these congruences, we obtain $a^{pq} = a \pmod{p}$ or, indifferent terms, $p \mid a^{pq} - a$. In an entirely similar manner, $q \mid a^{pq} - a$

Hence,

$a^{pq} \equiv a \pmod{pq}$.

## 4.4.3 Definition

A prime number of the form $M_n = 2^n - 1$, $n \geq 2$, is a *Mersenneprime*.

People continue to work on determining which *Mp*'s are prime. To date(2003-Dec-09), we know that $2p - 1$ is prime if $p$ is one of the following 40primes: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281,3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503,132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593,13466917, and 20996011.

The first number with more than a thousand digits known to be prime was$M_{4253}$. The largest number on that list was found on 2003-Nov-17. This numberhas 6, 320, 430 digits. It was found as part of the Great Internet Mersenne PrimeSearch (GIMPS).

One reason that we know so much about Mersenne primes is that the following test makes it easier to check whether or not $M_p$is prime when $p$ is a largeprime.

## 4.4.4 Theorem (The Lucas-Lehmer Mersenne Prime Test)

Let $p$ be anodd prime. Define the sequence $r_1, r_2, r_3, \ldots, r_{p-1}$ by the rules $r_1 = 4$, and for$k \geq 2$,

$$rk = (r_{k-1}^2 - 2) \bmod M_p.$$

Then $M_p$is prime if and only if $r_{p-1} = 0$.

**Example** Let $p = 5$. Then $Mp = M5 = 31$.

$r1 = 4$

$r2 = (42 - 2) \bmod 31 = 14 \bmod 31 = 14$

Notes

$r3 = (142 - 2) \bmod 31 = 194 \bmod 31 = 8$

$r4 = (82 - 2) \bmod 31 = 62 \bmod 31 = 0$

Hence by the Lucas-Lehmer test, $M5 = 31$ is prime.

**Remark** Note that the Lucas-Lehmer test for $M_p = 2^p - 1$ takes only $p-1$steps. On the other hand, if we try to prove that $M_p$is prime by testing allprimes less than or equal to$\sqrt{M_p}$then must consider about $2^{(p/2)}$ steps. Thisis much larger, in general, than $p$.No one knows whether there are infinitely many Mersenne primes.

**Check Your Progress 1**

1. Explain Wilson's theorem

2. Define

a. Fermat's Prime

b. Mersenne Prime

## 4.5 PSUEDOPRIMES

A pseudoprime number is a probable prime number that might actually be a composite number rather than an actual prime. Pseudoprimes are useful in public key cryptography and other aspects of IT. There are infinitely many pseudoprimes, the smallestfour being 341, 561, 645, and 1105.

### 4.5.1 Theorem

If $n$ is an odd pseudoprime, then$M_n = 2^n - 1$ is a larger one.

***Proof.*** Because $n$ is a composite number, we can write $n = rs$, with $1 < r \leq s < n$. So,
$2^r - 1 | 2^n - 1$, or equivalently $2^r - 1 | M^n$ making $M^n$ composite. By our hypotheses, $2n = 2 \pmod{n}$; hence $2n - 2 = kn$ for some integer $k$. It follows that

$$2^{M_n - 1} = 2^{2^n} = 2^{kn}$$

This yields

$$2^{M_n - 1} = 2^{kn} - 1$$

$$= (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1)$$
$$= M_n(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1)$$
$$\equiv 0 \ (mod\ M_n)$$

Therefore, $2^{M_n} - 2 \equiv 0 \pmod{M_n}$, in light of which $Mn$ is a pseudoprime.

More generally, a composite integer $n$ for which $a^n \equiv a \pmod{n}$ is called a *pseudoprime to the base a.* (When $a = 2$, $n$ is simply said to be a pseudoprime.)

## 4.5.2 Definition

There exist composite numbers $n$ that are pseudoprimes to every base $a$; that is,
$an = a \pmod{n}$ for all integers $a$. The least such is 561. These exceptional numbers are called *absolute pseudoprimes* or *Carmichael numbers*

**Example**: Check that $561 = 3 \cdot 11 \cdot 17$ must be an absolute pseudoprime,

**Solution:** gcd(a, 561) = 1 gives
gcd(a, 3) = gcd(a, 11) = gcd(a, 17) = 1
An application of Fermat's theorem leads to the congruences

$a^2 \equiv 1 \pmod{3}$ $a^{10} \equiv 1 \pmod{11}$ $a^{16} \equiv 1 \pmod{17}$

and, in tum, to

$a^{560} \equiv (a^2)^{280} \equiv 1 \pmod{3}$

$a^{560} \equiv (a^{10})^{56} \equiv 1 \pmod{11}$

$a^{560} \equiv (a^{16})^{35} \equiv 1 \pmod{17}$

Thesegiverisetothesinglecongruence $a^{560} \equiv 1 (\text{mod}561)$, wheregcd(a, 561) = 1.

But then $a^{561} = a \pmod{561}$ for all $a$, showing 561 to be an absolute pseudoprime.

## 4.5.3 Theorem

Let $n$ be a composite square-free integer, say, $n = p^1, p^2, \ldots, p^r$ where the $p_i$ are distinct primes. If $p_i - 1 \mid n - 1$ for $i = 1, 2, \ldots, r$, then $n$ is an absolutepseudoprime.

***Proof.*** Suppose that $a$ is an integer satisfying gcd(a, $n$) = 1, so that gcd(a, $p_i$) = 1

for each $i$. Then Fermat's theorem yields $p_i | a^{p_{1-1}} - 1$. From the divisibility hypothesis $p_i - 1 | n - 1$, we have $p_i | a^{n-1} - 1$., and therefore $p_i | a^n - a$., for all $a$ and $i = 1, 2, \ldots, r$.

As a result, we end up with $n \mid a^n - a$, which makes $n$ an absolute pseudoprime.

Examples of integers that satisfy the conditions of Theorem 4.5.1 are

1729 = 7. 13. 19 6601 = 7. 23 . 41 10585 = 5 . 29 . 73

**Check Your Progress 2**

1. Explain Pseudoprime with example

2. Define Absolute pseudoprime

## 4.6 SOLVED EXAMPLES

**1.** A concrete example should help to clarify the proofofWilson's theorem. Specifically, let us take $p = 13$. It is possible to divide the integers 2, 3, ... , 11 into

$(p-3)/2 = 5$ pairs, each product of which is congruent to 1 modulo 13. To write

these congruences out explicitly:

Solution : $2 \cdot 7 \equiv 1 \pmod{13}$

$3 \cdot 9 \equiv 1 \pmod{13}$

$4 \cdot 10 \equiv 1 \pmod{13}$

$5 \cdot 8 \equiv 1 \pmod{13}$

$6 \cdot 11 \equiv 1 \pmod{13}$

Multiplying these congruences gives the result

$$11! = (2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}$$

and so

$$12! \equiv 12 \equiv -1 \pmod{13}$$

Thus, $(p-1)! \equiv -1 \pmod{p}$, with $p = 13$.

**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 $x_1, x_2, \ldots, x_k$ for which the product $(x_i - n) \cdots (x_k - n)$ is a square, say $y^2$.

Then $(x_1 \ldots x_k)^2 \equiv y^2 \pmod{n}$, which might lead to a nontrivial factor of $n$.

**Notes**

A short search reveals that

$$112^2 - 12499 = 45$$
$$117^2 - 12499 = 1190$$
$$121^2 - 12499 = 2142$$

or, written as congruences,

$$112^2 \equiv 3^2.\ 5 \pmod{12499}$$
$$117^2 \equiv 2.\ 5.\ 7 \cdot 17 \pmod{12499}$$
$$1212 \equiv 2.\ 32 \bullet 7 \cdot 17 \pmod{12499}$$

Multiplying these together results in the congruence

$(112 \cdot 117 \cdot 121)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17)^2$ (mod 12499) that is,

$1585584^2 \equiv 107102$ (mod 12499)

But we are unlucky with this square combination. Because

$1585584 \equiv 10710$ (mod 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

$$1132 \equiv 2 \cdot 5 \cdot 33 \pmod{12499}$$
$$1272 \equiv 2.\ 3 \cdot 5 \cdot 11^2 \pmod{12499}$$

which gives rise to the congruence

$(113 \cdot 127)^2 = (2 \cdot 3^2 \cdot 5 \cdot 11)^2$ (mod 12499)

This reduces modulo 12499 to

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

and fortunately $1852 \neq \pm 990$ (mod 12499).

Calculating

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

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

# 4.7 SUMMARY

Wilson's theorem implies that there exists an infinitude of composite numbers of the form n! + 1. Fermat's methodrepresented the first real improvement over the classical method of attempting to find a factor*ofn* by dividing by all primes not exceeding$\sqrt{n}$. Fermat's factorization scheme has at its heart the observation that the search for factors of an odd integer *n*

# 4. 8 KEYWORDS

**1. Arithmetic Progression:** a sequence of numbers in which each differs from the preceding one by a constant quantity

**2. Proof by contradiction:** (also known as **indirect proof** or the method of **reductio ad absurdum**) is a common proof technique that is based on a very simple principle: something that leads to a contradiction *can not* be true, and if so, the opposite *must* be true.

3. **Factorisation** is the opposite process of expanding brackets.

4. **yields –**produce or provide

5. **Composite -** A whole number that can be made by multiplying other whole numbers

# 4.9 QUESTIONS FOR REVIEW

1. Find all pairs of primes *p* and *q* satisfying $p- q = 3$.
2. Determine whether 17 is a prime by deciding whether 16! = -1 (mod 17).
3. Factor the number $2^{11} - 1$ by Fermat's factorization method.

## 4.10 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.


## 4.11 ANSWERS TO CHECK YOUR PROGRESS

**1.** [HINT: Provide the statement and proof -- 4.2]

**2.** [HINT: Provide definitation, representation and example-- 4.5]

**3.** [HINT: Provide definition and example—4.5]

**4.** [HINT: Provide definition and example—4.5.2]

# UNIT 5: CONGRUENCE

**STRUCTURE**

# 5.0 OBJECTIVE

Understand the concept of Congruence

Comprehend its basic and extra properties that has wide application

# 5.1 INTRODUCTION

If n is a positive integer, we say the integers a and b are **congruent** modulo n, and write a≡b(modn), if they have the same remainder on division by nn. (By remainder, of course, we mean the unique number rr defined by the Division Algorithm.) This notation, and much of the elementary theory of congruence, is due to the famous German mathematician, Carl Friedrich Gauss—certainly the outstanding mathematician of his time, and perhaps the greatest mathematician of all time.

# 5.2 CONCEPT OF CONGRUENCE

## 5.2.1 Definition

Let $m \geq 0$. We we say that the numbers $a$ and $b$ are *congruentmodulo m*, denoted $a \equiv b \pmod{m}$, if $a$ and $b$ leave the same remainder whendivided by $m$. The number $m$ is the *modulus* of the congruence. The notation$a \not\equiv b \pmod{m}$ means that they are not congruent.

OR

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

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

if $n$ divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer $k$.

When$n \nmid (a - b)$, we say that $a$ is *incongruent to b modulo n,* and it is represented as$a \not\equiv b \pmod{n}$.

## 5.1.2 Theorem

For arbitrary integers *a* and *b*, $a \equiv b$ (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 divisionby *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 $a = q_1n + r$ and $b = q_2n + r$, with thesame remainder *r* ($0 \leq r < n$). Then

$$a - b = (q_1n + r) - (q_2n + r) = (q_1 - q_2)n$$

whence $n \mid a - b$. In the language of congruences, we have $a \equiv b$ (mod *n*).

