Handout

of

NUMBER THEORY

by

Kus Prihantoso Krisnawan

MATHEMATICS DEPARTMENT
FACULTY OF MATHEMATICS AND NATURAL SCIENCES
YOGYAKARTA STATE UNIVERSITY
2012

Contents

Topic 1

Some Preliminary Considerations

1.1 Basic Axioms for $\mathbb{Z}$

Some special sets are used throughout this handout. These sets are denoted by standard symbols,

$\mathbb{N} = \{1, 2, 3, ...\}$ = the set of natural numbers = $\mathbb{Z}_+$,

$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ = the set of integers,

$\mathbb{Q} = \left\{ \frac{n}{m} \mid n, m \in \mathbb{Z} \text{ and } m \neq 0 \right\}$ = the set of rational numbers, and

$\mathbb{R}$ = the set of real numbers.

Note that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Below, a list of some particularly important properties of $\mathbb{Z}$ that will be needed. These are called axioms since we will not prove them in this course.

Some basic axiom for $\mathbb{Z}$:

1. If $a, b \in \mathbb{Z}$, then $a + b$, $a - b$, and $ab \in \mathbb{Z}$. ($\mathbb{Z}$ is closed under addition, subtaction, and multiplication.)
2. If $a \in \mathbb{Z}$ then there is no $x \in \mathbb{Z}$ such that $a < x < a + 1$.
3. **Properties of inequalities:** If $a, b, c \in \mathbb{R}$ then
   a. If $a < b$ and $b < c$ then $a < c$.
   b. If $a < b$ then $a + c < b + c$.

c. If $a < b$ and $0 < c$ then $ac < bc$.

d. If $a < b$ and $c < 0$ then $bc < ac$.

e. Given a and b, then one and only one of the following holds:

$$a = b, \qquad a < b, \qquad a > b$$

4. **Laws of exponent:** If $n, m \in \mathbb{Z}$, $a, b \in \mathbb{R}$ and a and b are not zero then

   a. $(a^n)^m = a^{nm}$

   b. $(ab)^n = a^n b^n$

   c. $a^n a^m = a^{n+m}$

5. **The Well Ordering Property for $\mathbb{N}$:** Every nonempty subset A of $\mathbb{N}$ contain a least element, that is to say, there exist an element $m \in A \subset \mathbb{N}$ such that for each $a \in A$ we have $m \leq a$.

1.2 The Principle of Mathematical Induction

Let $P(n)$ be a statement concerning the integer variable n, and let n_0 be any fixed integer. $P(n)$ is true for all integers $n > n_0$ if one can establish both of the following statements:

i. $P(n)$ is true for $n = n_0$, and

ii. Whenever $P(n)$ is true for $n_0 \leq n \leq k$ then $P(n)$ is true for $n = k + 1$.

Example 1.2.1. *Prove that if $n \geq 5$ then $2^n > 5n$.*

Proof. We prove it by Mathematical Induction.

i. If $n = 5$, we have $2^5 = 32 > 25 = 5 \cdot 5$ which is true.

ii. Assume (the induction hypothesis)

$$2^n > 5n \quad for \quad n_0 \leq n \leq k.$$

Taking $n = k$ we have

$$2^k > 5k.$$

Multiplying both sides by 2 gives

$$2^{k+1} > 10k.$$

Now $10k = 5k + 5k$ and $k \geq 5$ so $k \geq 1$ and therefore $5k \geq 5$. Hence

$$10k = 5k + 5k \geq 5k + 5 = 5(k + 1).$$

It follows that

$$2^{k+1} > 10k \geq 5(k + 1).$$

and therefore

$$2^{k+1} > 5(k + 1).$$

Hence we conclude that $2^n > 5n$ for $n \geq 5$. □

1.3 The Binomial Theorem

For any $n, k \in \mathbb{Z}_+$ satisfying $0 \leq k \leq n$, the *combination* of k objects from n objects, denoted by $\begin{pmatrix} n \\ k \end{pmatrix}$, defined by

$$\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!}$$

Let $x, y \in \mathbb{R}$ and $n \in \mathbb{Z}_+$, *the binomial theorem* says that

$$(x + y)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} x^{n-k} y^k$$

It is easy to verify that

$$\begin{aligned} (x + y)^2 &= x^2 + 2xy + y^2; \\ (x + y)^5 &= x^5 + 5x^4 y + 10x^3 y^2 + 10x^2 y^3 + 5xy^4 + y^5; \\ \cdots &\quad \textit{etc.} \end{aligned}$$

1.4 Problems

1. We prove that every city is *small*, by induction on the number of its inhabitants. Clearly, if a city has just one inhabitant, it is small. Assume a city has n inhabitants. If this city is small, it is still so even if we add one inhabitant. So we deduce that all cities are small. Is everything right or is something amiss?

   a. Everything is right and it proves that mathematics cannot possibly be applied to concrete question.

   b. The basis of the induction is not right: if there is a single inhabitant, it is not a city.

   c. The basis of the induction is right, but the proof of the inductive step depends upon the definition of the small city.

   d. None of the above.

2. Assume we have defined a city to be *small* if it has less than 50.000 inhabitants. Which of the statements (a) - (d) of problem 1 is correct?

3. Conjecture a formula for A^n, if $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then by use of induction, prove your formula.

4. Proof that for $1 \leq k \leq n$, we have

$$\begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix} = \begin{pmatrix} n+1 \\ k \end{pmatrix}$$

   Hint: Multiply the identity $\frac{1}{k} + \frac{1}{n-k+1} = \frac{n+1}{k(n-k+1)}$ by $\frac{n!}{(k-1)!(n-k)!}$.

5. Use the mathematical induction to prove the binomial theorem.

6. Prove that

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

   (This problem is connected with the problem of Hanoi tower.)

Topic 2

Recursion Concept

2.1 The Concept of Recursion

Definition 2.1. We say that the function f is defined *recursively* if the value of f at 1 is specified and for each $n \in \mathbb{N}$, a rule is provided for determining $f(n+1)$ from $f(n)$.

