Discrete Mathematics

Number Theory and Cryptography

Prof. Steven Evans

4.1: Divisibility and Modular Arithmetic

Divisibility

Definition

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$ (equivalently: if $\frac{b}{a}$ is an integer), and we write $a \mid b$. In this case, we say that a is a *factor* or *divisor* of b and that b is a *multiple* of a.

Divisibility

Theorem

Let a, b, and c be integers with $a \neq 0$.

1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
2. If $a \mid b$, then $a \mid bc$ for all integers c.
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Divisibility

Theorem

Let a, b, and c be integers with $a \neq 0$.

1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
2. If $a \mid b$, then $a \mid bc$ for all integers c.
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Corollary

If a, b, and c are integers with $a \neq 0$ such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ whenever m and n are integers.

The division algorithm

Theorem: The division algorithm

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

The division algorithm

Theorem: The division algorithm

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Notation

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

The division algorithm

Theorem: The division algorithm

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Notation

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

Sometimes $q = a \,\mathbf{div}\, d$ and $r = a \,\mathbf{mod}\, d$ are used to denote these relationships.

Modular arithmetic

Definition

If a and b are integers and m is a positive integer, then a is *congruent to* b *modulo* m if $m \mid a - b$. We denote this by

$$a \equiv b \pmod{m}.$$

This sentence is called a *congruence* and that m is its *modulus* (pl.: *moduli*).

Modular arithmetic

Definition

If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if $m \mid a - b$. We denote this by

$$a \equiv b \pmod{m}.$$

This sentence is called a *congruence* and that m is its *modulus* (pl.: *moduli*).

Theorem

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Modular arithmetic

Theorem

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof:

Modular arithmetic

Theorem

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b \pmod{m}$, by the definition of congruence we know that $m \mid (a - b)$. This means there's an integer k with $a - b = km$, or equivalently that $a = b + km$.

Modular arithmetic

Theorem

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b \pmod{m}$, by the definition of congruence we know that $m \mid (a - b)$. This means there's an integer k with $a - b = km$, or equivalently that $a = b + km$.

Conversely, if there is an integer k with $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b \pmod{m}$.

Modular arithmetic

Definition

The set of all integers congruent to an integer a modulo m is called the *congruence class* of a modulo m. There are m pairwise disjoint equivalence classes modulo m, and the union of these equivalence classes is the entire set of integers.

Modular arithmetic

Definition

The set of all integers congruent to an integer a modulo m is called the *congruence class* of a modulo m. There are m pairwise disjoint equivalence classes modulo m, and the union of these equivalence classes is the entire set of integers.

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

and

$$ac \equiv bd \pmod{m}.$$

Modular arithmetic

Corollary

Let m be a positive integer and let a and b be integers. Then:

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m,$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

Arithmetic modulo m

We can define *modular arithmetic operations* on $\mathbb{Z}_m$, the set of nonnegative integers less than m (i.e., the set $\{0, 1, \ldots, m-1\}$). The operation of *addition modulo m* is given by

$$a +_m b = (a + b) \bmod m,$$

where the addition on the right-hand side of this equation is the ordinary addition of integers. The operation of *multiplication modulo m* is given by

$$a \cdot_m b = (a \cdot b) \bmod m,$$

where again the multiplication on the right-hand side is ordinary multiplication of integers. The operations $+_m$ and $\cdot_m$ are called *addition and multiplication modulo m*, respectively.

Arithmetic modulo m

- Closure: Let $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ are also in $\mathbb{Z}_m$.

Arithmetic modulo m

- Closure: Let $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ are also in $\mathbb{Z}_m$.
- Associativity: If a, b, and c belong to $\mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$.