## Lemma

The numbers *a* and *b* are congruent modulo *m* if and only if$m \mid (a - b)$, and also if and only if $m \mid (b - a)$.

**Proof.**Write $a = mq_a + r_a$ and $b = mq_b + r_b$ for some $q_a$, $q_b$, $r_a$, and $r_b$, with$0 \leq r_a, r_b < m$. Subtracting gives $a - b = m(q_a - q_b) + (r_a - r_b)$. Observe thatthe restrictions on the remainders imply that $-m < r_a - r_b < m$, and so $r_a - r_b$is not a multiple of *m* unless $r_a - r_b = 0$.

If *a* and *b* are congruent modulo *m* then $r_a = r_b$, which implies that $a - b = m(q_a - q_b)$ which in turn gives that $a - b$ is a multiple of *m*.

The implications in the prior paragraph reverse: if $a - b$ is a multiple of *m*then in the equation $a - b = m(q_a - q_b) + (r_a - r_b)$. we must have that $r_a - r_b = 0$by the observation in the first paragraph, and therefore $r_a = r_b$.The $b - a$ statement is proved similarly.

**Examples**

1. $25 \equiv 1 \pmod 4$ since $4 \mid 24$
2. $25 \not\equiv 2 \pmod 4$ since $4 \nmid 23$
3. $1 \equiv -3 \pmod 4$ since $4 \mid 4$
4. $a \equiv b \pmod 1$ for all $a$, $b$
5. $a \equiv b \pmod 0 \Leftrightarrow a = b$ for all $a$, $b$

$a$ mod $b \equiv r$ where $r$ is the remainder when $a$ is divided by $b$. The two are related but not identitical.

**Example:**One difference between the two is that $25 \equiv 5 \pmod 4$ is truewhile $25 = 5 \bmod 4$ is false (it asserts that $25 = 1$).
The 'mod' in $a \equiv b \pmod m$ defines a binary relation, a relationship betweentwo things. The 'mod' in $a$ mod $b$ is a binary operation, just as addition ormultiplication are binary operations. Thus,$a \equiv b \pmod m \Longleftrightarrow a \bmod m = b \bmod m$.
That is, if $m > 0$ and $a \equiv r \pmod m$ where $0 \le r < m$ then $a \bmod m = r$.
Expressions such as

$$x = 2$$

$$4^2 = 16$$

$$x^2 + 2x = \sin(x) + 3$$

are equations. By analogy, expressions such as

$$x \equiv 2 \pmod{16}$$

$$25 \equiv 5 \pmod 5$$

$$x^3 + 2x \equiv 6x^2 + 3 \pmod{27}$$

are called *congruences*.
The next two theorems show that congruences and equations share manyproperties.

## 5.1.4 Theorem

Congruence is an equivalence relation: for all $a$, $b$, $c$, and$m > 0$ we have
(1) *(Reflexivity property)* $a \equiv a \pmod m$
(2) *(Symmetry property)* $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

(3) *(Transitivity property)* $a \equiv b$ (mod $m$) and $b \equiv c$ (mod $m$) $\Rightarrow a \equiv c$(mod $m$)

**Proof.**For reflexivity: on division by $m$, any number leaves the same remainderas itself.

For symmetry, if $a$ leaves the same remainder as $b$, then $b$ leaves the sameremainder as $a$.

For transitivity, assume that $a$ leaves the same remainder as $b$ on divisionby $m$, and that $b$ leaves the same remainder as $c$.

The all three leave thesame remainder as each other, and in particular $a$ leaves the same remainder as$c$.

Below we will consider polynomials

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

We will assume that the coefficients $a_n, \ldots, a_0$ are integers and that $x$ alsorepresents an integer variable. Here the degree of the polynomial is an integer$n \geq 0$.

## 5.2.5 Theorem

If $a \equiv b$ (mod $m$) and $c \equiv d$ (mod $m$), then

(1) $a + c \equiv b + d$ (mod $m$) and $a - c \equiv b - d$ (mod $m$)

(2) $ac \equiv bd$ (mod $m$)

(3) $an \equiv bn$ (mod $m$) for all $n \geq 1$

(4) $f(a) \equiv f(b)$ (mod $m$) for all polynomials $f(x)$ with integer coefficients.

***Proof of (1).***Since $a - c = a + (-c)$, it suffices to prove only the addition case.

By assumption

$$m \mid a - b \text{ and } m \mid c - d.$$

By linearity of the 'divides' relation,

$$m \mid (a - b) + (c - d),$$

that is $m \mid (a + c) - (b + d)$.

Hence

$$a + c \equiv b + d \pmod{m}. \text{ qed}$$

***Proof of (2).*** Since $m \mid a - b$ and $m \mid c - d$, by linearity $m \mid c(a - b) + b(c - d)$.

Now,

$$c(a - b) + b(c - d) = ca - bd,$$

hence

$$m \mid ca - bd, \text{ and so } ca \equiv bd \pmod{m},$$

as desired.

***Proof of (3).*** We prove this by induction on $n$. If $n = 1$, the result is true bythe assumption that $a \equiv b \pmod{m}$. Assume that the result holds for $n = 1, \ldots,$ $k$. Then we have

$$a^k \equiv b^k \pmod{m}.$$

This, together with $a \equiv b \pmod{m}$ using property (2) above, gives that

$$aa^k \equiv bb^k \pmod{m}.$$

Hence

$$a^{k+1} \equiv b^{k+1} \pmod{m}$$

and the result holds in the $n = k + 1$ case. So the result holds for all $n \geq 1$, by induction.

***Proof of (4).*** Let $f(x) = c_n x^n + \cdots + c_1 x + c_0$.

We prove by induction onthe degree of the polynomial $n$ that if $a \equiv b \pmod{m}$ then

$$c_n a^n + \cdots + c0 \equiv c_n b^n + \cdots + c_0 \pmod{m}.$$

For the degree $n = 0$ base case, by the reflexivity ofcongruence we have that $c_0 \equiv c_0 \pmod{m}$.

For the induction assume that the result holds for $n = k$. Then we have

$$(*) \qquad c_k a^k + \cdots + c_1 a + c_0 \equiv c_k b_k + \cdots + c_1 b + c_0 \pmod{m}.$$

By item (3) above we have $a^{k+1} \equiv b^{k+1}$ (mod $m$). Since $c_{k+1} \equiv c_{k+1}$ (mod $m$), using item (2) above we have

(∗∗) $$c_{k+1}a^{k+1} \equiv c_{k+1}\, b^{k+1} \text{ (mod } m).$$

Now

$c_{k+1}\, a^{k+1} + c_k a^k + \cdots + c_0 \equiv c_{k+1}\, b^{k+1} + c_k b^k + \cdots + c_0$ (mod $m$).

So by induction the result holds for all $n \geq 0$.

**Example** (From [1].) The first five Fermat numbers 3, 5, 17, 257, and65, 537 are prime.

We will use congruences to show that $F5 = 2^{32} + 1$ is divisibleby 641 and is therefore not prime.

Everyone knows that $2^2 = 4$, $2^4 = 16$, and $2^8 = 256$.

Also, $2^{16} = (2^8)^2 = 256^2 = 65, 536$.

A straightforward division shows that

$$65, 536 \equiv 154 \text{ (mod 641)}.$$

Next, for 232, we have that

$$(216)^2 \equiv (154)^2 \text{ (mod 641)}.$$

That is, $2^{32} \equiv 23, 716$ (mod 641).

Since an easy division finds that 23,

716 ≡ 640 (mod 641),

and 640 ≡ −1 (mod 641),

we have that $2^{32} \equiv -1$ (mod 641).

Hence

$$2^{32} + 1 \equiv 0 \text{(mod 641), and}$$

so

$641 \mid 2^{32} + 1$, as claimed.

Clearly $2^{32} + 1 \neq 641$, so $2^{32} + 1$is composite.

The work done here did not require us to find the value of $2^{32} + 1 = 4, 294,$

967, 297 and divide it by 641; instead the calculations were with muchsmaller numbers.

**Example:** *Compute the least positive residue mod* 7 *of* $2^{37}$. *We compute powers*, $2^2 \equiv 4$

$2^4 \equiv 4^2 \equiv 2$

$2^8 \equiv 2^2 \equiv 4$

$2^{16} \equiv 4^2 \equiv 2$

$2^{32} \equiv 2^2 \equiv 4$

*Thus* $2^{37} = 2^{32} \cdot 2^4 \cdot 2^1 = 4 \cdot 2 \cdot 2 \equiv 2 \bmod 7$.

## 5.1.6 Theorem

If $ca = cb \pmod{n}$, then $a = b \pmod{n/d}$, 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 displayedequation and the common factor $d$ canceled, the net result is

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

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

Theorem 5.1.6 gets its maximum force when the requirement that gcd(c, n) = **1**isadded, for then the cancellation may be accomplished without a change in modulus.

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

**Corollary 2.** If $ca = cb \pmod{p}$ and $p \mid c$, where $p$ is a prime number, then $a \equiv b \pmod{p}$.

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

**Check Your Progress 1**

1. Explain the concept of congruence.

2. State any 4 properties of congruence

# 5.3 MORE PROPERTIES OF CONGRUENCES

## 5.3.1 Definition

Let a be an integer. The set a = {x ∈ Z | x ≡ a (mod m)} of all integers that are congruent modulo m to a is called a residue class, or congruence class, modulo m.

Since the congruence relation is an equivalence relation, it follows that all numbers belonging to the same residue class are mutually congruent, that numbers belonging to different residue classes are incongruent, that given two integers a and b either a = b or a ∩ b = ∅, and that a = b if and only if a ≡ b (mod m).

## 5.2.2 Proposition

There are exactly m distinct residue classes modulo m, viz.$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m - 1}$.

**Proof.** According to the division algorithm, there is for each integer a a unique integer rbelonging to the interval [0, m − 1] such that a ≡ r (mod m). Thus, each residue class a isidentical with one of the residue classes$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m - 1}$., and these are different since i ≢j (mod m) if 0 ≤ i < j ≤ m − 1.

## 5.2.3 Definition

Chose a number $x_i$ from each residue class modulo m. The resulting set of numbers $x_1$, $x_2$, . . . , $x_m$ is called a complete residue system modulo m. The set {0, 1, 2, . . . , m−1} is an example of a complete residue system modulo m. Example 2 {4, −7, 14, 7} is a complete residue system modulo 4.

## Lemma

If x and y belong to the same residue class modulo m, then (x, m) = (y, m). **Proof**. If x ≡ y (mod m), then x = y + qm for some integer q, and it follows that (x, m) = (y, m).

Two numbers a and b give rise to the same residue class modulo m, i.e. a = b, if and only if a ≡ b (mod m). The following definition is therefore consistent by virtue of Lemma 5.2.4

## 5.2.4 Definition

A residue class a modulo m is said to be relatively prime to m if (a, m) = 1.

## 5.2.5 Definition

Let φ(m) denote the number of residue classes modulo m that are relatively prime to m. The function φ is called Euler’s φ-function. Any set {r1, r2, . . . , rφ(m)} of integers obtained by choosing one integer from each of the residue classes that are relatively prime to m, is called a reduced residue system modulo m.

The following two observations are immediate consequences of the definitions: The number φ(m) equals the number of integers in the interval [0, m − 1] that are relatively prime to m. {y1, y2, . . . , yφ(m)} is a reduced residue system modulo m if and only if the numbers are pairwise incongruent modulo m and (yi , m) = 1 for all i.

**Example:** The positive integers less than 8 that are relatively prime to 8 are 1, 3, 5, and 7. It follows that φ(8) = 4 and that {1, 3, 5, 7} is a reduced residue system modulo 8.