Example 2.1.1. *The term $n!$ can be recursively define by:*

$$f(1) = 1 \quad \textit{and} \quad f(n+1) = (n+1)f(n).$$

Example 2.1.2. ***(Fibonacci sequence)*** *Two newborn rabbits, a male and female, are left on a desert island on the 1^{st} of January. This couple becomes fertile after two months and, starting on the 1^{st} of March, they give birth to two more rabbits, a male and a female, the first day of each month. Each couple of newborn rabbits, analogously, become fertile after two months and, starting on the first day of their third month, gives birth to a new couple of rabbits. How many couples are there on the island after n months?*

Answer: Let f_n denote the number of couples of rabbits, a male and a female, that are present in the island during the n^{th} month. It is clear that f_n is the sum of two numbers completely determined by the situation in the preceding months, that is:

i. the number f_{n-1} of the couples of rabbits in the island in the $(n-1)^{th}$ month, as no rabbit dies; and

ii. the number of the couples of rabbits born on the first day of n^{th} month, which are as many as the couples of rabbits which are fertile on that day, and these in turn are as many as the f_{n-2} couples of rabbits that were in the island two months before.

As a consequence, we may write for the sequence $f_1, f_2, f_3, ..., f_n$ recursively define by

$$f_1 = 1, \quad f_2 = 1, \quad and \quad f_n = f_{n-1} + f_{n-2} \quad for \quad n \geq 3. \tag{2.1}$$

We would like, in fact, to have a *solution* of the recurrence relation (2.1), that is *closed formula* giving the n^{th} term of Fibonacci sequence, without having to compute all the preceding terms. Actually, the closed formula for the n^{th} Fibonacci number is

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}^n - \frac{1-\sqrt{5}}{2}^n \right) \right]. \tag{2.2}$$

In order get the formula (2.2), we shall use matrix operations and some principles of linear algebra. Thus, we are not going to discuss about it yet.

2.2 Discussion

Each group discuss one of the subsections below, subsection 2.2.1 is for the groups: **1**, 3, 4, and 7, and subsection 2.2.2 is for the groups: **2**, 5, 6, 8, and 9. Each subsection will presents by selected group.

2.2.1 The Bright Graduate

Young Krisnawan, who was about to graduate at the head of his class at Yogyakarta State University, was in the pleasant position of having choice of two very attractive offers, both at $5000 a year. Unable to make up his mind between them immediately, he wrote the two companies and asked his chances were for raises over the next ten years.

Company A replied to the effect that it would guarantee a raise of $300 every six months for the next ten years. And its raises will be started at the second sixth-month. Meanwhile, company B said it would guarantee a raise of $1200 every twelve months for the next ten years since the second year.

Krisnawan quite confused with this offer. Can you help him to make the decision?

2.2.2 The Tower of Hanoi

The game of the tower of Hanoi was invented by the mathematician E. Lucas in 1883. The tower of Hanoi consist of n circular holed discs, with a vertical peg A running through all

of them; the discs are stacked with their diameters decreasing from bottom up.
The goal of the game is to transfer all discs, in the same order, that is to say, with their diameters decreasing from bottom up, on another peg C, by using a support peg B (see figure 2.1) and observing the following rules:

i the discs must transferred one at a time from one peg to another one;

ii never during the game, on any peg, a disc with a greater diameter may be located above a disc with a smaller diameter.

Determine the number of moves necessary to conclude the game starting with n discs!

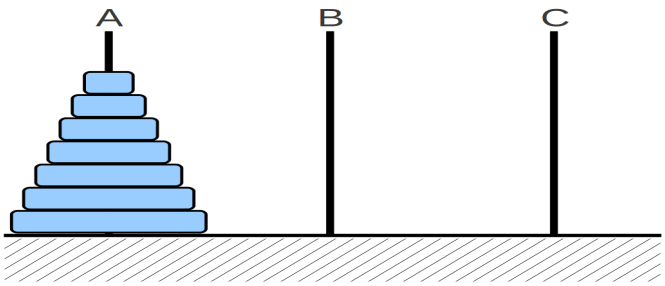

Figure 2.1: The tower of Hanoi with $n = 7$ discs

2.3 Problems

1. What is the recursive function (recurrence relation) for the sum of the first n odd natural number?

2. What is the solution of the geometric progression $a_n = r \cdot a_{n-1}$, $a_0 = k$ where r and k are fixed integer.

3. What is the recurrence relation for the world population if the population increase by 3% each year?

4. Iyan has opened a bank account for which there are no charges and yielding a yearly 4% interest which is computed and paid to his account every third month. Suppose Iyan deposited a certain amount of money when he opened the account and after that

he neither withdrew nor deposited money from the account. What is the recurrence relation determining amount of money Iyan has in his account after n years?

Topic 3

Divisibility

3.1 Elementary Divisibility Properties

Definition 3.1. The term $d|n$, $d \neq 0$ divides n, means that there is an integer k such that $n = dk$. The term $d \nmid n$ means that d does not divides n.

In other words, we can say that $d|n$ iff $d \neq 0$ and $n = dk$ for some k, and $d \nmid n$ iff there is no k such that $n = dk$.

Theorem 3.2. *(Divisibility Properties): If $n, m, d, a, b \in \mathbb{Z}$ then the following statements hold:*

1. $1|n$ *and if* $n \neq 0$ *then* $n|n$ *and* $n|0$
2. *If* $d|n$ *and* $n|m$ *then* $d|m$ (transitivity)
3. *If* $d|n$ *and* $d|m$ *then* $d|(an + bm)$ (linearity)
4. *If* $d|n$ *then* $ad|an$ (multiplication property)
5. *If* $ad|an$ *then* $d \neq 0$ *and* $d|n$ (cancellation property)
6. *If* $n|1$ *then* $n = \pm 1$
7. *If* $d, n \in \mathbb{Z}_+$ *and* $d|n$ *then* $d \leq n$. (comparison property)

Example 3.1.1. *Prove that if* $d|k$ *and* $d|l$ *then* $d|(k - l)$

Proof. By use of Theorem 3.2 (3), and pick up $a = 1$, $b = -1$, $k = n$, and $l = m$ we get the desired term. □

3.2 Floor and Ceiling of a Real Number

Definition 3.3. If x is any real number we define
$\lfloor x \rfloor$ = the greatest integer less than or equal to x, and
$\lceil x \rceil$ = the least integer greater than or equal to x
The term $\lfloor x \rfloor$ is called the floor of x and $\lceil x \rceil$ is called the ceiling of x.

