4&5 Binary Operations and Relations. The Integers (part II)

5.3: The Division Algorithm And Greatest Common Divisor

THEOREM 1. (Division Algorithm) *Let $a \in \mathbf{Z}$, $b \in \mathbf{Z}^+$. Then there exist unique integers q and r such that*

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

EXAMPLE 2. **(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 3. *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 4. *Every integer is either even, or odd.*

Divisors (see Chapter 1, part II of notes)

Recall the following

DEFINITION 5. *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 6. *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 7. *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 8. *Find* $\gcd(18,24)$.

EXAMPLE 9. **(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 10. *Let a and b be two positive integers. If $a|b$ then* $\gcd(a,b) = |a|$.

LEMMA 11. *Let a and b be two positive integers such that $b \geq a$. Then* $\gcd(a,b) = \gcd(a,b-a)$.

Proof.

COROLLARY 12. *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 13. *Find* $\gcd(1176, 3087)$.

EXAMPLE 14. *Find integers* x *and* y *such that* $147 = 1176x + 3087y$.

COROLLARY 15. *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 16. *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 15, we obtain

THEOREM 17. a *and* b *are relatively prime integers if and only if there exist integers* x *and* y *such that* $ax + by = 1$.

THEOREM 18. *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 19. *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 20. *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 21. 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 22. *Write* 1224 *and* 225 *in a standard form (i.e. find prime factorization).*

LEMMA 23. *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 24. *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 23 corresponds to $n = 2$. General proof of the above Corollary is by induction.

THEOREM 25. *(*`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 26. `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 27. *There are infinitely many prime numbers.*

Proof.

EXAMPLE 28. *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.