MATH 3336 - Discrete Mathematics
Primes and Greatest Common Divisors (4.3)

Definition: A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

Note: An integer is a composite if and only if there exists an integer a such that $a|n$ and $1 < a < n$.

Example: The integer 11 is prime because its only positive factors are 1 and 11, but 12 is composite because it is divisible by 3, 4, and 6.

The Fundamental Theorem of Arithmetic: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Examples:

a. $50 = 2 \cdot 5^2$ b. $121 = 11^2$ c. $256 = 2^8$

Theorem: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof:

Example (trial division): Show that 97 is prime.

Because every integer has a prime factorization, it would be helpful to have a procedure for finding this prime factorization.

Example: Find the prime factorization of 143.

Theorem: There are infinitely many primes.

Proof:

The *Sieve of Eratosthenes* can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.

a. Delete all the integers, other than 2, divisible by 2.
b. Delete all the integers, other than 3, divisible by 3.
c. Next, delete all the integers, other than 5, divisible by 5.
d. Next, delete all the integers, other than 7, divisible by 7.
e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:
{2,3,5,7,11,15,1719,23,29,31,37,41,43,47,53, 59,61,67,71,73,79,83,89, 97}

TABLE 1 **The Sieve of Eratosthenes.**

Integers divisible by 2 other than 2 receive an underline.

1	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	100

Integers divisible by 3 other than 3 receive an underline.

1	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	100

Integers divisible by 5 other than 5 receive an underline.

1	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	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	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	100

Mersenne primes (French monk Marin Mersenne):$2^p - 1$

$2^2 - 1 = 3$

$2^3 - 1 = 7$

$2^5 - 1 = 31$ etc.

$2^{11} - 1 = 2047 = 23 \cdot 89$

$2^{77,232,917} - 1$

Conjectures and open problems about primes.

Example: $f(n) = n^2 - n + 41$

$$f(1) = 41, \qquad f(2) = 43, \qquad f(3) = 47, \qquad f(4) = 53$$

Is $f(n)$ prime for all positive integers n?

Fact: For every polynomial with integer coefficients, there is a positive integer y such that $f(y)$ is composite.

Goldbach's Conjecture: Every even integer $n, n > 2$, is the sum of two primes.

$4 =$

$6 =$

$8 =$

$10 =$

$12 =$

The conjecture has been checked for all positive even integers up to $4 \cdot 10^{18}$, BUT there is NO proof.

There are many conjectures asserting that there are infinitely many primes of certain special forms.

The Twin Prime Conjecture: There are infinitely many twin primes.

Twin primes are a pair of primes that differ by 2:

3 & 5,

5 & 7,

11 & 13,

17 & 19,

4967 & 4969

Greatest Common Divisors and Least Common Multiples

Definition: Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor* of a and b.

Notation: $gcd(a, b)$

One way to find the greatest common divisor is to find all positive common divisors of both integers and then take the largest divisor.

Example: What is the greatest common divisor of 12 and 24?

Divisors of 12: 1, 2, 3, 4, 6, 12

Divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24

Hence $\gcd(12, 24) =$

Definition: The integers a and b are *relatively prime* if their greatest common divisor is 1.

Example: 11 and 25 are relatively prime since $\gcd(11, 25) = 1$.

Definition: The integers $a_1, a_2, \dots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$, whenever $1 \leq i < j \leq n$.

Example: Determine whether the integers in each of these sets are pairwise relatively prime.

a. 21, 34, and 55

$\gcd(21, 34) =$

$\gcd(21, 55) =$

$\gcd(34, 55) =$

b. 14, 17, 85

$\gcd(14, 17) =$

$\gcd(14, 85) =$

$\gcd(17, 85) =$

Another way to find the greatest common divisor of two integers is to use their prime factorization.

Let $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_n^{b_n}$.

Then $\gcd(a, b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ldots \cdot p_n^{\min(a_n,b_n)}$

Example: Find the greatest common divisor of $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$.

Prime factorization can also be used to find the least common multiple of two numbers.

Definition: The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b.

Notation: $lcm(a, b)$

Let $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_n^{b_n}$.

Then $\mathrm{lcm}(a, b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ldots \cdot p_n^{\max(a_n,b_n)}$

Example: Find the least common multiple of $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$

Theorem: Let a and b be positive integers. Then $ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$

Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Euclidean Algorithm

The algorithm is based on the following lemma

Lemma: Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

The algorithm can be written as a sequence of equations. Let $r_0 = a$ and $r_1 = b$.

$r_0 = r_1 q_1 + r_2 \;\; 0 \le r_2 \le r_1$

$r_1 = r_2 q_2 + r_3 \; 0 \le r_3 \le r_2$

.

.

.

$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \le r_n \le r_{n-1}$

$r_{n-1} = r_n q_n$

- If a is smaller than b, the first step of the algorithm swaps the numbers.
- The remainders decrease with every step but can never be negative. A remainder r_n must eventually equal zero. Then the algorithm stops.

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0)$$

Example: Find the greatest common divisor of 91 and 287.

gcd as a Linear Combinations

Bezout's Theorem: If a and b are positive integers, then there exists integers s and t such that

$$\gcd(a, b) = sa + tb$$

Example: Express gcd(252, 198) =18 as a linear combination of 252 and 198.