Example 3.2.1. $\lfloor 3, 2 \rfloor = 3$, $\lfloor -4, 7 \rfloor = -5$, $\lceil 8, 1 \rceil = 9$, *and* $\lceil 7, 8 \rceil = -7$.

Note that if n is an integer, by definition we have;

$$n = \lfloor x \rfloor \Leftrightarrow n \leq x < n + 1.$$

Lemma 3.4. *For all $x \in \mathbb{R}$, we have*

$$x - 1 < \lfloor x \rfloor \leq x.$$

Proof. Let $n = \lfloor x \rfloor$, this give immediately that $\lfloor x \rfloor \leq x$ and $x < n + 1$ which implies $x - 1 < n = \lfloor x \rfloor$. □

3.3 The Division Algorithm

Theorem 3.5. *(The Division Algorithm): If $a, b \in \mathbb{Z}$ and $b > 0$ then there exist unique integers $q, r \in \mathbb{Z}$ satisfying the two conditions:*

$$a = bq + r \quad \textit{and} \quad 0 \leq r < b.$$

In this situation, the term a will be called *dividend*, b the *divisor*, q the *quotient* and r the *remainder* when a is divided by b. Note that there are two parts to this result, existence and uniqueness of the integers q and r.

Proof. First, we will prove the *existence* of q and r.

Given $b > 0$ and any a, define

$$\begin{aligned} q &= \lfloor \frac{a}{b} \rfloor \\ r &= a - bq. \end{aligned}$$

Clearly, we have $a = bq + r$, but we need to prove that $0 \leq r < b$. By Lemma 3.4 we have

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

Multiply the terms by $-b$, since $b > 0$, it gives

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

Add all sides by a and replace $\lfloor \frac{a}{b} \rfloor$ by q, we obtain

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

Since $r = a - bq$, this gives us the desired result $0 \leq r < b$.

We still have to prove that q and r are *uniquely* determined.

Assume that

$$a = bq_1 + r_1 \quad \textit{and} \quad 0 \leq r_1 < b,$$

and

$$a = bq_2 + r_2 \quad \textit{and} \quad 0 \leq r_2 < b.$$

We must show that $r_1 = r_2$ and $q_1 = q_2$.

Now if $r_1 \neq r_2$, without loss of generality we can assume that $r_2 > r_1$. Subtracting the two equations above, we obtain

$$b(q_1 - q_2) + (r_1 - r_2) = 0 \Leftrightarrow b(q_1 - q_2) = (r_2 - r_1).$$

This implies that $b|(r_2 - r_1)$, by theorem 3.2 (7) this implies that $b \leq r_2 - r_1$.

On the other hand, we see that

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

We have $b > r_2 - r_1$, but this contradicts $b \leq r_2 - r_1$. So, we must conclude that $r_2 = r_1$.

Now, we see that $b(q_1 - q_2) = r_2 - r_1 = 0$, since $b > 0$ then $q_1 = q_2$. □

Example 3.3.1. *Show that the expression* $\frac{a(a^2+2)}{3}$ *is an integer for all* $a \geq 1$.

Proof. According to the Division Algorithm, every a is of the form $3q$, $3q+1$, or $3q+2$.

For if $a = 3q$ then

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

which clearly is an integer.

For if $a = 3q+1$ then

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

and $\frac{a(a^2+2)}{3}$ is an integer also.

Finally, for if $a = 3q+2$ then

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

an integer once more.

Consequently, our result is established in all cases. □

3.4 Problems

1. Show that any integer of the form $6k+5$ is also the form $3j+2$, but not conversely.

2. Use the Division Algorithm to establish the following:

   a. The square of any integer is either the form $3k$ or $3k+1$.

   b. The cube of any integer has one of the forms: $9k$, $9k+1$, or $9k+8$.

   c. The cube of any integer has one of the forms: $7k$, $7k+1$ or $7k-1$.

   d. The fourth power of any integer is either the form $5k$ or $5k+1$.

3. For $n \geq 1$, prove that $\frac{n(n+1)(2n+1)}{6}$ is an integer.

4. For $n \geq 1$, establish that the integer $n(7n^2+5)$ is of the form $6k$.

5. If n is an odd integer, show that $n^4 + 4n^2 + 11$ is of the form $16k$.

6. Verify that if an integer is simultaneously a square and a cube (as is the case with $64 = 8^2 = 4^3$), then it must be either of the form $7k$ or $7k+1$.

Topic 4

The Euclidean Algorithm

4.1 GCD (Greatest Common Divisor)

Definition 4.1. Let a and b be given integers, with at least one of them different from zero. The greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying the following:

i. $d|a$ and $d|b$

ii. If $c|a$ and $c|b$ then $c \leq d$.

For which $a = 0$ and $b = 0$, we define $\gcd(0, 0) = 0$.

If $e|a$ and $e|b$ then we call e as a *common divisor* of a and b. Now let

$$C(a, b) = \{e : e|a \ \ and \ \ e|b\}, \tag{4.1}$$

that is, $C(a, b)$ is the set of all common divisor of a and b. Note that, since everything divides 0 then $C(0, 0) = \mathbb{Z}$, so there is no largest common divisor of 0 with 0. This is why we must define $\gcd(0, 0)$.

Example 4.1.1. $C(18, 27) = \{-1, 1, -3, 3, -9, 9\}$, *so* $\gcd(18, 27) = 9$.

Example 4.1.2. $C(-15, 36) = \{-1, 1, -3, 3\}$, *so* $\gcd(-15, 36) = 3$.

Example 4.1.3. $C(16, 25) = \{-1, 1\}$, *so* $\gcd(16, 25) = 1$.

Theorem 4.2. *Let* $a, b, c \in \mathbb{Z}$ *with* $\gcd(a, b) = d$, *then*

i. $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$

ii. $\gcd(a + cb, b) = d$.

