4&5 Binary Operations and Relations. The Integers.

4.1: Binary Operations

DEFINITION 1. *A* **binary operation** $*$ *on a nonempty set* A *is a function from* $A \times A$ *to* A.

Addition, subtraction, multiplication are binary operations on **Z**.

Addition is a binary operation on **Q** because

Division is NOT a binary operation on **Z** because

Division is a binary operation on

- To prove that $*$ is a binary operation on a set A

- To show that $*$ is <u>not</u> a binary operation on a set A

Classification of binary operations by their properties

Associative and Commutative Laws

DEFINITION 2. *A binary operation* $*$ *on* A *is* **associative** *if*

$$\forall a, b, c \in A, \quad (a * b) * c = a * (b * c).$$

A binary operation $*$ *on* A *is* **commutative** *if*

$$\forall a, b \in A, \quad a * b = b * a.$$

EXAMPLE 3. *Using symbols complete the following*

(a) *A binary operation* $*$ *on* A *is* <u>*not*</u> **associative** *if*

(b) *A binary operation* $*$ *on* A *is* <u>*not*</u> **commutative** *if*

Identities

DEFINITION 4. *If* $*$ *is a binary operation on* A*, an element* $e \in A$ *is an* **identity element** *of* A *w.r.t* $*$ *if*

$$\forall a \in A, \quad a * e = e * a = a.$$

EXAMPLE 5. **(a)** 1 *is an identity element for* **Z**, **Q** *and* **R** *w.r.t. multiplication.*

(b) 0 *is an identity element for* **Z**, **Q** *and* **R** *w.r.t. addition.*

Inverses

DEFINITION 6. *Let* $*$ *be a binary operation on* A *with identity* e*, and let* $a \in A$*. We say that* a *is* **invertible** *w.r.t.* $*$ *if there exists* $b \in A$ *such that*

$$a * b = b * a = e.$$

If b *exists, we say that* b *is an* **inverse** *of* a *w.r.t.* $*$ *and write* $b = a^{-1}$.

Note, inverses may or may not exist.

EXAMPLE 7. *Every $x \in \mathbf{Z}$ has inverse w.r.t. addition because*

$$\forall x \in \mathbf{Z}, \quad x + (-x) = (-x) + x = 0.$$

However, very few elements in $\mathbf{Z}$ have multiplicative inverses. Namely,

EXAMPLE 8. *Let $*$ be an operation on $\mathbf{Z}$ defined by*

$$\forall a, b \in \mathbf{Z}, \quad a * b = a + 3b - 1.$$

(a) *Prove that the operation is binary.*

(b) *Determine whether the operation is associative and/or commutative. Prove your answers.*

(c) *Determine whether the operation has identities.*

(d) *Discuss inverses.*

EXAMPLE 9. *Let $*$ be an operation on the power set $P(A)$ defined by*

$$\forall X, Y \in P(A), \quad X * Y = X \cap Y.$$

(a) *Prove that the operation is binary.*

(b) *Determine whether the operation is associative and/or commutative. Prove your answers.*

(c) *Determine whether the operation has identities.*

(d) *Discuss inverses.*

EXAMPLE 10. *Let $*$ be an operation on $F(A)$ defined by*

$$\forall f, g \in F(A), \quad f * g = f \circ g.$$

(a) *Prove that the operation is binary.*

(b) *Determine whether the operation is associative and/or commutative.*

(c) *Determine whether the operation has identities.*

(d) *Discuss inverses.*

PROPOSITION 11. *Let $*$ be a binary operation on a nonempty set A. If e is an identity element on A then e is unique.*

Proof.

PROPOSITION 12. *Let $*$ be an associative binary operation on a nonempty set A with the identity e, and if $a \in A$ has an inverse element w.r.t. $*$, then this inverse element is unique.*

Proof.

Closure

DEFINITION 13. *Let $*$ be a binary operation on a nonempty set A, and suppose that $S \subseteq A$. If $*$ is also a binary operation on S then we say that S is closed in A under $*$.*

EXAMPLE 14. *Let $*$ be a binary operation on A and let $S \subseteq A$. Using symbols complete the following*

(a) *S is closed in A under $*$ if and only if*

(a) *S is <u>not</u> closed in A under $*$ if*

EXAMPLE 15. *Determine whether the following subsets of $\mathbf{Z}$ are closed in $\mathbf{Z}$ under addition and multiplication.*

(a) $\mathbf{Z}^+$

(b) $\mathbf{E}$

(c) $\mathbf{O}$

5.1: The Integers: Axioms and Basic Properties

`Operations on the set of integers`, **Z**: *addition* and *multiplication* with the following properties:

A1. Addition is **associative**:

A2. Addition is **commutative**:

A3. **Z** has an **identity** element with respect to addition namely, the integer 0.