**Example:**If p is a prime, then the numbers 1, 2, . . . , p − 1 are all relatively prime to p. It follows that φ(p) = p − 1 and that {1, 2, . . . , p − 1} is a reduced residue system modulo p.

## 5.2.6 Theorem

Let (a, m) = 1. Let {r1, r2, . . . , rm} be a complete residue system, and let {s1, s2, . . . , sφ(m)} be a reduced residue system modulo m. Then {ar1, ar2, . . . , arm} is a complete and {as1, as2, . . . , asφ(m)} is a reduced residue system modulo m. Proof. In order to show that the set {$ar_1$, $ar_2$, . . . , $ar_m$} is a complete residue system, we just have to check that the elements are chosen from distinct residue classes, i.e. that i 6= j ⇒ ari 6≡ arj (mod m).

But by properties of congruence, ari ≡ arj (mod m) implies ri ≡ rj (mod m) and hence i = j. Since (si , m) = 1 and (a, m) = 1, we have (asi , m) = 1 for i = 1, 2, . . . , φ(m) Hence as1, as2, . . . , asφ(m) are φ(m) numbers belonging to residue classes that are relatively prime to m, and by the same argument as above they are chosen from distinct residue classes. It follows that they form a reduced residue system.

## 5.2.7 Theorem

Let $m \geq 2$. If $a$ and $m$ are relatively prime then there existsa unique integer $a*$such that $aa* \equiv 1 \pmod{m}$ and $0 < a* < m$.

**Proof**. Assume that gcd($a$, $m$) = 1. Bezout's Lemma applies to give an $s$ and$t$ such that

$$as + mt = 1.$$

Hence $as - 1 = m(-t)$, that is, $m \mid as - 1$ and so

$$as \equiv 1 \pmod{m}.$$

Accordingly, let $a* = s \bmod m$ so that $0 < a* < m$.

Then

$$a* \equiv s \pmod{m} \text{ so } aa* \equiv 1 \pmod{m}.$$

To show uniqueness, assume that $ac \equiv 1 \pmod{m}$ and $0 < c < m$.

Then

$$ac \equiv aa* \pmod{m}.$$

Multiply both sides of this congruence on the left by $c$ anduse the fact that $ca \equiv 1 \pmod{m}$ to obtain $c \equiv a* \pmod{m}$. Because both arein [0 .. $m$), it follows that $c = a*$. qed

We call $a*$the *inverse* of $a$ modulo $m$.

Note that we do not denote $a*$by$a^{-1}$ here since we keep that symbol for the usual meaning of inverse.

**Remark** The proof shows that Blankinship's Method will compute theinverse of $a$, when it exists. But for small $m$ we may find $a*$by trial and error.

**For example,** take $m = 15$ and $a = 2$.

We can check each possibility: $2 \cdot 0 \not\equiv 1 \pmod{15}$,

$2 \cdot 1 \not\equiv 1 \pmod{15}$, . . . ,

$2 \cdot 8 \equiv 1 \pmod{15}$.

So we can take $2* = 8$.

Note that we may well have $ca \equiv 1 \bmod m$ with $c \neq a$ if $c \equiv a* \pmod{m}$and $c > m$ or $c < 0$.

For instance, $8 \cdot 2 \equiv 1 \bmod 15$ and also $23 \cdot 2 \equiv 1 \bmod 15$.

So the inverse is unique only if we specify that $0 < a* < m$.

The converse of Theorem 5.2.1 holds.

## 5.2.8 Theorem

Let $m > 0$. If $ab \equiv 1 \pmod{m}$ then both $a$ and $b$ are relativelyprime to $m$.

Proof. If $ab \equiv 1 \pmod{m}$, then $m \mid ab - 1$. So $ab - 1 = mt$ for some $t$.

Hence,

$ab + m(-t) = 1$.

The proof of Bezout's Lemma, Lemma 5.3, shows that gcd($a$, $m$) is the smallest positive linear combination of $a$ and $m$. The last paragraph shows thatthere is a combination that adds to 1. Since no combination can be positiveand smaller than 1, we have that gcd($a$, $m$) = 1. The case of gcd($b$, $m$) issimilar.

## Corollary

A number $a$ has an inverse modulo $m$ if and only if $a$ and $m$are relatively prime.

## 5.2.11 Theorem (Cancellation)

Let $m > 0$. If gcd($c$, $m$) = 1 then $ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m}$.

Proof. If gcd($c$, $m$) = 1 then it has an inverse $c*$modulo $m$, such that $c*c \equiv 1 \pmod{m}$.

Since $ca \equiv cb \pmod{m}$ by Theorem 5 .1. 4 ,

$$c*ca \equiv c*cb \pmod{m}.$$

But

$$c*c \equiv 1 \pmod{m} \text{ so } c*ca \equiv a \pmod{m} \text{ and } c*cb \equiv b \pmod{m}.$$

By reflexivityand transitivity this yields $a \equiv b \pmod{m}$.

Although in general we cannot cancel if gcd($c$, $m$) >1, the next result issome consolation.

## 5.2.12 Theorem

If $c > 0$ and $m > 0$ then $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{cm}$.

**Proof.**The congruence $a \equiv b \pmod{m}$ is true if and only if $m \mid (a - b)$ holds, which in turn holds if and only if $cm \mid (ca - cb)$.

## 5.2.13 Theorem

Fix $m > 0$ and let $d = \gcd(c, m)$.
Then $ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m/d}$.

**Proof**. Since $d = \gcd(c, m)$, the equations $c = d(c/d)$ and $m = d(m/d)$ involveintegers.
Rewriting $ca \equiv cb \pmod{m}$ gives

$$d\left(\frac{c}{d}\right) a \equiv d\left(\frac{c}{d}\right) b \pmod{d\left(\frac{m}{d}\right)}.$$

By Theorem 5.2.5 we have

$$\left(\frac{c}{d}\right) a \equiv \left(\frac{c}{d}\right) b \pmod{\frac{m}{d}}.$$

Since $d = \gcd(c, m)$, we have that $\gcd(c/d, m/d) = 1$ and so by cancellation,Theorem 5.2.4,
$a \equiv b \pmod{m/d}$.

## 5.2.14 Theorem

If $m > 0$ and $a \equiv b \pmod{m}$ then $\gcd(a, m) = \gcd(b, m)$.

**Proof**. Let $d_a = \gcd(m, a)$ and $d_b = \gcd(m, b)$. Since $a \equiv b \pmod{m}$ we have $a - b = mt$ for some $t$. Rewrite that as $a = mt + b$ and note that $d_b \mid m$ and $d_b \mid b$, so $d_b \mid a$. Thus, $d_b$ is a common divisor of $m$ and $a$, and so $d_b \leq d_a$.

Asimilar argument gives that $d_a \leq d_b$, and therefore $db = da$.

### Corollary

Fix $m > 0$. If $a \equiv b \pmod m$ then $a$ has an inverse modulo$m$ if and only if $b$ does also.

**Check Your Progress 2**

1. What do you understand by residue class and complete residue system

______________________________

______________________________

______________________________

2. Explain reduced residue system with example

______________________________

______________________________

## 5.3 LINEAR CONGRUENCE

### 5.3.1 Definition

The congruence

(1) $ax \equiv b \pmod m$

is equivalent to the equation

(2) $ax - my = b$

where we of course only consider integral solutions x and y. We know from Theorem 3.1 that this equation is solvable if and only if $d = (a, m)$ divides b, and if $x_0$, $y_0$ is a solution then the complete set of solution is given by

$$x = x_0 + \frac{m}{d}n, \quad y = y_0 + \frac{a}{d}n.$$

We get d pairwise incongruent x-values modulo m by taking n = 0, 1, . . . , d−1, and any solution x is congruent to one of these. This proves the following theorem.

## 5.3.1 Theorem

The congruence

$$ax \equiv b \pmod{m}$$

is solvable if and only if (a, m) | b. If the congruence is solvable, then it has exactly (a, m) pairwise incongruent solutions modulo m.

## Corollary

The congruene $ax \equiv 1 \pmod{m}$ is solvable if and only if (a, m) = 1, and in this case any two solutions are congruent modulo m.

## Corollary

If (a, m) = 1, then the congruence $ax \equiv b \pmod{m}$ is solvable for any b and any two solutions are congruent modulo m.

In (1) we can replace the numbers a and b with congruent numbers in the interval [0, m − 1], or still better in the interval [−m/2, m/2]. Assuming this done, we can now write equation (2) as

$$my \equiv -b \pmod{a} \qquad (1)$$

with a module a that is less than the module m in (1). If y = y0 solves (3), then

$$x = \frac{my_0 + b}{a}$$

is a solution to (1).

**Example**Solve the congruence

(4) $296x \equiv 176 \pmod{114}$.

Solution: Since 2 divides the numbers 296, 176, and 114, we start by replacing (4) with the following equivalent congruence:

(5) $148x \equiv 88 \pmod{57}$.

Now, reduce 148 and 88 modulo 57. Since $148 \equiv -23$ and $88 \equiv -26$, we can replace (5) with

(6) $23x \equiv 26 \pmod{57}$.

Now we consider instead the congruence $57y \equiv -26 \pmod{23}$, which of course is quivalent to

(7) $11y \equiv -3 \pmod{23}$.

Again, replace this with the congruence $23z \equiv 3 \pmod{11}$ which is at once reduced to $z \equiv 3 \pmod{11}$.

Using this solution, we see that

$$y = \frac{23 \cdot 3 - 3}{11} = 6$$

is a solution to (7) and that all solutions have the form $y \equiv 6 \pmod{23}$. It now follows that

$$x = \frac{57 \cdot 6 + 26}{23} = 16$$

solves (6) and the equivalent congruence (4), and that all solutions are of the form $x \equiv 16 \pmod{57}$, which can of course also be written as $x \equiv 16, 73 \pmod{114}$.

## 5.4 SOLVED EXAMPLES

**Example:** Solve the congruence $x^5 \equiv 9 \pmod{23}$.

Notes

Solution: First, let us note that 23 = 5 · 4 + 3. Therefore $l$ = 4 andwe get $x^2 \equiv 9^{-4}$ (mod 43). Since $9^4 \equiv 6$ (mod 23) and $6^{-1} \equiv 4$ (mod 23), we obtain the congruence $x^2 \equiv 4$ (mod 23) with the solutions 2 or 21. It is easy to check that 2 is the only solution of the given congruence.

**Example.** Solve the congruence $x^{10} \equiv 35$ (mod 43).

**Solution:** We have 43 = 10 · 4 + 3. Since g.c.d. (10, 42) = 2 and $35^{21} \equiv 1$ (mod 43), the given congruence has two solutions. Both solutions of the quadratic congruence, to which the given congruence will be reduced, are the solutions of the given congruence. It is easy to follow the chain of formulas:

$$x^{40} \equiv 11 \pmod{43},$$
$$x^{42} \equiv 11x^2 \pmod{43},$$
$$11x^2 \equiv 1 \pmod{43},$$
$$x^2 \equiv 4 \pmod{43},$$
$$x \equiv 2 \pmod{43}$$

or

$$x \equiv 41 \pmod{43}.$$

Both 2 and 41 are the solutions of the given congruence.

## 5.5 SUMMARY

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.

## 5.6 KEYWORDS

1. **Argument:**an argument of a function is a value that must be provided to obtain the function's result.

**2. Inverse :**an inverse operation is an operation that undoes what was done by the previous operation

**3. A combination** is a mathematical technique that determines the number of possible arrangements in a collection of items where the order of the selection does not matter.