Proof. There are two item to be prove, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ and $\gcd(a + cb, b) = d$.

i. Let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = d$, we will show that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.
Let $e \in C(\frac{a}{d}, \frac{b}{d})$ then $e|\frac{a}{d}$ and $e|\frac{b}{d}$. Based on the definition 3.1, there are integers k and l such that $\frac{a}{d} = ek$ and $\frac{b}{d} = el$, so that $a = dek$ and $b = del$. Hence, $de|a$ and $de|b$, so that $de \in C(a, b)$. But, since $\gcd(a, b) = d$, then d is the greatest element of $C(a, b)$, hence $de \leq d$, and its only happen if $e = \pm 1$. Thus, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

ii. Let $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = d$, we have to show that

$$\gcd(a + cb, b) = d. \tag{4.2}$$

Let p be any element of $C(a, b)$ then $p|a$ and $p|b$. By theorem 3.2 (3) we see that $p|(a + cb)$, so that $p \in C(a + cb, b)$, hence $C(a, b) \subset C(a + cb, b)$. Now let q be any element of $C(a + cb, b)$. Then again by theorem 3.2 (3), we see that q divides $(a+cb)-cb = a$, so that $q \in C(a, b)$. Hence $C(a+cb, b) \subset C(a, b)$. Thus $C(a+cb, b) = C(a, b)$, and it means that $\gcd(a + cb, b) = \gcd(a, b) = d$.

Hence $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ and $\gcd(a + cb, b) = d$. □

In some cases we are more interested in pairs if integers than sharing no common divisor than ± 1. Such pairs of integers are called *relatively prime*.

Definition 4.3. The integers a and b are called relatively prime if $\gcd(a, b) = 1$.

4.2 LCM (Least Common Multiple)

Definition 4.4. Let $a, b \in \mathbb{Z}$, $a \neq 0$, and $b \neq 0$. The least common multiple of a and b, denoted by $lcm(a, b)$, is the positive integer m satisfying the following:

i. $a|m$ and $b|m$

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

Example 4.2.1. *The positif common multiples of the integers* -12 *and* 30 *are 60, 120, 180,...; hence* $lcm(-12, 30) = 60$.

Theorem 4.5. *For positive integers* a *and* b

$$\gcd(a, b).lcm(a, b) = ab. \tag{4.3}$$

Proof. To begin, put $d = \gcd(a, b)$ and write $a = dr, b = ds$ for integers r and s. If $m = \frac{ab}{d}$, then $m = as = rb$, the effect of which is to make m a (positif) common multiple of a and b.

Now let c be any positif integer that is a common multiple of a and b; say, for definitness, $c = au = bv$. As we know, there exist integers x and y satisfying $d = ax + by$. In consequence,

$$\begin{aligned} \frac{c}{m} &= \frac{cd}{ab} && (4.4)\\ &= \frac{c(ax + by)}{ab} && (4.5)\\ &= \left(\frac{c}{b}\right) x + \left(\frac{c}{a}\right) y && (4.6)\\ &= vx + uy && (4.7) \end{aligned}$$

The equation states that $m|c$, allowing us to conclude that $m \leq c$. Thus, in accordance with definition (above), $m = lcm(a, b)$; that is,

$$lcm(a, b) = \frac{ab}{d} = \frac{ab}{\gcd(a, b)} \tag{4.8}$$

which is what we started out to prove. □

Corollary 4.6. *For any choice of positif integers* a *and* b, $lcm(a, b) = ab$ *iff* $\gcd(a, b) = 1$.

4.3 The Euclidean Algorithm

The greatest common divisor of two integers can be found by listing all their positive divisors and choosing the largest one common to each; but this is cumbersome for large numbers. The division algorithm provides a more efficient method to compute $\gcd(a, b)$. Prove that if $a > 0$ then $\gcd(a, 0) = a$ and $\gcd(a, a) = a$

Lemma 4.7. *Let* $a > b > 0$. *If* $a = bq + r$ *then*

$$\gcd(a, b) = \gcd(b, r). \tag{4.9}$$

Proof. It suffices to show that $C(a,b) = C(b,r)$, that is, the common divisors of a and b are the same as the common divisors of b and r. To show this, first let $d|a$ and $d|b$. Note that $r = a - bq$, which is a linear comination of a and b. So, by theorem 3.2.(3) $d|r$. Thus $d|b$ and $d|r$. Using theorem 3.2.(3) again and using the fact that $a = bq + r$ is a linear combination of b and r, we have $d|a$. So $d|a$ and $d|b$. We have thus shown that $C(a,b) = C(b,r)$. So $\gcd(a,b) = \gcd(b,r)$. □

By use of Division Algorithm and lemma 4.7 we may described **The Euclidean Algorithm** as follows:

i. Apply the Division Algorithm to a and b to get

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

ii. If $r_1 = 0$ then $b|a$ and $\gcd(a,b) = b$. If $r_1 \neq 0$, repeat step 1 (divide b by r_1) to get q_2 and r_2 satisfying

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

iii. If $r_2 = 0$ then $\gcd(a,b) = r_1$. If $r_2 \neq 0$, repeat step 1 (divide r_{n-1} by r_n) to get q_{n+1} and r_{n+1} satisfying

$$r_{n-1} = q_{n+1} r_n + r_{n+1}, \qquad 0 \leq r_{n+1} < r_n$$

iv. The division prcess continues until some zero reminder appears ($r_{n+1} = 0$), then $\gcd(a,b) = r_n$.

4.4 Discussion

Each group discuss one of the sections below, subsection 4.4.1 is for the groups: 1, 6, and **7**, subsection 4.4.2 is for the groups: 2, 5, and **8** and subsection 4.4.3 is for the groups: 3, 4, and **9**. Each section will presents by selected group.

4.4.1 Bézout's Identity

The Euclidean Algorithm also provides a way of proofing the following theorem

Theorem 4.8. *For all integers a and b there exist integer x and y such that*

$$\gcd(a, b) = ax + by. \tag{4.10}$$

Proof. See Clark, 2002: page 25, and Burton, 1998: page 22. □

Equation (4.10) is called *Bézout's Identity* and turns out to be very useful.
Use the Euclidean Algorithm to answer the following problems.