Arithmetic modulo m

- Closure: Let $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ are also in $\mathbb{Z}_m$.
- Associativity: If a, b, and c belong to $\mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$.
- Commutativity: If a and b belong to $\mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

Arithmetic modulo m

- Closure: Let $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ are also in $\mathbb{Z}_m$.
- Associativity: If a, b, and c belong to $\mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$.
- Commutativity: If a and b belong to $\mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- Identity elements: For $a \in \mathbb{Z}_m$, we have $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Arithmetic modulo m

- Closure: Let $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ are also in $\mathbb{Z}_m$.
- Associativity: If a, b, and c belong to $\mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$.
- Commutativity: If a and b belong to $\mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- Identity elements: For $a \in \mathbb{Z}_m$, we have $a +_m 0 = a$ and $a \cdot_m 1 = a$.
- Additive inverses: If $a \neq 0$ belongs to $\mathbb{Z}_m$, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is: $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

Arithmetic modulo m

- Closure: Let $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ are also in $\mathbb{Z}_m$.
- Associativity: If a, b, and c belong to $\mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$.
- Commutativity: If a and b belong to $\mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- Identity elements: For $a \in \mathbb{Z}_m$, we have $a +_m 0 = a$ and $a \cdot_m 1 = a$.
- Additive inverses: If $a \neq 0$ belongs to $\mathbb{Z}_m$, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is: $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.
- Distributivity: If a, b, and c belong to $\mathbb{Z}_m$, then

$$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c).$$

Arithmetic modulo m

Remark

Because $\mathbb{Z}_m$ with the operations of addition and multiplication modulo m satisfies the properties listed, $\mathbb{Z}_m$ with modular addition is said to be a *commutative group* and $\mathbb{Z}_m$ with both operations is said to be a *commutative ring*. Note that $\mathbb{Z}$ with the usual operations also forms a commutative ring. Groups and rings are studied in courses that cover "abstract algebra".

Arithmetic modulo m

Remark

Because $\mathbb{Z}_m$ with the operations of addition and multiplication modulo m satisfies the properties listed, $\mathbb{Z}_m$ with modular addition is said to be a *commutative group* and $\mathbb{Z}_m$ with both operations is said to be a *commutative ring*. Note that $\mathbb{Z}$ with the usual operations also forms a commutative ring. Groups and rings are studied in courses that cover "abstract algebra".

Remark

We will use the notations $+$ and $\cdot$ for $+_m$ and $\cdot_m$ whenever we work with $\mathbb{Z}_m$, leaving the subscript implicit.

4.2: Integer Representations and Algorithms

Integer representations

Theorem/Definition

Let b be an integer greater than 1. If n is a positive integer, then it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where k is a nonnegative integer, $a_0, \ldots, a_k$ are nonnegative integers less than b, then $a_k \neq 0$.

Integer representations

Theorem/Definition

Let b be an integer greater than 1. If n is a positive integer, then it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where k is a nonnegative integer, $a_0, \ldots, a_k$ are nonnegative integers less than b, then $a_k \neq 0$.

Bases 2, 8, 10, and 16 are called *binary*, *octal*, *decimal*, and *hexidecimal expansions* respectively.

Integer representations

Remark

Sixteen different digits are required for hexadecimal expansions. There are only 10 Arabic numerals, and so typically letters are used for digits 11-15:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.$$

Integer representations

Remark

Sixteen different digits are required for hexadecimal expansions. There are only 10 Arabic numerals, and so typically letters are used for digits 11-15:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.$$

Example

What is the decimal expansion of the integer that has $(1\ 0101\ 1111)_2$ as its binary expansion?

Integer representations

Example

Find the octal expansion of $(12345)_{10}$.

Integer representations

Example

Find the octal expansion of $(12345)_{10}$.

First, divide 12345 by 8 to obtain

$$12345 = 8 \cdot 1543 + 1.$$

Iterating division by 8 on the quotient gives

$$\begin{aligned} 1543 &= 8 \cdot 192 + 7, \\ 192 &= 8 \cdot 24 + 0, \\ 24 &= 8 \cdot 3 + 0, \\ 3 &= 8 \cdot 0 + 3. \end{aligned}$$

The remainders give the digits in octal: $(12345)_{10} = (30071)_8$.

4.3: Primes and Greatest Common Divisors

Primes

Definition

An integer p greater than 1 is called *prime* if its only positive factors are 1 and p. A positive integer that is greater than 1 and not prime is called *composite*.

Primes

Definition

An integer p greater than 1 is called *prime* if its only positive factors are 1 and p. A positive integer that is greater than 1 and not prime is called *composite*.

Remark

The integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$.

Primes

The Fundamental Theorem of Arithmetic

Every 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.