**4. Consistent :** In mathematics and in particular in algebra, a linear or nonlinear system of equations is consistent if there is at least one set of values for the unknowns that satisfies every equation in the system

**5. Unique** - Unique means that a variable, number, value, or element is one of a kind and the only one that can satisfy the conditions of a given statement.

# 5.7 QUESTIONS FOR REVIEW

1. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a = b$ (modn).
2. Use the theory of congruences to verify that $89 \mid 2^{44} - 1$
3. Establish that if $a$ is an odd integer, then for any $n \geq 1$
   $a^{2^n} = 1 \pmod{2^{n+2}}$
4. Establish that if $a$ is an odd integer, then for any $n \geq 1$

$$a^{2^n} \equiv 1 \ (mod\ 2^{n+2})$$

# 5.8 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.
9. M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer.

## 5.9 ANSWERS TO CHECK YOUR PROGRESS

1. .[HINT: Provide definition ,representation and example—5.1.1]
2. [HINT: Provide statement of 4 properties with proof—either 5.1.4 or 5.1.5]
3. [HINT: Provide definition, example with explananation and also provide one related theorem and proof—5.2.1 ,5.2.2]
4. [HINT: Provide definition and explain with the help of theorem – 5.2.6 & 5.2.7]

# UNIT 6: CONGRUENCE

## STRUCTURE



# 6.0 OBJECTIVE

Understand the binary and Decimal representation of integers

Enumerate the Chinese remainder theorem

# 6.1 BINARY AND DECIMAL REPRESENTATIONS OF INTEGERS

Given an integer $b > 1$, any positive integer $N$ can be written uniquely in terms of powers of $b$ as

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

where the coefficients $ak$ can take on the $b$ different values 0, 1, 2, ... , $b$- 1.

For the Division Algorithm yields integers $q_1$ and $a_0$ satisfying

$$N = q_1 b + a_0 \qquad 0 \le a_0 < b$$

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

$$q_1 = q_2 b + a_1 \qquad 0 \le a_1 < b$$

Now substitute for $q_1$ in the earlier equation to get

$$N = (q_2 b + a_1)b + a_o = q_2 b_2 + a_1 b + a_o$$

As long as $q_2 \ge b$, we can continue in the same fashion.

Going one more step:

$q_2 = q_3 b + a_2$, where $0 \le a_2 < b$; hence

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

Because $N > q_1 > q_2 > \cdot \cdot \cdot \ge 0$ is a strictly decreasing sequence of integers, thisprocess must eventually terminate, say, at the $(m$ - 1)th stage, where

$q_{m-1} = q_m b + a_{m-1} \qquad 0 \le a_{m-1} < b$

nd $0 \le qm < b$. Setting $a_m = q_m$, we reach the representation

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

which was our aim.

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

$$N = a_m b^m + \ldots + a_1 b + a_o = C_m b_m + \ldots + c_1 b + c_o$$

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

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

where $d_i = a_i - c$; fori = 0, 1, ... , $m$. Because the two representations for $N$ areassumed to be different, we must have $d_i \ne 0$ for some value of $i$. Take $k$ to be thesmallest subscript for which $d_k \ne 0$. Then

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

and so, after dividing by $b^k$,

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

This tells us that $b|d_k$. Now the inequalities $0 \leq ak <$ band $0 \leq ck < b$ lead us to$-b < a_k - c_k < b$, or $|d_k| < b$. The only way of reconciling 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 determinedby the ordered array $a_m, a_{m-1} \ldots , a_,, a_o$of coefficients, with the plus signs and thepowers of $b$ beingsuperfluous. Thus, the number

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

may be replaced by the simpler symbol(the right-hand side is not to be interpreted as a product, but only as an abbreviationfor N). We call this the *base b place-value notation for N.*

**Example:** Calculate $5^{110}$ (mod 131), first note that the exponent 110 can beexpressed in binary form as

$110 = 64 + 32 + 8 + 4 + 2 = (110110)_2$

Thus, we obtain the powers$5^{2^j}$(mod 131) for $0 \leq j \leq 6$ by repeatedly squaring whileat each stage reducing each result modulo 131:

$5^2 \equiv 25$ (mod 131)

$5^4 \equiv 101$ (mod 131)

$5^8 \equiv 114$ (mod 131)

$5^{16} \equiv 27$ (mod 131)

$5^{32} \equiv 74$ (mod 131)

$5^{64} \equiv 105$ (mod 131)

When the appropriate partial results-those corresponding to the 1's in the binaryexpansion of 110---are multiplied, we see that

$5^{110} = 5^{64+32+8+4+2}$

$= 5^{64} . 5^{32} . 5^8 .5^4 . 5^2$

$=105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60$ (mod 131)

Notes

As a minorvariation ofthe procedure, one might calculate, modulo 131, the powers

$5, 5^2, 5^3, 5^6, 5^{12}, 5^{24}, 5^{48}, 5^{96}$ to arrive at

$5^{110} = 5^{96} \cdot 5^{12} \cdot 5^2 \equiv 41 \cdot 117 \cdot 25 \equiv 60 \pmod{131}$

which would require two fewer multiplications.

**Example:**Find the expansion of 214 base 3:

Solution:

$214 = 3 \cdot 71 + 1$

$71 = 3 \cdot 23 + 2$

$23 = 3 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$

$2 = 3 \cdot 0 + 2$

As a result, to obtain a base 3 expansion of 214, we take the remainders of divisions and we get that

$(214)_{10} = (21221)_3$

## 6.1.1 Theorem

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

***Proof.***Because $a = b \pmod{n}$, can be applied to give$a_k = b_k \pmod{n}$ *for*$k = 0, 1, \ldots, m$. Therefore,

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

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, $P(a) = P(b) \pmod{n}$.

If *P(x)* is a polynomial with integral coefficients, we say that *a* is a solution ofthe congruence *P(x)* =0 (mod *n)* if *P(a)* =0 (mod *n).*

## Corollary

If *a* is a solution of *P(x)* = 0 (mod *n)* and *a*= *b* (mod *n)*, then *b* also is asolution.

***Proof.***From the last theorem, it is known that *P(a)* = *P(b)* (mod *n).* Hence, if *a* is asolution of *P(x)* = 0 (mod *n)*, then *P(b)* = *P(a)* = 0 (mod *n)*, making *b* a solution.

## 6.1.2 Theorem

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*, $0 \leq ak < 10$, and let$S = a_0 + a_1 + \cdots + a_m$. Then9 |*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 keyobservation is that 10 = 1 (mod 9), whence by Theorem 6.1.1, $P(10) \equiv P(1)$ (mod 9).
But P(10) = *N* and $P(1) = a_0 + a_1 + \cdots + a_m = S$, so that $N \equiv S$ (mod 9). It follows that $N \equiv 0$ (mod 9) if and only if $S \equiv 0$ (mod 9), which is what we wanted toprove.

## 6.1.3 Theorem

Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$be the decimal expansion of thepositive integer *N*, $0 \leq a_k < 10$, and let $T = a_0 - a_1 + a_2 - \ldots + (-1)^m a_m$. Then 11|*N* if and only if 11|*T*.
***Proof.***As in the proof of Theorem 6.1.3, put $P(x) = \sum_{k=0}^{m} a_k x^k$. Because 10 = - 1(mod 11), we get P(10) = *P(*-1) (mod 11). But P (10) = *N*, whereas *P(*-1)

Notes

$= a_0 - a_1 + a_2 - \ldots + (-1)^m a_m = T$, so that $N = T$ (mod 11). The implication is thateither both $N$ and $T$ are divisible by 11 or neither isdivisible by 11.

**Example.** To see an illustration of the last two results, take the integer $N$ =1,571,724. Because the sum1 + 5 + 7 + 1 + 7 + 2 + 4 = 27is divisible by 9, Theorem 6.1.3 guarantees that 9 divides $N$. It also can be divided by11; for, the alternating sum4-2+7-1+7-5+1=11is divisible by 11.

**Check Your Progress1**

1.What is *base b place-value notation?*

---

---

---

*2.* Explain the concept of decimal expansion of the positive integer.

---

---

---

# 6.2 THE CHINESE REMAINDER THEOREM

## 6.2.1 Definition

A *linear congruence* has the form $ax \equiv b \pmod{n}$ where $x$ isa variable.

**Example** The linear congruence $2x \equiv 1 \pmod{3}$ is solved by $x$ =2 because $2 \cdot 2 = 4 \equiv 1 \pmod{3}$. The solution set of that congruence is$\{\ldots, 2, 5, 8, 11, \ldots\}$.

**Example** The congruence $4x \equiv 1 \pmod{2}$ has no solution, because $4x$ is even, and so is not congruent to 1, modulo 2.

## Lemma

Fix a modulus $m$ and a number $a$. The congruence $ax \equiv b(\text{mod } m)$ has a solution if an only if $\gcd(a, m) \mid b$. If a solution $x_0$ does existthen, where $d = \gcd(a, b)$, the set of solutions is$\{. . . , x_0 + (-m/d), x_0, x_0 + (m/d), x_0+ (2m/d), x_0 + (3m/d), . . . \}$the residue class $[x_0]$ modulo $m/d$.

Proof. The existence of an $x$ solving $ax \equiv b \pmod m$ is equivalent to theexistence of a $k$ such that $ax - b = km$, which in turn is equivalent to theequivalence of a $k$ such that $xa + (-k)m = b$.

**Lemma** If gcd $(a, b) = 1$ and $c$ is a number such that $a \mid c$ and $b \mid c$ then$ab \mid c$

**Proof**. Because $a \mid c$ and $b \mid c$ there are numbers $k_a$, $k_b$ such that $k_a a = c$ and$k_b b = c$.By Bezout's Lemma, there are $s$ and $t$ such that $as + bt = 1$. Multiplyby $c$ to get $cas + cbt = c$. Substitution gives $(k_b b)as + (k_a a)bt = c$. Then $ab$divides the left side of the equation and so $ab$ must divide the right side, $c$.

## 6.2.2 Theorem (Chinese Remainder Theorem)

Suppose that $m_1, . . . , m_n$are pairwiserelatively prime (that is, $\gcd(m_i, m_j) = 1$ whenever $i \neq j$). Thenthe system of congruences

$$x \equiv a1 \pmod{m1}$$
$$x \equiv a2 \pmod{m2}$$
$$.$$
$$.$$
$$.$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m_1m_2. . . m_n$.

Proof. Let $M = m_1m_2. . . m_n$and for $i \in \{1, . . . , n\}$ let $M_i= M/m_i=m_1m_2. . . m_{i-i}m_{i+1}. . . m_n$.

Observe that $\gcd(M_i, m_i) = 1$ and so Lemma 6.2.2 says that the linear congruence

$M_ix \equiv 1 \pmod{mi}$ has a set of solutions thatis a single congruence class $[xi]$ modulo $mi$.

Now consider the number

$$s_0 = a_1M_1x_1 + a_2M_2x_2 + \cdots + a_nM_nx_n.$$

We claim that $s_0$ solves the system. For, consider the $i$-th congruence $x \equiv ai \pmod{mi}$.

Because $m_i$ divides $M_j$when $i \neq j$, we have that $s_0 \equiv a_iM_ix_i \pmod{mi}$. Since $x_i$was chosenbecause of the property that $M_ix_i \equiv 1 \pmod{m_i}$,we have that $s_0 \equiv a_i \cdot 1 \equiv a_i \pmod{m_i}$, as claimed.

To finish we must show that the solution is unique modulo $M$. Suppose that$x$ also solves the system, so that for each $i \in \{1, . . . , n\}$ we have that $x \equiv a_i \equiv x_0 \pmod{mi}$.

Restated, for each $i$ we have that $n_i \mid (x - x_0)$.