1. Find x and y of Bézout's identity $\gcd(480, 245) = 480x + 245y$
2. What are the coefficients of 28231 and of 1515 in Bézout's identity for $\gcd(28231, 1515)$?
3. Determine the greatest common divisor of the real polynomials $f(x) = x^3+3x^2-x-3$ and $g(x) = x^2 + 3x + 2$, and find a Bézout's Identity.

4.4.2 The Diophantine Equation

The simplest type of Diophantine equation that we shall consider is the linear Diophantine equation in two unknowns:

$$ax + by = c$$

where a, b, c are given integers and a, b are not both zero. A solution of this equation is a pair of integers x_0 and y_0 which, when substitued into the equation, satisfy it; that is, we ask that $ax_0 + by_0 = c$.

Theorem 4.9. *The linear diophantine equation $ax + by = c$, with $a, b \in \mathbb{Z}$, and a, b are not both zero, admits solution $x, y \in \mathbb{Z}$ iff $d|c$, where $d = \gcd(a, b)$. If x_0, y_0 is any particular of this equation, then all other solutions are given by*

$$x = x_0 + \left(\frac{b}{d}\right) t \qquad y = y_0 - \left(\frac{a}{d}\right) t$$

Proof. See Burton, 1998: page 34, and Baldoni, et al., 2009: page 20. □

Use the Euclidean Algorithm to answer the following problems.

1. Find x and y of the Diophantine equation $95 = 480x + 245y$
2. Find the coefficients of 28762 and of 1515 in Diophantine equation,

$$13 = 28231x + 1515y.$$

3. A farmer purchased one hundred head of livestock for a total cost of $4000. Prices were as follow: calves, $120 each; lambs, $50 each; and piglets, $25 each. If the farmer obtained at least one animal of each type, how many did he buy?

4.4.3 Continued Fractions

Definition 4.10. A *finite continued fractions* is a fraction of the form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

where $a_1, a_2, \cdots, a_n \in \mathbb{R}$, all positive with the possible exception of a_1. The number $a_2, \cdots, a_n$ are called *partial denominators*, or *partial quotiens*, of the fraction.
A finite continued fraction is said to be *simple* if all of its partial quotiens are integer.

Use the Euclidean Algorithm to answer the following problems.

1. Write $\frac{480}{245}$ as a continued fraction.

2. What is the expression of $\frac{28231}{1515}$ in a continued fraction?

3. What is the expression of the quotiens of two successive Fibonacci number, $\frac{f_{n+1}}{f_n}$, in a continued fraction?

Topic 5

Counting in Arbitrary Base

5.1 Positional Notation of Numbers

When we write the number 2532 in base 10, we mean the following expression:

$$2562 = 2 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10^1 + 2 \cdot 10^0.$$

The writen above is the *positional* notation in base 10.Examining further this example, notice that dividing 2562 by 10 we get

$$2562 = 256 \cdot 10 + 2,$$

that is 2, the rightmost digit, gives the remainder of the division by 10 of the original number. Going on, we divide the quotient we found by 10 again, we get

$$256 = 25 \cdot 10 + 6.$$

So the second digit from the right, that is 6, once more gives the remainder of the division, and is so uniquely determined. If we continue our algorithm then we found that the next remainder will be 5 and 2. In conclusion, three digits appearing in the decimal representasion of the number are uniquely determined by successive divisions.

Theorem 5.1. *Let β be an integer greather than 1. Then, for each $n \in \mathbb{N}$ there exist a non-negative integer k and $k+1$ integers a_0, a_1, ..., a_k such that $0 \leq a_i < \beta$, for each $i = 0$, ..., k, these being the only such integers satisfying:*

$$n = a_k\beta^k + a_{k-1}\beta^{k-1} + \cdots + a_1\beta + a_0. \tag{5.1}$$

Proof. Apply the Euclidean algorithm in the following way: divide n by β obtaining

$$n = q_1 \cdot \beta + a_0, \qquad 0 \leq a_0 < \beta.$$

If $q_1 \neq 0$, divide it by β obtaining

$$q_1 = q_2 \cdot \beta + a_1, \qquad 0 \leq a_1 < \beta.$$

Going on the same way we get

$$\begin{aligned} q_2 &= q_3 \cdot \beta + a_2, && 0 \leq a_2 < \beta \\ q_3 &= q_4 \cdot \beta + a_3, && 0 \leq a_3 < \beta \\ &\vdots \\ q_{k-1} &= q_k \cdot \beta + a_{k-1}, && 0 \leq a_{k-1} < \beta. \end{aligned}$$

Since $n > q_1 > q_2 > \cdots > 0$ is a strictly decreasing sequence of positive integers, this process must eventually end, say, at the $(k-1)$ stage, that is $q_k < \beta$. It means that if we continue our step then we will get $q_{k+1} \leq 0$. Setting $a_k = q_k$, proceed backwards, and we will reach the representation

$$n = a_k\beta^k + a_{k-1}\beta^{k-1} + \cdots + a_1\beta + a_0 \tag{5.2}$$

which was our aim. The uniqueness of this expression is clear, as the digits a_i appearing in it are uniquely determined (Theorem 3.5) as the remainders of the successive divisions. □

Example 5.1.1. *Express the ten-base number, 2562, in the number of base 9.*

Answer: Apply the Euclidean algorithm in the following way:

$$\begin{aligned} 2562 &= 284 \cdot 9 + 6 \\ 248 &= 27 \cdot 9 + 5 \\ 27 &= 3 \cdot 9 + 0 \end{aligned}$$

Thus, based on the Theorem 5.1 above, we have that $2562 = 3056_9$.

Example 5.1.2. *By use of Theorem 5.1 above, we can find that* $2562 = 101000000010_2$.

The choice of 10 as a notational base is purely conventional; in fact, along the centuries different cultures used different bases in their numerical systems: Babylonians used the base 60, Mayans the base 20 and so on. Computers use the base 2 and that why we called it the *binary system*. Each digits in the binary system conveys one *bit* of information; the symbol 0 interpreted by the computer as the command *off* and the symbol 1 as the command *on*. Other bases used in computer science are 8 and 16.

