Chapter 5: The Integers

5.1: 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 1. 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 2. *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 w.r.t. addition and multiplication:

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

PROPOSITION 3. *If* $x \in \mathbf{Z}$, $x \neq 0$, *then* $x^2 \in \mathbf{Z}^+$.

Proof.

COROLLARY 4. $\mathbf{Z}^+ = \{1, 2, 3, \ldots, n, n+1, \ldots\}$

Proof.

Inequalities (the order relation less than)

DEFINITION 5. *For $x, y \in \mathbf{Z}$, $x < y$ if and only $y - x \in \mathbf{Z}^+$.*

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

PROPOSITION 6. *For all $a, b \in \mathbf{Z}$:*

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 $ab > 0$.*

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 $ac > bc$.*

Proof.

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

Proof.

COROLLARY 8. 1 *is the smallest element of* $\mathbf{Z}^+$.

COROLLARY 9. *The only integers having multiplicative inverses in* $\mathbf{Z}$ *are* ± 1.

5.2: Induction

"Domino Effect"

Step 1. The first domino falls.

Step 2. When any domino falls, the next domino falls.

Conclusion. All dominos will fall!

THEOREM 10. *(*`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.

Strategy

The proof by induction consists of the following steps:

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

Induction hypothesis: Assume that k is a positive interger for which $P(k)$ is true .

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

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

EXAMPLE 11. *Prove by induction the formula for the sum of the first n positive integers*

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}. \tag{1}$$

EXAMPLE 12. *Find the sum of all odd numbers from* 1 *to* $2n + 1$ *(*$n \in \mathbf{Z}^+$*).*

EXAMPLE 13. *Prove by induction the following formula*

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

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

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

Inductive step. Assume as induction hypothesis that within any set of k horses, there is only one color. Now look at any set of $k+1$ horses. Number them: $1, 2, 3, ..., k, k+1$. Consider the sets $\{1, 2, 3, ..., k\}$ 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.

5.3: The Division Algorithm And Greatest Common Divisor

THEOREM 14. (`Division Algorithm`) *Let $a \in \mathbf{Z}$, $b \in \mathbf{Z}^+$. Then there exist unique integers q and r such that*

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

Divisors

DEFINITION 15. *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.*

For example,

EXAMPLE 16. *Prove that $3|4^n - 1$, where $n \in \mathbf{Z}^+$.*

PROPOSITION 17. *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 18. *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 19. *Find* $\gcd(18,24)$.

Euclidean Algorithm

is based on the following two lemmas:

LEMMA 20. *Let a and b be two positive integers. If $a|b$ then* $\gcd(a,b) = |a|$.

LEMMA 21. *Let a and b be two positive integers such that $b \geq a$. Then* $\gcd(a,b) = \gcd(a, b-a)$.

Proof.

COROLLARY 22. *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 23. *Find* $\gcd(1176, 3087)$.

EXAMPLE 24. *Find integers* x *and* y *such that* $147 = 1176x + 3087y$.

COROLLARY 25. *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 26. *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 25, we obtain

THEOREM 27. a *and* b *are relatively prime integers if and only if there exist integers* x *and* y *such that* $ax + by = 1$.

THEOREM 28. *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 29. *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**.

For example,

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 30. *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 31. 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* <u>not</u> *crossed out are prime.*

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

EXAMPLE 32. *Write* 1224 *in standard form (i.e. find its prime factorization).*

LEMMA 33. *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 34. *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 33 corresponds to $n = 2$. General proof of the above Corollary is by induction.

THEOREM 35. *(*`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 $i \leq k$, then $P(k+1)$ is true. Then $P(n)$ is true for every positive integer n.*

THEOREM 36. `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 37. *There are infinitely many prime numbers.*

Proof.

EXAMPLE 38. *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.