A4. Every integer x in **Z** has an **inverse** w.r.t. addition, namely, its negative $-x$:

A5. Multiplication is **associative**:

A6. Multiplication is **commutative**:

A7. **Z** has an **identity** element with respect to multiplication namely, the integer 1. (and $1 \neq 0$.)

A8. **Distributive Law:**

REMARK 16. We do not prove A1-A8. We take them as **axioms**: statements we *assume* to be true about the integers.

We use xy instead $x \cdot y$ and $x - y$ instead $x + (-y)$.

PROPOSITION 17. *Let* $a, b, c \in \mathbf{Z}$.

P1. *If* $a + b = a + c$ *then* $b = c$. *(cancellation law for addition)*

P2. $a \cdot 0 = 0 \cdot a = 0$.

P3. $(-a)b = a(-b) = -(ab)$

P4. $-(-a) = a$

P5. $(-a)(-b) = ab$

P6. $a(b - c) = ab - ac$

P7. $(-1)a = -a$

P8. $(-1)(-1) = 1$.

Proof

$\mathbf{Z}$ contains a subset $\mathbf{Z}^+$, called the **positive integers**, that has the following properties:

A9. Closure property: $\mathbf{Z}^+$ is closed in $\mathbf{Z}$ w.r.t. addition and multiplication:

A10. Trichotomy Law: for all $x \in \mathbf{Z}$ exactly one is true:

PROPOSITION 18. *If $x \in \mathbf{Z}$, $x \neq 0$, then $x^2 \in \mathbf{Z}^+$.*

Proof.

COROLLARY 19. $\mathbf{Z}^+ = \{1, 2, 3, \ldots, n, n+1, \ldots\}$

Proof.

Inequalities (the order relation less than)

DEFINITION 20. *For $x, y \in \mathbf{Z}$, $x < y$ if and only $y - x \in \mathbf{Z}^+$.*

REMARK 21. If $x < y$, we can also write $y > x$. We can also write $x \leq y$ if $x < y$ or $x = y$. Similarly, $y \geq x$ if $y > x$ or $y = x$.

Note that $\mathbf{Z}^+ = \{n \in \mathbf{Z} | n > 0\}$.

EXAMPLE 22. *Let $x, y \in \mathbf{Z}$. Using symbols complete the following*

- $x < y \quad \Leftrightarrow$
- $x > y \quad \Leftrightarrow$
- $x < 0 \quad \Leftrightarrow$
- $x > 0 \quad \Leftrightarrow$

PROPOSITION 23. *Let $a, b \in \mathbf{Z}$.*

Q1. *Exactly one of the following holds: $a < b$, $b < a$, or $a = b$.*

Q2. *If $a > 0$ then $-a < 0$; if $a < 0$ then $-a > 0$.*

Q3. *If $a > 0$ and $b > 0$ then $a + b > 0$ and $ab > 0$.*

Q4. *If $a > 0$ and $b < 0$ then $ab < 0$.*

Q5. *If $a < 0$ and $b < 0$ then $ab > 0$.*

Proof.

PROPOSITION 24. *Let $a, b, c \in \mathbf{Z}$.*

Q6. *If $a < b$ and $b < c$ then $a < c$.*

Q7. *If $a < b$ and $a + c < b + c$.*

Q8. *If $a < b$ and $c > 0$ then $ac < bc$.*

Q9. *If $a < b$ and $c < 0$ then $ac > bc$.*

A11. The Well Ordering Principle Every nonempty subset on $\mathbf{Z}^+$ 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 $x \in S$.

PROPOSITION 25. *There is no integer x such that $0 < x < 1$.*

Proof.

COROLLARY 26. 1 *is the smallest element of $\mathbf{Z}^+$.*

COROLLARY 27. *The only integers having multiplicative inverses in $\mathbf{Z}$ are ± 1.*

5.2: Induction[1]

THEOREM 28. *(*`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.*

Proof.

Paradox: All horses are of the same color.
Question: What's wrong in the following "proof" of G. Pólya?

$P(n)$: Let $n \in \mathbf{Z}^+$. Within any set of n horses, there is only one color.

Basic Step. If there is only one horse, there is only one color.

Induction Hypothesis. Assume that within any set of k horses, there is only one color.

Inductive step. Prove that within any set of $k+1$ horses, there is only one color.

Indeed, look at any set of $k+1$ horses. Number them: $1, 2, 3, ..., k, k+1$. Consider the subsets $\{1, 2, 3, ..., k\}$ and $\{2, 3, 4, ..., k+1\}$. Each is a set of only k horses, therefore within each there is only one color. But the two sets overlap, so there must be only one color among all $k+1$ horses.