5.2 Base 2 and Its Operations

We describe now the rules to perform the four operation $(+, -, \div, \times)$ when we represent the numbers in base 2.

5.2.1 Addition

The addition tables we must learn in order to perform additions in base 2 are very simple:

$$0 + 0 = 0, \qquad 0 + 1 = 1,$$
$$1 + 0 = 1, \qquad 1 + 1 = 10.$$

Let $a = \sum_{i=0}^{n} a_i \cdot 2^i$ and $b = \sum_{i=0}^{n} b_i \cdot 2^i$ be two positif integers. Then

$$a + b = \sum_{i=0}^{n} (a_i + b_i) \cdot 2^i.$$

Now use the addition table and remember that $1 + 1 = 10$, this means that the term $(a_i + b_i) \cdot 2^i = 2^{i+1}$, if $a_i = b_i = 1$, and so we must *carry* 1 to the next coefficient, so the coefficient of 2^{i+1} becomes $a_{i+1} + b_{i+1} + 1$, while the coefficient of 2^i is 0.

Example 5.2.2. *Suppose we have to sum the numbers: a.)* 10111111 *and* 1011*; b.)* 1100110 *and* 101010

```
carries  1 1 1 1 1 1 1          carries  1 0 1 1 1
     1 0 1 1 1 1 1 1                  1 1 0 0 1 1 0
           1 0 1 1                    1 0 1 0 1 0
   ---------------- +               ---------------- +
   1 1 0 0 1 0 1 0                  1 0 0 1 0 0 0 0
```

5.2.3 Subtraction

In the same way, if $a = \sum_{i=0}^{n} a_i \cdot 2^i$ and $b = \sum_{i=0}^{n} b_i \cdot 2^i$ and $a \geq b$, then

$$a - b = \sum_{i=0}^{n} (a_i - b_i) \cdot 2^i.$$

Here we face the problem if for some i we have $a_i = 0$ and $b_i = 1$. In this case, in the row representing a, we *borrow* a 1 from the firs 1 appearing when we move leftwards starting form a_i. Let us see how we actually perform the subtraction of two numbers:

Example 5.2.4. *Suppose we want to subtract* 100001 *by* 1010

Answer: We have here $a = 100001 = 2^5 + 2^0$ and $b = 1010 = 2^3 + 2^1$,

$$\begin{aligned}
a - b &= 2^5 - 2^3 - 2^1 + 2^0 = 2^5 - 2^3 + (-2^2 + 2^2) - 2^1 + 2^0 \\
&= 2^5 - 2^3 - 2^2 + 2 \cdot 2^1 - 2^1 + 2^0 = 2^5 - 2^3 - 2^2 + (2-1)2^1 + 2^0 \\
&= 2^5 - 2^3 + (-2^3 + 2^3) - 2^2 + 2^1 + 2^0 = 2^5 - 2^3 - 2^3 + 2 \cdot 2^2 - 2^2 + 2^1 + 2^0 \\
&= 2^5 - 2 \cdot 2^3 + (2-1)^2 + 2^1 + 2^0 = 2^5 - 2^4 + 2^2 + 2^1 + 2^0 \\
&= 2^5 + (-2^5 + 2^5) - 2^4 + 2^2 + 2^1 + 2^0 = 2 \cdot 2^4 - 2^4 + 2^2 + 2^1 + 2^0 \\
&= (2-1)2^4 + 2^2 + 2^1 + 2^0 = 2^4 + 2^2 + 2^1 + 2^0 \\
&= 10111
\end{aligned}$$

5.2.5 Multiplication

If we are considering the number $a = \sum_{i=0}^{n} a_i \cdot 2^i$, then $2^j \cdot a = \sum_{i=0}^{n} a_i \cdot 2^{i+j}$, that is, $(2^j \cdot a)$ may written simply moving leftwards by j positions the digits of a and putting on their right the same number of zeros. On the other hand, suppose we have the numbers

$$a = \sum_{i=0}^{n} a_i \cdot 2^i \quad \textit{and} \quad b = \sum_{j=0}^{m} b_j \cdot 2^j.$$

Suppose the non-zero digits of b are exactly the h digits $b_{j_1}, b_{j_2}, \cdots, b_{j_h}$, that is, let

$$b = \sum_{l=1}^{h} 2^{j_l}.$$

In this case, we have

$$a \cdot b = \sum_{l=1}^{h} \sum_{i=0}^{n} a_i \cdot 2^{i+j_l}.$$

Example 5.2.6. *Suppose we deal with a multiplication of* 11101 *by* 1101

```
      1 1 1 0 1
        1 1 0 1
  ---------------  x
      1 1 1 0 1
    1 1 1 0 1
  1 1 1 0 1
---------------------  +
1 0 1 1 1 1 0 0 1
```

5.2.7 Division

Finally, as regards *division*, we may proceed in the same way as in base 10.

Example 5.2.8. *Consider* $a = 11001$ *and* $b = 101$. *What is the value of* $a \div b$ *in base 2?*

```
          1 0 1
        ---------
1 0 1 ) 1 1 0 0 1
        1 0 1
      -----------  -
          1 0 1
          1 0 1
      -----------  -
                0
```

5.3 Base 8 and 16 (Discussion)

Each group discuss one of the sections below, subsection 5.3.1 is for the groups: 3, 4, **5**, 7, and 8, and subsection 5.3.2 is for the groups: 1, 2, **6**, and 9. Each section will presents by selected group.

5.3.1 Base 8

Discuss within your group about: transforming a number in base 10 to a number in base 8 and vice versa, transforming a number in base 2 to a number in base 8 and vice versa, and explain the four operations $(+, -, \div, \times)$ in base 8.

5.3.2 Base 16

Discuss within your group about: transforming a number in base 10 to a number in base 16 and vice versa, transforming a number in base 2 to a number in base 16 and vice versa, and explain the four operations $(+, -, \div, \times)$ in base 16.

Topic 6

Prime Factorization

6.1 Fundamental Theorem of Arithmetic

Theorem 6.1. ***Fundamental Theorem of Arithmetic.*** *Every integer $n > 1$ can be writen uniquely in the form*

$$n = p_1 p_2 p_2 \cdots p_s,$$

where s is a positive integer and p_1, p_2, ...p_s are primes satisfying

$$p_1 \leq p_2 \leq \cdots \leq p_s.$$

To prove Theorem 6.1, we need to establish some lemmas.