We can now show that $m_1m_2 . . . m_n \mid (x-x_0)$. We have that $\gcd(m_1, m_2) =1$ and $m1 \mid (x - x_0)$ and $m2 \mid (x - x_0)$, so the prior lemma applies and weconclude that $m_1m_2 \mid (x - x_0)$. In this way, we can build up to the entireproduct $m_1 . . . m_n$.

**Example:** First consider the linear congruence 18x = 30 (mod 42). Becausegcd (18, 42) = 6 and 6 surely divides 30, concept of linear congruence guarantees the existence ofexactly sixsolutions, which are incongruent modulo 42. By inspection, one solutionis found to be $x = 4$. Our analysis tells us that the six solutions are as follows:

$x = 4 + (42/6)t = 4 + 7t \pmod{42}$ $\qquad t = 0, 1, ... , 5$

or, plainly enumerated,

$x =4, 11, 18, 25, 32, 39 \pmod{42}$

**Example:**The problem posed by Sun-Tsu corresponds to the system of threecongruences

$x = 2 \pmod 3$

$x = 3 \pmod 5$

$x = 2 \pmod 7$

In the notation of Theorem 6.2.4, we have $n = 3 \cdot 5 \cdot 7 = 105$ and

$$N_1 = \frac{n}{3} = 35$$

$$N_2 = \frac{n}{5} = 21$$

$$N_3 = \frac{n}{7} = 15$$

Now the linear congruences

$35x = 1 \pmod 3$ $\quad$ $21x = 1 \pmod 5$ $\quad$ $15x = 1 \pmod 7$

are satisfied by $x_1 = 2$, $x_2 = 1$, $x_3 = 1$, respectively. Thus, a solution of the system isgiven by

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

Modulo 105, we get the unique solution $x = 233 = 23 \pmod{105}$.

Example: Solve the linear congruence$17x = 9 \pmod{276}$

Because $276 = 3 \cdot 4 \cdot 23$, this is equivalent to finding a solution for the system ofcongruences

$17x \equiv 9 \pmod 3$

$17x \equiv 9 \pmod 4$

$17x \equiv 9 \pmod{23}$

or $x \equiv 0 \pmod 3$

$x \equiv 1 \pmod 4$

$17x = 9 \pmod{23}$

Note that if $x = 0 \pmod 3$, then $x = 3k$ for any integer $k$. We substitute into the secondcongruence of the system and obtain

$$3k \equiv 1 \pmod 4$$

Multiplication of both sides of this congruence by 3 gives us$k \equiv 9k \equiv 3 \pmod 4$

so that $k = 3 + 4j$, where $j$ is an integer. Then

$$x = 3(3 + 4j) = 9 + 12j$$

For $x$ to satisfy the last congruence, we must have

$$17(9 + 12j) \equiv 9 \pmod{23}$$

or$204j \equiv -144 \pmod{23}$, which reduces to $3j \equiv 6 \pmod{23}$; in consequence, $j \equiv 2 \pmod{23}$. This yields $j \equiv 2 + 23t$, with $t$ an integer, where

$$x = 9 + 12(2 + 23t) = 33 + 276t$$

All in all, $x \equiv 33 \pmod{276}$ provides a solution to the system of congruences and, intum, a solution to $17x \equiv 9 \pmod{276}$

## 6.2.3 Theorem

The system of linear congruences

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

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

has a unique solution modulo $n$ whenever $gcd(ad - be, n) = 1$.

***Proof***. Let us multiply the first congruence of the system by $d$, the second congruenceby $b$, and subtract the lower result from the upper. These calculations yield

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

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

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

posseses a unique solution; denote the solution by $t$. When congruence (1) is multipliedby $t$, we obtain

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

A value for $y$ is found by a similar elimination process. That is, multiply the firstcongruence ofthe system by $c$, the second one by $a$, and subtract to end up with

$$(ad - bc)y \equiv as - cr \pmod{n}$$

Multiplication of this congruence by *t* leads to

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

A solution of the system is now established.

**Example.** Consider the system

$$7x + 3y \equiv 10 \pmod{16}$$

$$2x + 5y \equiv 9 \pmod{16}$$

Because gcd(7 · 5 - 2 ·3, 16) = gcd(29, 16) = 1, a solution exists. It is obtained bythe method developed in the proof of Theorem 6.2.5. Multiplying the first congruenceby 5, the second one by 3, and subtracting, we arrive at

$$29x \equiv 5 \cdot 10 - 3 \cdot 9 \equiv 23 \pmod{16}$$

or, what is the same thing, $13x \equiv 7 \pmod{16}$. Multiplication of this congruence by 5(noting that $5 \cdot 13 \equiv 1 \pmod{16}$) produces $x = 35 = 3 \pmod{16}$. When the variable$x$ is eliminated from the system of congruences in a like manner, it is found that

$$29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43 \pmod{16}$$

But then $13y \equiv 11 \pmod{16}$, which upon multiplication by 5, results in $y \equiv 55 \equiv 7 \pmod{16}$. The unique solution of our system turns out to be

$$x \equiv 3 (mod\ 16) \qquad y \equiv 7 (mod\ 16)$$

**Example:** Let us solve the system

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5}. \end{cases}$$

**Solution:** Using the method in our first proof of the Chinese Remainder Theorem, we replace the first congruence by $x = 1 + 3y$.
Substituting this into the second congruence we obtain

$$3y + 1 \equiv 2 \pmod{4} \text{ or } 3y \equiv 1 \pmod{4}.$$

This congruence has the solutions $y \equiv -1 \pmod{4}$, i.e. $y = -1 + 4z$.
Hence,

$$x = -2 + 12z,$$

and substituting this into the last congruence we end up in the congruence $12z - 2 \equiv 3 \pmod{5}$ or $12z \equiv 5 \equiv 0 \pmod{5}$.

This congruence has the unique solution

$$z \equiv 0 \pmod{5}, \text{ that is } z = 5t \text{ and } x = -2 + 60t.$$

Hence, the system has the unique solution $x \equiv -2 \pmod{60}$.

Solution 2: Let us instead use the method of the second proof. Then we have first to findnumbers $b_1$, $b_2$, and $b_3$ such that

$$20b_1 \equiv 1 \pmod{3},\ 15b_2 \equiv 1 \pmod{4},\ 12b_3 \equiv 1 \pmod{5}.$$

One easily obtains $b_1 = 2$, $b_2 = 3$, and $b_3 = 3$.

Next, we compute

$$\delta_1 = 20b_1 = 40,\ \delta_2 = 15b_2 = 45, \text{ and } \delta_3 = 12b_3 = 36.$$

Finally, $x = \delta_1 + 2\delta_2 + 3\delta_3 = 40 + 90 + 108 = 238 \equiv 58 \pmod{60}$.

## 6.2.4 Theorem

*If* $m = m_1m_2$, *where the integers* $m_1$ *and* $m_2$ *are relatively prime, then*

$\varphi(m) = \varphi(m_1)\varphi(m_2)$.

## Corollary

*If* $n = p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$, *where* $p_1, p_2, \ldots, p_r$ *are different primes, then*

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

*Proof.* By repeated application of Theorem 6.2, we obtain

$\varphi(m_1m_2 \cdots m_r) = \varphi(m_1)\varphi(m_2) \cdots \varphi(m_r)$

if the integers $m_1, m_2, \ldots, m_r$ are pairwise relatively prime. In particular, this

holds when the numbers *mi* are powers of distinct primes. By Example 5 in section 4, $\varphi(pk) = pk-1(p-1) = pk(1-1/p)$ if $p$ is prime.

## Definition

A polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ with coefficients $ai \in \mathbf{Z}$ is called an *integral polynomial*, and the congruence

$$f(x) \equiv 0 \pmod{m},$$

is called a *polynomial congruence*. An integer $a$ is called a solution or a *root* ofthe polynomial congruence if $f(a) \equiv 0 \pmod{m}$.

If $a$ is a root of the polynomial congruence and if $b \equiv a \pmod{m}$, then $b$ isalso a root. Therefore, in order to solve the polynomial cogruence it is enoughto find all roots that belong to a given complete residue system $C(m)$ modulo$m$, e.g. to find all solutions among the numbers $0, 1, 2, \ldots, m-1$. By *thenumber of roots* of a polynomial congruence we will mean the number of such incongruent roots.

Consider a system

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ f_2(x) \equiv 0 \pmod{m_2} \\ \quad\vdots \\ f_r(x) \equiv 0 \pmod{m_r} \end{cases}$$

of polynomial congruences, where the moduli $m_1, m_2, \ldots, m_r$are assumed to bepairwiserelatively prime. By a solution of such a system we mean, of course,an integer which solves simultaneously all the congruences of the system. If $a$is a solution of the system, and if $b \equiv a \pmod{m_1 m_2 \cdots m_r}$, then $b$ is also asolution of the system, since for each $j$ we have $b \equiv a \pmod{m_j}$. Hence, tofind all solutions of the system it suffices to consider solutions belonging to a complete residue system modulo $m_1m_2 \cdots m_r$; by the number of solutions of thesystem we will mean the number of such incongruent solutions.

**Theorem 6.2.9***Let*

$$(5) \qquad \begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ f_2(x) \equiv 0 \pmod{m_2} \\ \vdots \\ f_r(x) \equiv 0 \pmod{m_r} \end{cases}$$

be a system of polynomial congruences, and assume that the the moduli m1, m2,..., mr are pairwise relatively prime. Let Xj be a complete set of incongruentsolutions modulo mj of the jth congruence, and let nj denote the number ofsolutions. The number of solutions of the system then equals $n_1n_2 \cdots n_r$, andeach solution of the system is obtained as the solution of the system

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

with (a1, a2, . . . , ar) ranging over the set X1 × X2 × · · · × Xr.Of course, a set Xj might be empty in which case nj = 0

**Proof**. Write m = m1m2 · · · mr, let C(mj) be a complete residue system modulomj containing the solution set Xj (j = 1, 2, . . . , r), and let C(m) be a completeresidue system modulo m containing the solution set X of the system (5) ofcongruences. By the Chinese Remainder Theorem we obtain a bijection

$$\tau : C(m) \to C(m1) \times C(m2) \times \cdots \times C(mr)$$

by defining

$$\tau(x) = (x1, x2, \ldots, xr),$$

where each $x_j \in C(m_j)$ is a number satisfying the congruence $x_j \equiv x$ (mod $m_j$).If $a \in X$, then $a$ is a solution of each individual congruence in the system (5).Consequently, if $a_j \in C(m_j)$ and $a_j \equiv a$ (mod $m_j$), then $a_j$ is a solution of the$j$th congruence of the system, i.e. $a_j$ belongs to the solution set $X_j$. We concludethat $\tau(a) = (a_1, a_2, \ldots, a_r)$ belongs to the set $X_1 \times X_2 \times \cdots \times X_r$ for each $a \in X$,and the image $\tau(X)$ of $X$ under $\tau$ is thus a subset of $X_1 \times X_2 \times \cdots \times X_r$.Conversely, if $\tau(a) = (a_1, a_2, \ldots, a_r) \in X_1 \times X_2 \times \cdots \times X_r$, then $a$ solves eachindividual congruence and thus belongs to $X$. As $a \equiv a_j$ (mod $m_j$) and $f_j(a_j) \equiv 0$ (mod $m_j$) for each $j$. Hence,the bijection $\tau$ maps the subset $X$ onto the subset $X_1 \times X_2 \times \cdots \times X_r$, and weconclude that the number of elements in $X$ equals $n_1 n_2 \cdots n_r$.

