# 6: An introduction to Number Theory

## 6.1 The Division ALgorithm and the Well-Ordering Principle.

### The Well Ordering Principle (WOP):

*Every nonempty subset on $\mathbb{Z}^+$ has a smallest element; that is, if $S$ is a nonempty subset of $Z^+$, then there exists $a \in S$ such that $a \leq x$ for all $x \in S$.*

THEOREM 1. *(`First Principle of Mathematical Induction`) Let $P(n)$ be a statement about the positive integer $n$. Suppose that $P(1)$ is true. Whenever $k$ is a positive integer for which $P(k)$ is true, then $P(k+1)$ is true. Then $P(n)$ is true for every positive integer $n$.*

THEOREM 2. *The well-ordering principle implies the principle of mathematical induction.*

*Proof.*

REMARK 3. Note that the converse of the above result is also true: the well-ordering principle can be derived from the principle of mathematical induction. So, the two principles are logically equivalent.

### Some useful variations of PMI

THEOREM 4. *(`A Modified Principle of Mathematical Induction`) Let $P(n)$ be a statement about the positive integer $n$. Suppose that there is an integer $n_0$ such that $P(n_0)$ is true and whenever $k$ is a positive integer such that $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true. Then $P(n)$ is true for every positive integer $n \geq n_0$.*

THEOREM 5. *(`The Strong Principle of Mathematical Induction`) Let $P(n)$ be a statement about the positive integer $n$. Suppose that $P(1)$ is true. Whenever $k$ is a positive integer for which $P(i)$ is true for every positive integer $i$ such that $i \leq k$, then $P(k+1)$ is true. Then $P(n)$ is true for every positive integer $n$.*

THEOREM 6. `(Division Algorithm)` *Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$. Then there exist unique integers $q$ and $r$ such that*

$$a = bq + r, \quad \text{where} \quad 0 \leq r < b.$$

EXAMPLE 7. **(a)** *Rewrite the Division Algorithm using symbols.*

**(b)** *Let $a = 33, b = 7$. Determine $q$ and $r$.*

**(b)** *Let $a = -33, b = 7$. Determine $q$ and $r$.*

COROLLARY 8. *Let $b \in \mathbb{Z}^+$. Then for every integer $a$ there exists a unique integer $q$ such that exactly one of the following holds:*

$$a = bq, \quad a = bq + 1, \quad a = bq + 2, \ldots, a = bq + (b - 1).$$

COROLLARY 9. *Every integer is either even, or odd.*

EXAMPLE 10. *Prove that the square of any integer has one of the forms $4k$ or $4k + 1$, where $k \in \mathbb{Z}$.*

## 6.2 Greatest common divisors and the Euclidean Algorithm

DEFINITION 11. *Let $a$ and $b$ be integers, not both zero. The* **greatest common divisor** *of $a$ and $b$ (written $\gcd(a,b)$, or $(a,b)$) is the largest positive integer $d$ that divides both $a$ and $b$.*

EXAMPLE 12. *Find* $\gcd(18,24)$.

EXAMPLE 13. **(a)** *Compute*

$$\gcd(-18,24) = \qquad\qquad \gcd(-24,-18) =$$

*and make a conclusion.*

**(b)** *Compute*

$$\gcd(5,0) = \qquad\qquad \gcd(-5,0) =$$

*and make a conclusion.*

**(c)** *Complete the statement: If $a \neq 0$ and $b \neq 0$, then* $\gcd(a,b) \leq$ _____

**(d)** *Let $c \in \mathbb{Z}$. Then* $\gcd(a,ac) =$ _____

**Euclidean Algorithm** is based on the following

LEMMA 14. *Let $a$ and $b$ be integers, not both zero. Suppose we have integers $q$ and $r$ such that $a = bq+r$. Then* $\gcd(a,b) = \gcd(b,r)$.

**Procedure for finding** gcd **of two integers (the Euclidean Algorithm)**

1. Given $a, b \in \mathbb{Z}^+$ $(a > b)$.
2. If $b|a$, then $\gcd(a, b) = b$, and *STOP.*
3. *If* $b \not| a$, *then use the Division Algorithm to find* $q, r \in \mathbb{Z}$ *such that* $a = bq + r$, *where* $0 \leq r < b$. *Note that* $\gcd(a, b) = \gcd(b, r)$.
4. *Repeat from step 2, replacing* $a$ *by* $b$ *and* $b$ *by* $r$.

EXAMPLE 15. *Find* $\gcd(1176, 3087)$.

EXAMPLE 16. *Find integers* $x$ *and* $y$ *such that* $147 = 1176x + 3087y$.

DEFINITION 17. *Let* $a, b \in \mathbb{Z}$. *The integer* $n$ *is a* ***integral linear combination*** *of* $a$ *and* $b$ *if there exist integers* $x$ *and* $y$ *such that* $n = ax + by$.

The integer 147 is an integral linear combination of _____ and _____.
Also, the integer 147 is an integral linear combination of _____ and _____.