Lemma 6.2. *If $a|bc$ and $\gcd(a, b) = 1$ then $a|c$*

Proof. See Clark, 2002: page 38 and Burton, 1998: page 24. □

Lemma 6.3. ***(Euclid's Lemma)*** *If p is a prime and $p|ab$ then $p|a$ or $p|b$*

Proof. See Clark, 2002: page 38 and Burton, 1998: page 40. □

Lemma 6.4. *Let p be prime and let $a_1, a_2, \cdots, a_n$ be integers and $n \geq 1$. If $p|a_1 a_2 \cdots a_n$, then $p|a_i$ for at least one $i \in \{1, 2, \cdots, n\}$.*

Proof. See Clark, 2002: page 39. □

So, now is the time to prove Theorem 6.1.

Proof. **existence**

If n is a prime, then there is nothing more to prove. If n is composite, then there exists an integer d satisfying $d|n$ and $d < n$. Among all such integers d, we can choose p_1 the smallest by Well-Ordering Principle. Then p_1 must be prime, otherwise it would have a divisor q with $1 < q < p_1$; but then $q|p_1$ and $p_1|n$ imply that $q|n$, which contradicts the choice of p_1 as the smallest positive divisor, not equal to 1, of n.

We therefore may write $n = p_1 n_1$, where p_1 is prime and $1 < n_1 < n$. If n_1 happens to be a prime, then we have our representation. In the contrary case, the argument is repeated to produce a second prime number p_2 such that $n_1 = p_2 n_2$; that is

$$n = p_1 p_2 n_2, \quad 1 < n_2 < n_1. \tag{6.1}$$

If n_2 is a prime, then it is not necessary to go further. Otherwise $n_2 = p_3 n_3$, with p_3 a prime;

$$n = p_1 p_2 p_3 n_3, \quad 1 < n_3 < n_2. \tag{6.2}$$

The decreasing sequence

$$n > n_1 > n_2 > n_3 > \cdots > 1 \tag{6.3}$$

cannot continue indefinitely, so after a finite number steps n_{k-1} is a prime, call it, p_s. This lead to the prime factorization

$$n = p_1 p_2 \cdots p_s. \tag{6.4}$$

uniqueness

Suppose that $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ where $s \geq 1, t \geq 1$, $p_1, p_2, \cdots, p_s, q_1, q_2, \cdots, q_t$ are primes, $p_1 \leq p_2 \leq \cdots \leq p_s$, and $q_1 \leq q_2 \leq \cdots \leq q_t$. We will show by mathematical induction on s that $s = t$ and $p_i = q_i$ for $i = 1, 2, \cdots t$.

Suppose $s = 1$, then $n = p_1$ is prime and we have

$$p_1 = n = q_1 q_2 \cdots q_t.$$

If $t > 1$, this contradicts the fact that p_1 is prime, so $t = 1$ and we have $p_1 = q_1$ as desired. Now assume the result holds for all s such that $1 \leq s \leq k$. We want to show that it holds for $s = k + 1$. So assume

$$n = p_1 p_2 \cdots p_k p_{k+1}$$

and

$$n = q_1 q_2 \cdots q_t$$

where $p_1 \leq p_2 \leq \cdots \leq p_{k+1}$ and $q_1 \leq q_2 \leq \cdots \leq q_t$.

Clearly that $p_{k+1}|n$ so $p_{k+1}|q_1 q_2 \cdots q_t$. By Lemma 6.4, $p_{k+1}|q_i$ for some $i \in \{1, 2, \cdots t\}$. Since p_{k+1} and q_i are primes then $p_{k+1} = q_i$ (Why?). Hence $p_{k+1} = q_i \leq q_t$.

By the similar argument $q_t|n = p_1 p_2 \cdots p_{k+1}$ then $q_t = p_j$ for some $j \in \{1, 2, \cdots k+1\}$. Hence $q_t = p_j \leq p_{k+1}$. This shows that

$$p_{k+1} \leq q_t \leq p_{k+1}$$

so $p_{k+1} = q_t$. Note that

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

since $p_{k+1} = q_t$ we can cancel this prime fromboth sides and we have

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_{t-1}.$$

By induction hypothesis, $k = t-1$ and $p_i = q_i$ for $i = 1, 2, \cdots t-1$. Thus we have $k+1 = t$ and $p_i = q_i$ for $i = 1, 2, \cdots t-1$. So this theorem holds. □

By the Fundamental Theorem of Arithmetic, it is clear that if $n > 1$ then it can be written uniquely in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}, \tag{6.5}$$

for some $s \geq 1$. The term (6.5) called the *canonical* form of n. The Fundamental Theorem of Arithmetic also helps us to find gcd and lcm of 2 or more integers easily.

Suppose there are k positive integers, $n_1, n_2, \cdots n_k$, where $n_i > 1$ for all $i \leq k$. We can write these integers in the canonical form

$$\begin{aligned} n_1 &= p_1^{a1_1} p_2^{a1_2} \cdots p_s^{a1_s} \\ n_2 &= p_1^{a2_1} p_2^{a2_2} \cdots p_s^{a2_s} \\ &\cdots \\ n_k &= p_1^{ak_1} p_2^{ak_2} \cdots p_s^{ak_s}. \end{aligned}$$

Then

$$\gcd(n_1, n_2, \cdots, n_k) = p_1^{\min\{a1_1, a2_1, \cdots ak_1\}} p_2^{\min\{a1_2, a2_2, \cdots ak_2\}} \cdots p_s^{\min\{a1_s, a2_s, \cdots ak_s\}}$$

and

$$lcm(n_1, n_2, \cdots, n_k) = p_1^{\max\{a1_1, a2_1, \cdots ak_1\}} p_2^{\max\{a1_2, a2_2, \cdots ak_2\}} \cdots p_s^{\max\{a1_s, a2_s, \cdots ak_s\}}.$$