**Example:** Consider the system

$$\begin{cases} x^2 + x + 1 \equiv 0 \pmod 7 \\ 2x - 4 \equiv 0 \pmod 6. \end{cases}$$

By trying $x = 0, \pm 1, \pm 2, \pm 3$, we find that $x \equiv 2$ (mod 7) and $x \equiv -3$ (mod 7)are the solutions of the first congruence. Similarly, we find that $x \equiv -1$ (mod 6)and $x \equiv 2$ (mod 6) solve the second congruence. We conclude that the systemhas 4 incongruent solutions modulo 42. To find these, we have to solve each ofthe following four systems:

$$\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv -1 \pmod 6 \end{cases} \qquad \begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 2 \pmod 6 \end{cases}$$

$$\begin{cases} x \equiv -3 \pmod 7 \\ x \equiv -1 \pmod 6 \end{cases} \qquad \begin{cases} x \equiv -3 \pmod 7 \\ x \equiv 2 \pmod 6. \end{cases}$$

We use the solution formula (4) obtained in the proof of the Chinese RemainderTheorem. Thus, we determine $b_1$ and $b_2$ such that

$\frac{42}{7} b_1 \equiv 1$ (mod 7) and $\frac{42}{7} b_2 \equiv 1$ (mod 6).

We easily find that $b_1 = -1$ and $b_2 = 1$ solve these congruences, and hence we can take $\delta_1 = -6$ and $\delta_2 = 7$. We conclude that four different solutions modulo 42 of our original system are

$$x_1 = -6 \cdot 2 + 7 \cdot (-1) = -19 \equiv 23$$
$$x_2 = -6 \cdot 2 + 7 \cdot 2 = 2$$
$$x_3 = -6 \cdot (-3) + 7 \cdot (-1) = 11$$
$$x_4 = -6 \cdot (-3) + 7 \cdot 2 = 32.$$

## 6.2.5 Theorem

*Let $f(x)$ be an integral polynomial. For each positive integer $m$, let $X(m)$ denote a complete set of roots modulo $m$ of the polynomial congruence $f(x) \equiv 0 \pmod{m}$,*

*and let $N(m)$ denote the number of roots.*

*Assume $m = m_1m_2 \cdots m_r$, where the numbers $m_1, m_2, \ldots, m_r$ are pairwise relatively prime; then*

$N(m) = N(m1)N(m2) \cdots N(mr)$.

*Moreover, to each r-tuple $(a1, a2, \ldots, ar) \in X(m1)\times X(m2)\times \cdots \times X(mr)$ there*

*corresponds a unique solution $a \in X(m)$ such that $a \equiv aj \pmod{mj}$ for each $j$.*

***Proof.*** The congruence $f(x) \equiv 0 \pmod{m}$ is equivalent to the system

$$\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \\ \quad\vdots \\ f(x) \equiv 0 \pmod{m_r}. \end{cases}$$

Hence, Theorem 6.2.9 applies. It follows that in order to solve a polynomial congruence modulo $m$ it is sufficient to know how to solve congruences with prime power moduli.

**Example** Let $f(x) = x2 + x + 1$. Prove that the congruence $f(x) \equiv 0 \pmod{15}$ has no solutions.

***Solution:*** By trying the values $x = 0, \pm 1, \pm 2$ we find that the congruence $f(x) \equiv 0 \pmod{5}$ has no solutions. Therefore, the given congruence modulo 15 (= $5 \cdot 3$) has no solutions.

**Example**: Let $f(x) = x2 + x + 9$. Find the roots of the congruence $f(x) \equiv 0 \pmod{63}$.

***Solution****:* Since $63 = 7 \cdot 9$, we start by solving the two congruences

$$f(x) \equiv 0 \pmod{7} \text{ and } f(x) \equiv 0 \pmod{9}.$$

The first congruence has the sole root 3 (mod 7), and the second congruence has the roots 0 and −1 (mod 9). It follows that the given congruence has two roots modulo 63, and they are obtained by solving the congruences

$$x \equiv 3 \pmod{7} \qquad \text{and } x \equiv -3 \pmod{7}$$
$$x \equiv 0 \pmod{9} \qquad x \equiv 1 \pmod{9}.$$

Using the Chinese remainder theorem, we find that the roots are 45 and 17 modulo 63.

## 6.3 SUMMARY

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 ofsome kind appear on passports, credit cards, bank accounts,and a variety of other settings.

The binary system is most convenient for use in modem 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

## 6.4 KEYWORDS

1. Notation -A **mathematical notation** is a writing system used for recording concepts in **mathematics**. The **notation** uses symbols or symbolic expressions that are intended to have a precise semantic **meaning**
2. Expansion - any mathematical series that converges to a function for specified values in the domain of the function, as $1 + x + x^2 + \ldots$ for $1/(1 - x)$ when $x < 1$.
3. Decimal - the numbers we use in everyday life are decimal numbers, because they are based on 10 digits
4. Binary - **binary number** is a **number** expressed in the base-2 numeral system or **binary** numeral system, which uses only two symbols: typically "0" (zero) and "1" (one).

## 6.5 QUESTIONS FOR REVIEW

**1.** Use the binary exponentiation algorithm to compute both $19^{53}$ (mod 503) and $141^{47}$
(mod 1537).

**2.** Convert (7482)10to base 6 notation

**3.** Assuming that 495 divides *273x49y5*, obtain the digits *x* andy.

**4.** Solve the linear congruence $9x = 21$ (mod 30).

**5.** Solve the linear congruence 17x = 9 (mod 276)

## 6.6 SUGGESTED READINGS

10. David M. Burton, Elementary Number Theory, University of New Hampshire.
11. G.H. Hardy, and , E.M. Wrigh,. An Introduction to the Theory of Numbers (6th ed, Oxford University Press, (2008).
12. W.W. Adams and L.J. Goldstein, Introduction to the Theory of Numbers, 3rd ed., Wiley Eastern, 1972.

13. A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1984.
14. I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers, 4th Ed., Wiley, New York, 1980.
15. T.M. Apostol, Introduction to Analytic number theory, UTM, Springer, (1976).
16. J. W. S Cassel, A. Frolich, Algebraic number theory, Cambridge.
17. M Ram Murty, Problems in analytic number theory, springer.
18. M Ram Murty and Jody Esmonde, Problems in algebraic number theory, springer.

## 6.7 ANSWERS TO CHECK YOUR PROGRESS

1. [HINT: Provide the notation and explanation with example—6.1 ]
2. .[HINT: Explain with example –6.1.4]

# UNIT 7: THECONGRUENCE –II

## STRUCTURE



# 7.0 OBJECTIVES

Understand the application of the congruence $x^2 \equiv a \ (mod\ m)$.

Unfold the importance of quadratic congruence

Understand the concept of Gauss Lemma

# 7.1 THE CONGRUENCE $x^2 \equiv a\ (mod\ m)$.

(1) $$x^2 \equiv a\ (mod\ m).$$

There are three main problems to consider.

Firstly, when do solutions exist, secondly, how many solutions are there, and thirdly, how to find them. We will first show that we can always reduce a congruence of the form (1) to a congruence of the same form with $(a, m) = 1$.

Assume therefore that $(a, m) > 1$, and let $p$ be a prime dividing $(a, m)$, that is $p \mid a$ and $p \mid m$. Suppose $x$ is a solution of (1). Then $p \mid x^2$ and hence $p \mid x$. Write $x = py$; then (1) is equivalent to $p^2y^2 \equiv a$ (mod $m$). Divide by $p$ to obtain

(2) $$py^2 \equiv a/p\ (mod\ m/p).$$

There are three separate cases to consider:

(i) If $p^2 \mid m$ and $p^2 \mid a$, then (2) is equivalent to the congruence $y^2 \equiv a/p^2$ (mod $m/p^2$), and for each solution $y_0$ of this congruence (if there are any), there are $p$ incongruent solutions modulo $m$ of the original congruence (1). These are

$$x \equiv py_0 \text{ (mod } m/p).$$

If $(a/p^2, m/p^2) > 1$, we repeat the whole procedure.

(ii) If $p^2 \mid m$ but $p^2 6 \mid a$, then (2) is a contradiction. Hence, (1) has no solutions in this case.

(iii) If $p^2 6 \mid m$, then $(p, m/p) = 1$, and hence there is a number $c$ such that $cp \equiv 1$ (mod $m/p$). It follows that (2) is equivalent to the congruence

$$y^2 \equiv ca/p \text{ (mod } m/p).$$

Notes

Any solution $y_0$ of this congruence yields a unique solution

$$x \equiv py_0 \pmod{m} \text{ of (1).}$$

If $(ca/p, m/p) > 1$ we can repeat the whole procedure.

Note that if $p2 \mid a$, then

$$ca/p = cp \cdot a/p^2 \equiv 1 \cdot a/p^2 \equiv a/p^2 \pmod{m/p},$$

i.e. (2) is equivalent to the congruence $y^2 \equiv a/p^2 \pmod{m/p}$ in that case.

**Example:** Solve the four congruences:

(i) $x^2 \equiv 36 \pmod{45}$, (ii) $x^2 \equiv 15 \pmod{45}$,

(iii) $x^2 \equiv 18 \pmod{21}$, (iv) $x^2 \equiv 15 \pmod{21}$.

**Solution:**

(i) Here $(36, 45) = 9$ and writing $x = 3y$ we obtain the equivalent congruence $y^2 \equiv 4 \pmod{5}$ with the solutions $y \equiv \pm 2 \pmod{5}$. Hence $x \equiv \pm 6 \pmod{15}$, i.e. 6, 9, 21, 24, 36, and 39 are the solutions of (i).

(ii) Since $9 \mid 45$ but $96 \mid 15$ there are no solutions of (ii).

(iii) Since $(18, 21) = 3$, we write $x = 3y$ and obtain the following sequence of equivalent congruences: $9y2 \equiv 18 \pmod{21}$, $3y2 \equiv 6 \pmod{7}$, $y2 \equiv 2 \pmod{7}$ with the solutions $y \equiv \pm 3 \pmod{7}$. Hence (iii) has the solutions $x \equiv \pm 9 \pmod{21}$.

(iv) Since $(15, 21) = 3$, we put $x = 3y$ and obtain $9y2 \equiv 15 \pmod{21}$, that is $3y^2 \equiv 5 \pmod{7}$. Since $5 \cdot 3 \equiv 1 \pmod{7}$, we multiply the last congruence by 5, which yields $y2 \equiv 4 \pmod{7}$ with the solutions $y \equiv \pm 2 \pmod{7}$. Consequently, $x \equiv \pm 6 \pmod{21}$ are the solutions of (iv).

For the rest of this section, we will assume that $(a, m) = 1$.

## 7.1.1 Definition

Suppose that $(a, m) = 1$. Then $a$ is called a *quadratic residue of m* if the congruence $x^2 \equiv a \pmod{m}$ has a solution. If there is no solution, then $a$ is called a *quadratic nonresidue of m.*

By decomposing the modulus $m$ into a product of primes, we reduce the study of the congruence (1) to a study of congruences of the form

$$x^2 \equiv a \pmod{pk}$$

where the modulus is a prime power. However, since the derivative of $x^2$ is $2x$, and $2x \equiv 0 \pmod{2}$ we have to distinguish between the cases $p = 2$ and $p$ odd prime.

**Lemma**

*If p is an odd prime,* $(a, p) = 1$ *and a is a quadratic residue of p, then the congruence* $x^2 \equiv a \pmod{p}$ *has exactly two roots.*

*Proof.* By assumption, there is at least one root $b$. Obviously, $-b$ is a root, too, and $-b \not\equiv b \pmod{p}$, since $b \not\equiv 0$. As, there can not be more than two roots.

