CONTENTS

Preface

This lecture notes is written based on our experiences in giving 'Elementary Number Theory Course" at the Department of Mathematics Education, Faculty of Mathematics and Science Education, Indonesia University of Education, in 2009. During the lectures we used several Elementary Number Theory textbooks either English or Indonesian textbooks. However, the main source of the notes is based on the book written by James K. Strayer, "Elementary Number Theory" published by PWS Publishing Company, 1994. Therefore, the organization of the notes mostly follows this book.

The notes consist of three chapters. Chapter 1 contains several important topics needed to understand next chapters, namely proof techniques (direct and indirect proofs techniques, and Mathematical Induction) and properties of the integers. In Chapter 2, we discuss Divisibility (Definition, Prime Numbers, Greatest Common Divisors, the Euclidean Algorithm, and the Fundamental Theorem of Arithmetic). And in Chapter 3, we discuss Congruences (Definition, Linear Conruences in One Variable, The Chinese Remainder Theorem, Wilson's, Euler's and Fermat's Theorems).

We hope this lecture notes will be useful for students in attending the Elementary Number Theory course in the future time. We also open for suggestions and constructive criticizes from the readers who want this lecture notes better.

Bandung, August 2009

Turmudi and Al Jupri

Chapter 1. Preliminary Topics

1.1 Direct Proofs

Let P and Q be statements. The construction of **a direct proof** of $P \Longrightarrow Q$ involves of a string of statements $R_1, R_2, \ldots, R_n$ such that

$$P \Longrightarrow R_1, R_2 \Longrightarrow R_2, \ldots, R_n \Longrightarrow Q.$$

This construction is usually not an easy task; it may take insight, intuition, and considerable effort. Often it also requires experience and luck.

Example 1.1: Prove the following theorem

The square of an odd integer is also an odd integer.

Proof:

If n is an odd integer, then $n = 2k + 1$ for some integer k. Then the square of n is given by $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. If we let $m = 2k^2 + 2k$, then m is an integer (why?). Therefore, n^2 is an odd integer.

Q.E.D.

1.2 Indirect Proofs

a. Contrapositive proofs

Instead of proving $P \Longrightarrow Q$, we may prove its logically equivalent contrapositive: not $Q \Longrightarrow$ not P.

Example 1.2: Prove the following theorem

If n is an integer and n^2 is even, then n is even.

Proof:

The contrapositive of this theorem is: If n is odd, then n^2 is odd. But this actually equals to theorem in Example 1.1. Therefore, the proof is equal to the proof of theorem in Example 1.1.

b. Proof by contradiction

This method of proof employs the fact if C is a contradiction (i.e., a statement that is always false, such as "1 = 2"), then two statements

$$(P \text{ and } (\text{not } Q)) \Longrightarrow C,\ P \Longrightarrow Q$$

are logically equivalent. Thus we establish $P \Longrightarrow Q$ by showing that the statement (P and (not Q)) implies a contradiction.

Example 1.3: Prove the following theorem

There are infinitely many prime numbers.

Proof:

Assume, by way of contradiction, that there are only finitely many prime numbers, say p_1, p_2, …, p_n. Consider the number $N = p_1 p_2 \ldots p_n + 1$. Now N has a prime divisor, say p. So $p = p_i$ for some i, $i = 1, 2, \ldots, n$. Then $p|N - p_1 p_2 \ldots p_n$, which implies that $p|1$, a contradiction. Hence, there are infinitely many prime numbers.

1.3 Mathematical Induction

a. Principle of Mathematical Induction (First Version)

For each $n \in N$, let $P(n)$ be a statement about n. Suppose that:

(1) $P(1)$ is true.

(2) For every $k \in N$, if $P(k)$ is true, then $P(k + 1)$ is true.

Then $P(n)$ is true for all $n \in N$.

b. Principle of Mathematical Induction (Second Version)

Let $n_0 \in N$ and let $P(n)$ be a statement for each natural number $n \geq n_0$. Suppose that:

(1) The statement $P(n_0)$ is true.