[1]see also Chapter 1(Part III)

5.3: The Division Algorithm And Greatest Common Divisor

THEOREM 29. `(Division Algorithm)` *Let* $a \in \mathbf{Z}$, $b \in \mathbf{Z}^+$. *Then there exist* <u>*unique*</u> *integers* q *and* r *such that*

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

EXAMPLE 30. **(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 31. *Let* $b \in \mathbf{Z}^+$. *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 32. *Every integer is either even, or odd.*

Divisors (see Chapter 1, part II of notes)

Recall the following

DEFINITION 33. *Let* a *and* b *be integers. We say that* b **divides** a, *written* $b|a$, *if there is an integer* c *such that* $bc = a$. *We say that* b *and* c *are* **factors** *of* a, *or that* a *is* **divisible** *by* b *and* c.

Recall the following divisibility properties.

PROPOSITION 34. *Let* $a, b, c \in \mathbf{Z}$.

(a) *If* $a|1$, *then* $a = \pm 1$.

(b) *If* $a|b$ *and* $b|a$, *then* $a = \pm b$.

(c) *If* $a|b$ *and* $a|c$, *then* $a|(bx + cy)$ *for any* $x, y \in \mathbf{Z}$.

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

Greatest common divisor (gcd)

DEFINITION 35. *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 36. *Find* $\gcd(18,24)$.

EXAMPLE 37. **(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 $c \in \mathbf{Z}$. Then* $\gcd(a,ac) =$ _____

Euclidean Algorithm is based on the following two lemmas:

LEMMA 38. *Let a and b be two positive integers. If $a|b$ then* $\gcd(a,b) = |a|$.

LEMMA 39. *Let a and b be two positive integers such that $b \geq a$. Then* $\gcd(a,b) = \gcd(a,b-a)$.

Proof.

COROLLARY 40. *Let a and b be integers, not both zero. Suppose that there exist integers q_1 and r_1 such that $b = aq_1 + r_1$, $0 \leq r_1 < a$. Then* $\gcd(a, b) = \gcd(a, r_1)$.

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

EXAMPLE 41. *Find* $\gcd(1176, 3087)$.

EXAMPLE 42. *Find integers* x *and* y *such that* $147 = 1176x + 3087y$.

COROLLARY 43. *If* $d = \gcd(a, b)$ *then there exist integers* x *and* y *such that* $ax + by = d$. *Moreover,* d *is the minimal natural number with such property.*

Relatively prime (or coprime) integers

DEFINITION 44. *Two integers* a *and* b*, not both zero, are said to be* **relatively prime (or coprime)**, *if* $\gcd(a, b) = 1$.

For example,

Combining the above definition and the proof of Corollary 43, we obtain

THEOREM 45. a *and* b *are relatively prime integers if and only if there exist integers* x *and* y *such that* $ax + by = 1$.

THEOREM 46. *Let $a, b, c \in \mathbf{Z}$. Suppose $a|bc$ and $\gcd(a, b) = 1$. Then $a|c$.*

Proof.

5.4: Primes and Unique Factorization

DEFINITION 47. *An integer p greater than 1 is called a* **prime** *number if the only divisors of p are ± 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

Sieve of Eratosthenes.

The method to find all primes from 2 to n.

1. Write out all integers from 2 to n.
2. Select the smallest integer p that is not selected or crossed out.
3. Cross out all multiples of p (these will be $2p, 3p, 4p, \ldots$; the p itself should not be crossed out).
4. If not all numbers are selected or crossed out return to step 2. Otherwise, all selected numbers are prime.

EXAMPLE 48. *Find all two digit prime numbers.*

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	

REMARK 49. It is sufficient to cross out the numbers in step 3 starting from p^2, as all the smaller multiples of p will have already been crossed out at that point. This means that the algorithm is allowed to terminate in step 4 when p^2 is greater than n. In other words, *if the number p in step 2 is greater than $\sqrt{n}$ then all numbers that are already selected or not crossed out are prime.*

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 $p_1 \le p_2 \le \ldots \le p_k$

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 $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbf{Z}$.

EXAMPLE 50. *Write* 1224 *and* 225 *in a standard form (i.e. find prime factorization).*

LEMMA 51. *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 52. *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 $a_1, a_2, \ldots, a_n$.*

Note that Lemma 51 corresponds to $n = 2$. General proof of the above Corollary is by induction.

THEOREM 53. *(*`Second 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 $i \le k$, then $P(k+1)$ is true. Then $P(n)$ is true for every positive integer n.*

THEOREM 54. `Unique Prime Factorization Theorem`. *Let* $n \in \mathbf{Z}$, $n > 1$. *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 Second Principle of Mathematical Induction.

$P(n)$:

Basic step:

Induction hypothesis:

Inductive step:

Uniqueness Use the Second Principle of Mathematical Induction.

$P(n)$:

Basic step:

Induction hypothesis:

COROLLARY 55. *There are infinitely many prime numbers.*

Proof.

EXAMPLE 56. *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 $4n+3$.*

Proof