## 7.1.2 Theorem

If p is an odd prime and (a, p) = 1, then x2 ≡ a (mod pk) has exactly two solutions if a is a quadratic residue of p, and no solutions if a is a quadratic nonresidue of p.

***Proof.*** Let $f(x) = x2 - a$; then $f_0(x) = 2x$ is not divisible by $p$ for any $x \not\equiv 0 \pmod{p}$. Hence, it follows from Lemma 7.1.2 that the equation $x^2 \equiv a$ (mod $p^k$) has exactly two roots for each $k$ if $a$ is a quadratic residue. Since every solution of the latter congruence also solves the congruence
$x^2 \equiv a \pmod{p}$, there can be no solution if $a$ is a quadratic nonresidue of

$p$.The case $p$ = 2 is different, and the complete story is given by the following theorem.

## 7.1.3 Theorem

Suppose a is odd. Then

(i) The congruence $x^2 \equiv a \pmod 2$ is always solvable and has exactly one solution;

(ii) The congruence $x^2 \equiv a \pmod 4$ is solvable if and only if $a \equiv 1 \pmod 4$, in which case there are precisely two solutions;

(iii) The congruence $x^2 \equiv a$ (mod 2k), with $k \geq 3$, is solvable if and only if $a \equiv 1 \pmod 8$, in which case there are exactly four solutions. If $x_0$ is a solution, then all solutions are given by ±x0 and $\pm x_0 + 2^{k-1}$.

***Proof.*** (i) and (ii) are obvious.

(iii) Suppose $x^2 \equiv a \pmod{2^k}$ has a solution $x_0$. Then obviously $x_0^2 \equiv a$ (mod 8), and $x_0$ is odd since $a$ is odd. But the square of an odd number is congruent to 1 modulo 8, and hence $a \equiv 1 \pmod 8$. This proves the necessity of the condition $a \equiv 1 \pmod 8$ for the existence of a solution. Moreover, $(-x_0)^2 = x_0^2 \equiv a \pmod{2^k}$ and $(\pm x0 + 2^{k-1})^2 = x_0^2 \pm 2^k x_0 + 2^{2k-2} \equiv x_0^2 \equiv \equiv a$ $\pmod{2^k}$,
since $2k - 2 \geq k$. It is easily verified that the four numbers ±$x$0 and ±$x$0 + $2^{k-1}$ are incongruent modulo 2$k$. Hence, the congruence has at least four solutions if there is any.

It remains to verify that the condition on $a$ is sufficient and that there are at most four solutions. We show sufficiency by induction on $k$. The case $k$ = 3 is clear, since $x$2 ≡ 1 (mod 8) has the solution $x \equiv 1$. Now assume that $x^2 \equiv a$

(mod $2^k$) is solvable with a solution $x_0$. Then we know that $\pm x_0$ and $\pm x_0+2^{k-1}$ also solve the congruence, and we will prove that one of them also solves the congruence

(3) $$x^2 \equiv a \pmod{2^{k+1}}.$$

We know that $x_0^2 \equiv = a+2^k n$ for some integer $n$. If $n$ is even, then $x0$ is obviously
a solution of (3). If $n$ is odd, then

$$(x_0 + 2^{k-1})^2 = x_0^2 \equiv + 2^k x_0 + 2^{2k-2} = a + 2^k(n + x_0) + 2^{2k-2} \equiv a \pmod{2^{k+1}},$$

because $(n + x0)$ is even (since $n$ and $x0$ are both odd) and $2k - 2 \geq k + 1$ (since $k \geq 3$). This completes the induction step

Finally, in the interval $[1, 2k]$ there are $2k-3$ integers $a$ that are congruent to 1 modulo 8. For each such number $a$ we have already found 4 different solutions of the congruence $x^2 \equiv a$ (mod $2k$) in the same interval, all of them odd. Taking all these solutions together we get

**4** $\cdot 2^{k-3} = 2^{k-1}$ solutions. But there are exactly $2k-1$ odd numbers in the interval, so there is no room for any more solutions. Hence, each equation has exactly four solutions.

## 7.1.5 Theorem

*Let* $m = 2^k p_1^{k_1} \cdots p_r^{k_r}$, *where the* $p_i$ *are distinct odd primes, and let a be a number which is relatively prime to m. Then the congruence* $x^2 \equiv a$ (mod $m$) *is solvable if and only if a is a quadratic residue of* $p_i$ *for each i, and* $a \equiv 1 \pmod 4$ *in the case* $k = 2$, *and* $a \equiv 1 \pmod 8$ *in the case* $k \geq 3$. *If the congruence is solvable, then there are* $2r$ *solutions if* $k = 0$ *or* $k = 1$, $2^{r+1}$ *solutions if* $k = 2$, *and* $2^{r+2}$ *solutions if* $k \geq 3$.

In order to apply Theorem 7.1.5 we need some criterion telling when a number is a quadratic residue of given prime $p$. First, note that there are as many quadratic residues as nonresidues of an odd prime.

## 7.1.4 Theorem

*Let p be an odd prime. Then there are exactly* $(p - 1)/2$ *incongruent quadratic residues of p and exactly* $(p - 1)/2$ *quadratic nonresidues of p.*

***Proof***. All quadratic residues can be found by squaring the elements of a reduced residue system. Since each solvable congruence $x^2 \equiv a \pmod{p}$ has exactly two solutions if $(a, p) = 1$, it follows that the number of quadratic residues equals half the number of elements in the reduced residue system, that is $(p-1)/2$. To get all quadratic residues one can for example take $1^2, 2^2, \ldots, [(p-1)/2]^2$.

**Lemma**

*Let p be an odd prime and suppose* $a \not\equiv 0 \pmod{p}$. *Then modulo p*

$$(p-1)! \equiv \begin{cases} a^{(p-1)/2} & \text{if } a \text{ is a quadratic nonresidue of } p \\ -a^{(p-1)/2} & \text{if } a \text{ is a quadratic residue of } p. \end{cases}$$

***Proof.*** The congruence $mx \equiv a \pmod{p}$ is solvable for each integer $m$ in the interval $1 \le m \le p - 1$, i.e. for each $m$ there is an integer $n$, $1 \le n \le p - 1$ such that $mn \equiv a \pmod{p}$. If the congruence $x^2 \equiv a \pmod{p}$ has no solution, then $n \neq m$. If it has a solution, then it has exactly two solutions of the form $x \equiv m_0 \pmod{p}$ and $x \equiv p - m_0 \pmod{p}$, and it follows that $n \neq m$ for all but two values of $m$. Now consider the product $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$. If the congruence $x^2 \equiv a \pmod{p}$ has no solution, then we can pair off the $p - 1$ numbers into $(p - 1)/2$ pairs such that the product of the two numbers in each pair is congruent to $a \pmod{p}$, and this means that $(p - 1)!$ is congruent to $a(p-1)/2$.

On the other hand, if the congruence has two solutions, $m_0$ and $p - m_0$, then we take away these two numbers and pair off the remaining $p - 3$ numbers into $(p - 3)/2$ pairs such that the product of the two numbers in each pair is congruent to $a \pmod p$. Since $m_0(p - m_0) \equiv -m_0^2 \equiv -a \pmod p$, it follows that $(p - 1)! \equiv -a \cdot a^{(p-3)/2} \equiv -a^{(p-1)/2} \pmod p$.

Lets recall the Wilson's theorem

**Wilson's theorem** *If p is a prime then* $(p - 1)! \equiv -1 \pmod p$.

First let us note that Wilson's theorem for $p > 2$ is a obtained as a special case of Lemma 7.1.7 by taking $a = 1$, which is obviously a quadratic residue of any prime $p$. Secondly, and more important, by combining Wilson's theorem with Lemma 1.1.7 we get the following solvability criterion due to Euler:

## 7.1.5 Theorem

(Euler's Criterion) *Let p be an odd prime and suppose* $(a, p) = 1$. *Then a is a quadratic residue or nonresidue of p according as* $a(p-1)/2 \equiv 1 (\mathrm{mod}\ p)$ *or* $a(p-1)/2 \equiv -1 \pmod p$.

The following important result follows immediately from Euler's criterion.

## 7.1.6 Theorem

Let p be a prime.Then −1 is a quadratic residue of p if and only if p = 2 or p ≡ 1 (mod 4).

***Proof.*** −1 is a quadratic residue of 2 since $1^2 = 1 \equiv -1 \pmod 2$. For odd primes, we apply Euler's Criterion noting that $(-1)^{(p-1)/2} = 1$ if and only if $(p - 1)/2$ is even, that is if and only if $p$ is a prime of the form $4k + 1$.

Let us also note that Fermat's theorem is an easy consequence of Euler's criterion; by squaring we obtain

$$a^{p-1} = \left(a^{(p-1)/2}\right)^2 \equiv (\pm 1)^2 = 1 \pmod{p}.$$

Let us finally address the question of finding a solution to the congruence $x^2 \equiv a \pmod{p}$ assuming that $a$ is a quadratic residue of $p$. In the case $p \equiv 3 \pmod{4}$ we have the following answer.

## 7.1.7 Theorem

*Let p be a prime and assume that* $p \equiv 3 \pmod{4}$. *If a is a quadratic residue of p, then the congruence* $x^2 \equiv a \pmod{p}$ *has the two solutions* $\pm a(p+1)/4$.

***Proof.*** Since $a$ is a quadratic residue, $a^{(p-1)/2} \equiv 1 \pmod{p}$. It follows that

$$\left(\pm a^{(p+1)/4}\right)^2 = a^{(p+1)/2} = a \cdot a^{(p-1)/2} \equiv a \pmod{p}.$$

Note that it is not necessary to verify in advance that $a^{(p-1)/2} \equiv 1 \pmod{p}$. It is enough to compute $x \equiv a^{(p+1)/4} \pmod{p}$. If $x^2 \equiv a \pmod{p}$, then $\pm x$ are the two solutions, otherwise $x^2 \equiv -a \pmod{p}$, and we can conclude that there are no solutions.

**Check Your Progress 1**

1. Explain the problems associated with $x^2 \equiv a \ (mod\ m)$.

______________________________

______________________________

2. What is Quadratic residue?

______________________________

______________________________

# 7.2 GENERAL QUADRATIC CONGRUENCES

A general quadratic congruence

(1) $$ax^2 + bx + c \equiv 0 \pmod{m},$$

can be reduced to a system consisting of a congruence of the form $y^2 \equiv d \pmod{m'}$ and a linear congruence by completing the square.

The simplest case occurs when $(4a, m) = 1$, because we may then multiply the congruence (1) by $4a$ without having to change the modulus $m$ in order to get the following equivalent congruence

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{m},$$

that is,

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{m}.$$

Writing $y = 2ax + b$, we obtain the following result.

## 7.2.1 Theorem

*Assume that* $(4a, m) = 1$. *Then all solutions of the congruence*

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

*can be found by solving the following chain of congruences*

$$y^2 \equiv b^2 - 4ac \pmod{m}, \qquad 2ax \equiv y - b \pmod{m}.$$

Since $(2a, m) = 1$, the linear congruence has a unique solution modulo $m$ for each root $y$.

**Example** Let us solve the congruence $8x^2 + 5x + 1 \equiv 0 \pmod{23}$.

Notes

Solution : Complete the square by multiplying by 32 to get (16$x$+5)2 ≡ 52−32 = −7 ≡ 16 (mod 23).

Thus 16$x$ + 5 ≡ ±4.

Solving 16$x$ ≡ −1 (mod 23) gives $x$ ≡ 10, and 16$x$ ≡ −9 (mod 23) yields $x$ ≡ 21.

Hence, 10 and 21 are the only solutions of the original congruence.