(2) For all $k \geq n_0$, the truth of $P(k)$ implies the truth of $P(k+1)$.

Then $P(n)$ is true for all $n \geq n_0$.

Example 1.4: Prove that for each $n \in N$ the following statement is true.

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

Proof:

Let $P(n)$ be the statement: $1 + 3 + 5 + \ldots + (2n - 1) = n^2$.

(1) $P(1)$ is $1 = 1^2$, it is obviously true.

(2) Let $P(k)$ is true, namely $1 + 3 + 5 + \ldots + (2k - 1) = k^2$.

For $n = k + 1$, then $P(k + 1)$ is the following:

$$1 + 3 + 5 + \ldots + (2k - 1) + (2(k + 1) - 1) = k^2 + 2(k + 1) - 1$$
$$= k^2 + 2k + 2 - 1$$
$$= k^2 + 2k + 1$$
$$= (k + 1)^2$$

This last statement means $P(k + 1)$ is true. Therefore, we conclude that $P(n)$ is true for all $n \in N$.

Example 1.5: Prove that $7^n - 2^n$ is always divisible by 5, for each $n \in N$.

Proof:

Let $P(n)$ be the statement $7^n - 2^n$ is always divisible by 5, for each $n \in N$.

(1) $P(1)$ is $7^1 - 2^1 = 5$ is divisible by 5. So, $P(1)$ is true.

(2) Let $P(k)$ is true, namely $7^k - 2^k$ is always divisible by 5, then for $n = k + 1$, $P(k+1)$ is the following:

$$7^{k+1} - 2^{k+1} = 7^k.7 - 2^k.2$$
$$= 7^k.7 - 7.2^k + 7.2^k - 2^k.2$$
$$= 7(7^k - 2^k) + 2^k(7 - 2)$$

Since $7^k - 2^k$ is always divisible by 5 and $7 - 2 = 5$ is also divisible by 5, then $7(7^k - 2^k) + 2^k(7 - 2)$ is divisible by 5. This means $P(k+1)$ is true. Thus, $P(n)$ is true for each $n \in N$.

Example 1.6: Prove that $n^2 > n + 1$, for each positive integer $n \geq 2$.

Proof:

Let $P(n)$ be the statement $n^2 > n + 1$, for each positive integer $n \geq 2$.

(1) $P(2)$ is $2^2 = 4 > 2 + 1 = 3$, so $P(2)$ is true.

(2) Let $P(k)$ is true, namely $k^2 > k + 1$, for each positive integer $k \geq 2$. Then for $n = k + 1$, $k \geq 2$, $P(k + 1)$ is the following:

$$(k + 1)^2 = k^2 + 2k + 1 \geq (k + 1) + 2k + 1 = k + 2 + 2k$$
$$\geq (k + 1) + 1.$$

This last statement means $P(k + 1)$ is true. Therefore, $P(n)$ is true for each positive integer $n \geq 2$.

Exercises 1.1

1. Prove that
   $2 + 4 + 6 + \ldots + 2n = n(n+1)$, for each $n \in N$.

2. Prove that $n^2 \leq 2^n$, for n $\in N$ with $n \geq 4$.
3. Prove that $2^n > n^3$ for each $n \in N$ with $n > 9$.
4. Prove that $n^5 - n$ is divisible by 5 for each $n \in N$.
5. Prove that $n^3 - 4n + 6$ is divisible by 3.
6. Prove that $11^n - 4^n$ is divisible by 7 for each $n \in N$.
7. Prove that
   $1^3 + 2^3 + 3^3 + \ldots + n^3 = (1 + 2 + 3 + \ldots + n)^2$ for each $n \in N$.