COROLLARY 18. *If* $d = \gcd(a, b)$ *then there exist integers* $x$ *and* $y$ *such that* $ax + by = d$*, i.e.* $d$ *is an integral linear combination of* $a$ *and* $b$*.*

### 6.3 Relatively prime (coprime) integers and the Fundamental Theorem of Arithmetic

DEFINITION 19. *Two integers* $a$ *and* $b$*, not both zero, are said to be* **relatively prime (or coprime)***, if* $\gcd(a, b) = 1$.

For example,

THEOREM 20. *The numbers* $a$ *and* $b$ *are relatively prime integers if and only if there exist integers* $x$ *and* $y$ *such that* $ax + by = 1$.

*Proof.*

THEOREM 21. *(Euclid's Lemma) Let* $a, b, c \in \mathbb{Z}$. *Suppose* $a|bc$ *and* $\gcd(a, b) = 1$. *Then* $a|c$.

EXAMPLE 22. *Suppose that* $\gcd(a, c) = \gcd(b, c) = 1$. *Prove that* $\gcd(ab, c) = 1$.

EXAMPLE 23. *Prove that for every integer* $n$, $\gcd(n, n + 1) = 1$.

DEFINITION 24. *An integer $p$ greater than 1 is called a* **prime** *number if the only divisors of $p$ are $\pm 1$ and $\pm p$. If an integer greater than 1 is not prime, it is called* **composite**.

| -7 | -4 | 0 | 1 | 2 | 4 | 7 | 10209 |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

Note that *if $p$ is prime, then for every $a \in \mathbb{Z}$, we have*

$$\gcd(p,a) = \begin{cases} p, & \text{if } \ p|a \\ 1, & \text{if } \ p \not| a \end{cases}$$

LEMMA 25. *Let $a$ and $b$ be integers. If $p$ is prime and divides $ab$, then $p$ divides either $a$, or $b$. (Note, $p$ also may divide both $a$ and $b$.)*

*Proof.*

COROLLARY 26. *Let $a_1, a_2, \ldots, a_n$ be integers.If $p$ is prime and divides $a_1 a_2 \cdot \ldots \cdot a_n$, then $p$ divides at least one integer from $a_1, a_2, \ldots, a_n$.(In other words, there exists $i \in \mathbb{Z}$, $1 \leq i \leq n$, such that $p|a_i$.)*

Note that Lemma 25 corresponds to $n = 2$. General proof of the above Corollary is by induction.

COROLLARY 27. *Let $a \in \mathbb{Z}$ and $p$ be a prime number. If $p|a^n$ for some $n \in \mathbb{Z}^+$, then $p|a$.*

COROLLARY 28. *Let $a \in \mathbb{Z}$. For every $n \in \mathbb{Z}^+$, $a^n \in \mathbb{E}$ if and only if $a \in \mathbb{E}$.*

COROLLARY 29. *Let $p, q_1, q_2, \ldots, q_m$ be prime with $p|q_1 q_2 \cdots q_m$. Then there exists $i \in \mathbb{Z}$, $1 \leq i \leq m$, such that $p = q_i$.*

EXAMPLE 30. *Prove that* $\sqrt[n]{5}$ *is irrational for every integer* $n \geq 2$.

**Prime Factorization** of a positive integer $n$ greater than 1 is a decomposition of $n$ into a product of primes.

**Standard Form** $n = p_1 p_2 \cdots p_k$, where primes $p_1, p_2, \ldots, p_k$ satisfy $p_1 \leq p_2 \leq \ldots \leq p_k$

**Compact Standard Form** $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, where primes $p_1, p_2, \ldots, p_m$ satisfy $p_1 < p_2 < \ldots < p_m$ and $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{Z}$.

EXAMPLE 31. *Write* 1224 *and* 225 *in a standard form (i.e. find prime factorization).*

**Strategy to use the Strong Principle of Mathematical Induction**

**Basic Step:** Verify that $P(1)$ is true.

**Induction hypothesis:** Assume that $k$ is a positive integer for which $P(1), P(2), \ldots, P(k)$ are true .

**Inductive Step:** With the assumption made, prove that $P(k+1)$ is true.

**Conclusion:** $P(n)$ is true for every positive integer $n$.

THEOREM 32. `Fundamental Theorem of Arithmetic`. *Let $n \in \mathbb{Z}$, $n > 1$. Then $n$ is a prime number or can be written as a product of prime numbers. Moreover, the product is unique, except for the order in which the factors appears.*

*Proof.*

**Existence:** Use the Strong Principle of Mathematical Induction.

$P(n)$ :

Basic step:

Induction hypothesis:

Inductive step:

**Uniqueness** Use the Strong Principle of Mathematical Induction.

$P(n)$ :

Basic step:

Induction hypothesis:

Inductive step:

COROLLARY 33. *There are infinitely many prime numbers.*

*Proof.*

EXAMPLE 34. *Prove that* 2 *is the only prime of the form* $n^3 + 1$.

EXAMPLE 35. *Prove that if* $a$ *is a positive integer of the form* $4n + 3$*, then at least one prime divisor of* $a$ *is of the form* $4n + 3$.