When (4$a$, $m$) ≠ 1, we start by factoring $4a = a_1a_2$ in such a way that ($a_2$, $m$) = 1. We may now multiply the congruence (1) by the number $a_2$ without having to change the modulus, but when we then multiply by $a_1$ we must change the modulus to $a1m$ in order to get the equivalent congruence

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{a1m},$$

which, of course, in turn is equivalent to the congruence

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{a1m}.$$

This proves the following generalization of theorem 7.2.1.

**Theorem 7.2.2** *Write* $4a = a_1a_2$ *with* $a_2$ *relatively prime to m. Then all solutions of the congruence*

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

*can be found by solving the following chain of congruences*

$$y^2 \equiv b^2 - 4ac \pmod{a1m},\ 2ax \equiv y - b \pmod{a1m}$$

**Example:** Let us solve the congruence 3$x$2 + 3$x$ + 2 ≡ 0 (mod 10) using Theorem 7.2.2.. Since (4· 3, 10) = 2 6= 1 but (3, 10) = 1, multiplication by 4 · 3 transforms the given congruence into the equivalent congruence

(6$x$ + 3)2 ≡ 32 − 4 · 3 · 2 = −15 ≡ 25 (mod 40).

The congruence $y^2 \equiv 25$ (mod 40) has four roots modulo 40, namely 5, 15, 25, and 35. For each root $y$ we then solve the linear congruence 6$x$ ≡ $y$ – 3 (mod 40).

The solutions are in turn $x$ ≡ 7, 2, 17, 12 (mod 20), which means that the solutions of our original congruence are $x$ ≡ 2 and $x$ ≡ 7 (mod 10).

**Example:** Solve . $x^2 \equiv 5 \pmod{61}$

According to Euler's Criterion, the equation

$$x^2 \equiv 5 \pmod{61}$$

has solutions since . $5^{30} \equiv 1 \pmod{61}$

To find the solutions, we keep adding the modulus to $a = 5$ until we get a perfect square.

$$x^2 \equiv 5 \equiv 5 + 61 \equiv 5 + 2(61) \equiv \cdots \equiv 5 + 20(61) = 1225 = 35^2 \pmod{61}$$

So we have $x^2 \equiv 35^2 \pmod{61}$, which gives $x = 35$ and $x = -35$. The solutions are $x \equiv -35 \equiv 26 \pmod{61}$ and $x \equiv 35 \pmod{61}$.

# 7.3 THE LEGENDRE SYMBOL AND GAUSS' LEMMA

Let $p$ be an odd prime.The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p \\ -1, & \text{if } a \text{ is a quadratic nonresidue of } p \\ 0, & \text{if } p \mid a. \end{cases}$$

## 7.3.1 Theorem

*Let p be an odd prime. Then*

*(i)* $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,

*(ii)* $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

*(iii)* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

*(iv)* *If* $(a,p) = 1$ *then* $\left(\frac{a^2}{p}\right) = 1$ *and* $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$,

*(v)* $\left(\frac{1}{p}\right) = 1$,

*(vi)* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$

Notes

***Proof.*** If $p \mid a$ then (i) is obvious, and if $(p, a) = 1$ then (i) is just a reformulation of Euler's criterion (Theorem 7.1.8). The remaining parts are all simple consequences of (i).

Because of Theorem 7.3.2 (iii) and (iv), in order to compute $\left(\frac{a}{p}\right)$for an arbitrary integer *a* it is enough, given its prime factorization, to know $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{q}{p}\right)$for each odd prime *q*.

## 7.3.2 Theorem (Gauss' Lemma)

Let p be an odd prime and suppose that the number a is relatively prime to p. Consider the least positive residues modulo p of the numbers a, 2a, 3a, ..., $\frac{p-1}{2}$a. If N is the number of these residues that are greater than p/2, then $\left(\frac{a}{p}\right) = (-1)^N$

*Proof.* The numbers $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ are relatively prime to *p* and incongruent modulo *p*. Let $r_1, r_2, \ldots, r_N$ represent the least positive residues that exceed $p/2$, and let $s_1, s_2, \ldots, s_M$ denote the remaining residues, that is those that are less than $p/2$; then $N + M = (p - 1)/2$.

The quotient *q* when *ja* is divided by *p* is $q = [ja/p]$. (Here $[x]$ denotes the greatest integer less than or equal to *x*.) It follows that

(1) $$ja = [ja/p]\, p + \text{some } r_i \text{ or some } s_k.$$

The numbers $p - r_1, p - r_2, \ldots, p - r_N$ are positive and less than $p/2$, relatively prime to *p* and incongruent in pairs modulo *p*. Also, no $p-r_i$ is and $s_j$. For suppose $p - r_i = s_j$, and let $r_i \equiv ma \pmod{p}$ and $s_j \equiv na \pmod{p}$, where *m* and *n* are distinct integers between 1 and $p/2$. Then

$$p = ri + sj \equiv (m + n)a \pmod{p},$$

and since $(a, p) = 1$, we must have $p \mid (m + n)$, a contradiction since $0 < m + n < p$.

Thus, $p - r_1, p - r_2, \ldots, p - r_N, s_1, s_2, \ldots, s_M$ are all different integers in the intervall $[1, (p - 1)/2]$, and since they are $M + N = (p - 1)/2$ in number, they are equal in some order to the numbers $1, 2, \ldots, (p - 1)/2$. Therefore,

$$(p - r_1)(p - r_2) \cdots (p - r_N) s_1 s_2 \cdots s_M = ((p - 1)/2)!,$$

that is

$$(-1)^N r_1 r_2 \cdots r_N s_1 s_2 \cdots s_M \equiv ((p - 1)/2)! \pmod{p}.$$

But the numbers $r_1, r_2, \ldots, r_N, s_1, s_2, \ldots, s_M$ are also congruent in some order to the numbers $a, 2a, \ldots, \frac{p-1}{2}a$ and hence

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^N a \cdot 2a \cdots \frac{p-1}{2}a = (-1)^N a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv$$

(mod $p$).

Since each factor in $((p - 1)/2)!$ is relatively prime to $p$, we can divide each side of the last congruence by $((p- 1)/2)!$ to obtain $a(p-1)/2 \equiv (-1)N$ (mod $p$). The conclusion of the lemma now follows from part (i) of Theorem 7.3.2.

As a simple application of Gauss' lemma, we now compute $\left(\frac{2}{p}\right)$

## 7.3.3 Theorem

*Let p be an odd prime. Then 2 is a quadratic residue of p if p* $\equiv \pm 1 \pmod{8}$, *and a quadratic nonresidue of p if p* $\equiv \pm 3 \pmod{8}$, *that is*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

*Proof.* Take $a = 2$ in Gauss' lemma; then $N$ is the number of integers in the sequence $2, 4, \ldots, p - 1$ that are greater than $p/2$, that is $N$ is the number of integers $k$ such that $p/2 < 2k < p$, or equivalently $p/4 < k < p/2$.

Consequently,

$$N = [p/2] - [p/4].$$

Taking $p = 4n + 1$ we get $N = 2n - n = n$, and $p = 4n - 1$ yields

$$N = (2n - 1) - (n - 1) = n, \text{ too.}$$

Hence, $N$ is even if $n$ is even, i.e. if $p = 8m \pm 1$, and $N$ is odd if $n$ is so, i.e. if $p = 8m \pm 3$.

**Example:** The equation $x^2 \equiv 2 \pmod{17}$ is solvable since $17 \equiv 1 \pmod 8$. Indeed, $x \equiv \pm 6 \pmod{17}$ solves the congruence.

## 7.3.4 Theorem

*If p is an odd prime and a is an odd number that is not divisible by p, then*

$$\left(\frac{a}{p}\right) = (-1)^n, \qquad \text{where } n = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right].$$

*Proof.* We have to prove that $n$ has the same parity as the number $N$ in Gauss' lemma, i.e. that $n \equiv N \pmod 2$. We use the same notation as in the proof of the lemma. By summing over $j$ in equation (1), we obtain

$$\text{(2)} \qquad \sum_{j=1}^{(p-1)/2} ja = p \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right] + \sum_{i=1}^{N} r_i + \sum_{k=1}^{M} s_k.$$

Since the numbers $p - r_1, p - r_2, \ldots, p - r_N, s_1, s_2, \ldots, s_M$ are the numbers $1, 2, \ldots, (p - 1)/2$ in some order, we also have

$$\sum_{j=1}^{(p-1)/2} j = \sum_{i=1}^{N} (p - r_i) + \sum_{k=1}^{M} s_k.$$

Subtracting this from equation (2), we obtain

$$(a-1)\sum_{j=1}^{(p-1)/2} j = 2\sum_{i=1}^{N} r_j + p\left(\sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] - N\right) = 2\sum_{i=1}^{N} r_j + p(n-N).$$

Since $a - 1$ is an even number, it follows that $p(n - N)$ is even, that is $n - N$ is even.

**Example**: Let us use Theorem 7.3.4 to compute $\left(\frac{3}{p}\right)$ for primes $p \geq 5$. Since

$$\left[\frac{3j}{p}\right] = \begin{cases} 0 & \text{if } 1 \leq j \leq [p/3], \\ 1 & \text{if } [p/3]+1 \leq j \leq (p-1)/2. \end{cases}$$

it follows that $\left(\frac{3}{p}\right) = (-1)n$, where $n = (p - 1)/2 - [p/3]$. By considering the cases $p = 12k \pm 1$ and $p = 12k \pm 5$ separately, we see that $n$ is even if and only if $p \equiv \pm 1 \pmod{12}$. Hence, $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$. Gauss' lemma and Theorem 7.3.5 are too cumbersome for numerical calculations of $\left(\frac{a}{p}\right)$

**Check Your Progress 2**

1. Define Legendre symbol

_______________________________________________

_______________________________________________

2. Explain Gauss Lemma

_______________________________________________

_______________________________________________

_______________________________________________

3. What do you understand by Quadratic congruence?

Notes

## 7.4 SUMMARY

Gauss Lemma has theoretical significance, being involved in some proofs of quadratic reciprocity.

**Quadratic Reciprocity is important** in cryptography and in computer security.

## 7.5 KEYWORDS

1. Parity: In **mathematics**, **parity** is the property of an integer's inclusion in one of two categories: even or odd.

2. Lemma - In **mathematics**, a "helping theorem" or **lemma** (plural **lemmas** or lemmata) is a proven proposition which is used as a stepping stone to a larger result rather than as a statement of interest by itself.

3. Sequence - A list of numbers or objects in a special order.

4. Incongruent - two numbers are **incongruent** when, after being divided by the same number, their remainders are different.

5. **Consequently** is a word that has to do with cause and effect

## 7.6 QUESTIONS FOR REVIEW

1. Solve $x^2 \equiv 899 \pmod{50261}$

2. Use Gauss' lemma to compute each of the Legendre symbols below (that is, in each case

obtain the integer $n$ for which $(a/p) = (-1)^n$)

(a) (8/11).

(b) (7/13).

3. For an odd prime *p*, prove that there are $(p-1)/2 - \phi(p-1)$ quadratic nonresidues of
*p* that are not primitive roots of *p*.

4. If pis an odd prime, show that

$$\sum_{a=1}^{p-2} (a(a+1)/p) = -1$$

# 7.7 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.

## 7.8 ANSWERS TO CHECK YOUR PROGRESS

1. [HINT: Discuss three problems ---7.1]

2. [HINT:Provide definition and related lemma—7.1.1 & 7.1.2 ]
3. [HINT: Provide definition—7.3]
4. [HINT:Provide statement with proof—7.3.2]
5. [HINT:Provide definition with example –7.2 ]