1.4 Properties of Integers

In the elementary number theory course, we study the system of integers. This system consists of the set of integers $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots.\}$ and properties of this set under the operations of addition and multiplication, and under the usual ordering relation "less than". The important properties of the integers are summarized below:

1. If $a, b \in Z$, then $a + b \in Z$ (Closure property of addition).
2. If $a, b \in Z$, then $a.b \in Z$ (Closure property of multiplication).
3. If $a, b \in Z$, then $a + b$ = b + a (Commutative property of addition).
4. If $a, b \in Z$, then $a.b = b.a$ (Commutative property of multiplication).
5. If $a, b, c \in Z$, then $(a + b) + c = a + (b + c)$ (Associative property of addition).
6. If $a, b, c \in Z$, then $(a.b).c = a\ (bc)$. (Associative property of multiplication).

7. If $a, b, c \in Z$, then $a(b + c) = ab + ac$ (Distributive property of multiplication over addition).
8. If $a \in Z$, then $a + 0 = 0 + a = a$ (Additive identity property).
9. If $a \in Z$, then $a.1 = 1.a = a$ (Multiplicative identity property)
10. If $a \in Z$, then $a + (-a) = (-a) + a = 0$. (Additive inverse property). If $a, b \in Z$, then $a + (-b)$ is written as $a - b$.
11. If $a \in Z$, then $a.0 = 0.a = 0$ (Zero property of multiplication).
12. If $a, b, c \in Z$ and $a + b = a + c$, then $b = c$ (Cancellation property of addition).
13. If $a, b, c \in Z$, a $\neq$ 0, and $ab = ac$, then $b = c$ (Cancellation property of multiplication)
14. If $a \in Z$, then exactly one of the following statements is true: (i) $a < 0$, (ii) $a = 0$, and (iii) $a > 0$ (Trichotomy law).
15. (i) If $a, b, c \in Z$ and $a < b$, then $a + c < b + c$.

    (ii) If $a, b, c \in Z$, $a < b$ and $c > 0$, then $ac < bc$

    (iii) If $a, b, c \in Z$, $a < b$ and $c < 0$, then $ac > bc$.

    (Properties of inequality)
16. Every nonempty set of positive integers contains a least element (Well-ordering property).

In this lecture notes, the properties above are taken as axioms of the system of integers.

Chapter 2. Divisibility and Factorization

2. 1 Divisibility

Definition 2.1: Let $a, b \in Z$. Then a divides b, denoted $a|b$, if there exists $c \in Z$ such that $b = ac$. If $a|b$, then a is said to be a divisor or factor of b. The notation $a \nmid b$ means that a does not divide b.

Example 2.1

(1) $4|12$ since there exists $c \in Z$ such that $12 = 4.c$, where $c = 3$. Hence, 4 is a divisor of 12.

(2) $4 \nmid 11$ since there does not exist $c \in Z$ such that $11 = 4c$. Here $c = 4/11$ which is not element of Z. Thus, 4 is not a divisor of 11.

(3) $5|0$ since there exist $c \in Z$ such that $0 = 5c$, where $c = 0$.

Theorem 2.1: Let $a, b, c \in Z$. If $a|b$ and $b|c$, then $a|c$.

Proof: (See hand-writing notes)

Theorem 2.2: Let $a, b, c, m, n \in Z$. If $c|a$ and $c|b$, then $c|(ma + nb)$.

Proof: (see hand-writing notes)

Definition 2.2: The expression $ma + nb$ in the Thorem 2.2 is said to be an integral linear combination of a and b.

Definition 2.3: Let $x \in R$. The greatest integer function of x, denoted $[x]$, is the greatest integer less than or equal to x.

Lemma 2.3: Let $x \in R$. Then $x - 1 < [x] \leq x$.

Proof:

Theorem 2.4: (The Division Algorithm) Let $a, b \in Z$ with $b > 0$. Then there exist unique q, $r \in Z$ such that

$$a = bq + r, \quad 0 \leq r < b$$

(q stands for *quotient* and r stands for *remainder*).

Proof:

Definition 2.4: Let $n \in Z$. Then n is said to be even if $2|n$ and n is said to be odd if $2 \nmid n$.