Example 6.1.1. *Find the gcd and lcm of 198, 216, and 252.*

Answer: It is clear that

$$\begin{aligned} 198 &= 2 \cdot 3^2 \cdot 11 \\ 216 &= 2^3 \cdot 3^3 \\ 252 &= 2^2 \cdot 3^2 \cdot 7 \end{aligned}$$

Thus

$$\begin{aligned} \gcd(198, 216, 252) &= 2^{\min\{1,2,3\}} \cdot 3^{\min\{2,3\}} \cdot 7^{\min\{0,1\}} \cdot 11^{\min\{0,1\}} \\ &= 2^1 \cdot 3^2 \cdot 7^0 \cdot 11^0 = 18 \\ lcm(198, 216, 252) &= 2^{\max\{1,2,3\}} \cdot 3^{\max\{2,3\}} \cdot 7^{\max\{0,1\}} \cdot 11^{\max\{0,1\}} \\ &= 2^3 \cdot 3^3 \cdot 7^1 \cdot 11^1 = 16632 \end{aligned}$$

Theorem 6.5. *If $n > 1$ is composite then it has a prime divisor $p \leq \sqrt{n}$*

Proof. See Clark, 2002: page 32. □

Topic 7

Congruences

7.1 Basic Properties

Definition 7.1. Let n be a fixed integer. Two integers a and b are said to be congruent modulo n, symbolized by

$$a \equiv b(\mod n)$$

if $n|a-b$.

Example 7.1.1. *Consider $n = 7$, prove that*

$3 \equiv 24(\mod 7) why???$ $\quad -31 \equiv 11(\mod 7) why???$ $\quad -15 \equiv -64(\mod 7) why???$

yang ga kongruen???

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

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

Then, by definition of congruence, $a \equiv r(\mod n)$. Since there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values 0, 1, $\cdots$, $n-1$; in particular, $a \equiv 0(\mod n)$ iff $n|a$. The set of n integers 0, 1, $\cdots$, $n-1$ is called the set of *least positive residues modulo n*.

In general, a collection of n integers a_1, a_2, $\cdots$, a_n is said to form a *complete set of residues modulo n* if a_k is congruent modulo n to 0, 1, $\cdots$, or $n-1$. For instance, -12, -4, 11, 13, 22, 82, and 91 constitute a complete set of residues modulo 7.

The next theorem shows that congruence is an equivalence relation.

Theorem 7.2. *(Congruence is an equivalence relation.) For all $a, b, c \in \mathbb{Z}$ and $m > 0$ we have*

i $a \equiv a(\mod m)$ {*reflexivity*}

ii *If* $a \equiv b(\mod m)$ *then* $b \equiv a(\mod m)$ {*symmetry*}

iii *If* $a \equiv b(\mod m)$ *and* $b \equiv c(\mod m)$ *then* $a \equiv c(\mod m)$ {*transitivity*}

Proof. i $a - a = 0 = 0.m$ so $m|a - a$ hence $a \equiv a(\mod m)$.

ii If $a \equiv b(\mod m)$ then $m|a - b$ it means that $a - b = qm$ hence $b - a = (-q)m$ so $m|b - a$ hence $b \equiv a(\mod m)$

iii If $a \equiv b(\mod m)$ and $b \equiv c(\mod m)$ then $m|a - b$ and $m|b - c$. By linearity property (Theorem 3.2), we have $m|(a - b) + (b - c) = a - c$ so $a \equiv c(\mod m)$.

hehehe.... □

Congruence is an equivalence relation so we can make sets those we called *equivalence classes* of integers by congruence relation.

Example 7.1.2. *We can make 5 equivalence classes of integers by congruence relation modulo 5, those are:*

1. $\bar{0}_5 = [0]_5 = \{\cdots, -10, -5, 0, 5, 10, \cdots\}$
   ($\bar{0}_5$ is a set of integers such that if $a \in \bar{0}_5$ then $a \equiv 0(\mod 5)$)

2. $\bar{1}_5 = [1]_5 = \{\cdots, -9, -4, 1, 6, 11, \cdots\}$
   ($\bar{1}_5$ is a set of integers such that if $a \in \bar{1}_5$ then $a \equiv 1(\mod 5)$)

3. $\bar{2}_5 = [2]_5 = \{\cdots, -8, -3, 2, 7, 12, \cdots\}$
   ($\bar{2}_5$ is a set of integers such that if $a \in \bar{2}_5$ then $a \equiv 2(\mod 5)$)

4. $\bar{3}_5 = [3]_5 = \{\cdots, -7, -2, 3, 8, 13, \cdots\}$
   ($\bar{3}_5$ is a set of integers such that if $a \in \bar{3}_5$ then $a \equiv 3(\mod 5)$)

5. $\bar{4}_5 = [4]_5 = \{\cdots, -6, -1, 4, 9, 14, \cdots\}$
   ($\bar{4}_5$ is a set of integers such that if $a \in \bar{4}_5$ then $a \equiv 4(\mod 5)$)

7.2 Linear Congruences

An equation of the form $ax \equiv b(\mod n)$ is called *linear congruence*, and by a solution of such equation we mean an integer x_0 for which $ax_0 \equiv b(\mod n)$. By definition, $ax_0 \equiv b(\mod n)$ iff $n|ax_0 - b$ iff $ax_0 - b = ny_0$. Thus the problem of finding all integers which satisfy the linear congruence $ax \equiv b(\mod n)$ is identical with that of obtaining all solutions of the linear Diophantine equation $ax - ny = b$ (Topic 5.2.2).

Theorem 7.3. *The linear congruence* $ax \equiv b(\mod n)$ *has a solution iff* $d|b$ *where* $d = \gcd(a, n)$.

References

[1] Baldoni, M. W., Ciliberto, C., and Cattaneo, G. M. P. 2009. *Elementary Number Theory, Cryptography, and Codes*. Springer-Verlag Berlin Heidelberg.

[2] Burton, D. M. 1998. *Elementary Number Theory*. Fourth Edition. The McGraw-Hill Companies, Inc.

[3] Clark, W. E. 2002. *Elementary Number Theory*.

[4] Jacoby, O. and Benson, W.H. 1965. *Mathematics for Pleasure*. Fawcett World Library: New York.