Trial division

Theorem

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

Trial division

Theorem

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

It follows that an integer is prime if it is not divisible by any prime less than or equal to its square root. This leads to the brute-force algorithm known as *trial division*. To use trial division we divide n by all primes not exceeding $\sqrt{n}$ and conclude that n is prime if it is not divisible by any of these primes.

The Sieve of Eratosthenes

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

The Sieve of Eratosthenes

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

The Sieve of Eratosthenes

1	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

The Sieve of Eratosthenes

1	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

The Sieve of Eratosthenes

1	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

The Sieve of Eratosthenes

1	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

The Sieve of Eratosthenes

1	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

The Sieve of Eratosthenes

1	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

The Sieve of Eratosthenes

1	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	

The primes up to 100.

Primes

Theorem

There are infinitely many primes.

Primes

Theorem

There are infinitely many primes.

The Prime Number Theorem

The ratio of the number of primes not exceeding x and $\frac{x}{\ln x}$ approaches 1 as x grows large.

Greatest common divisors and least common multiples

Definition

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. This number is denoted $\gcd(a, b)$.

Greatest common divisors and least common multiples

Definition

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. This number is denoted $\gcd(a, b)$.

Definition

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

Greatest common divisors and least common multiples

Definition

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. This number is denoted $\gcd(a, b)$.

Definition

The integers a and b are *relatively prime* if their greatest common divisor is 1. Integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ for each pair of distinct indices $i \neq j$.

Greatest common divisors and least common multiples

One way to find the greatest common divisor of two positive integers is to use their prime factorizations. Suppose that

$$a = p_1^{a_1} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} \cdots p_n^{b_n}.$$

Then $\gcd(a, b)$ is given by

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdots p_n^{\min(a_n, b_n)},$$

where $\min(x, y)$ is the smallest of the two integers x and y.

Greatest common divisors and least common multiples

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. This number is denoted $\text{lcm}(a, b)$.

Greatest common divisors and least common multiples

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. This number is denoted $\text{lcm}(a, b)$.

Remark

The least common multiple exists because the set of integers divisible by both a and b is nonempty, and every nonempty set of positive integers has a least element by the "well-ordering property".

Greatest common divisors and least common multiples

Remark

When a and b have prime factorizations as before, then

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdots p_n^{\max(a_n, b_n)}.$$

Greatest common divisors and least common multiples

Remark

When a and b have prime factorizations as before, then

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdots p_n^{\max(a_n,b_n)}.$$

Theorem

Let a and b be positive integers. Then

$$ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b).$$

The Euclidean algorithm

Lemma: Descent

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

Proof:

The Euclidean algorithm

Lemma: Descent

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

Proof: If d divides a and b, then d also divides $r = a - bq$. If d divides b and r, then d also divides $a = bq + r$. Since the common divisors of the pairs (a, b) and (b, r) are the same, they must have the same greatest common divisor.

The Euclidean algorithm

Algorithm

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. Successively applying the division algorithm, we obtain a sequence:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 && (0 \leq r_2 < r_1), \\ r_1 &= r_2 q_2 + r_3 && (0 \leq r_3 < r_2), \\ &\vdots = \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n (0 \leq r_n < r_{n-1}), \\ r_{n-1} &= r_n q_n. \end{aligned}$$

Applying the previous lemma, we have

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

The Euclidean algorithm

Example

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

The Euclidean algorithm

Example

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2 \qquad \text{(Here's the last nonzero remainder.)}$$
$$82 = 2 \cdot 41.$$

gcds as linear combinations

Theorem: Bézout's Theorem

If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$. This equation is called Bézout's identity, and the integers s and t are called *Bézout coefficients* of a and b.

gcds as linear combinations

Lemma

If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof:

gcds as linear combinations

Lemma

If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof: Apply Bézout's theorem to produce integers s and t with $sa + tb = 1$. Multiplying both sides by c, we have

$$sac + tbc = c.$$

Because a divides both summands (it appears in sac, and it is assumed to divide bc which appears in tbc), it also divides c.

gcds as linear combinations

Lemma

If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

gcds as linear combinations

Lemma

If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Proof of the uniqueness of prime factorizations

We proceed by contradiction. Suppose that a positive integer n can be written as the product of primes in two different ways:

$$n = p_1 p_2 \cdots p_s, \qquad \text{and} \qquad n = q_1 q_2 \cdots q_t,$$

where $p_1 \leq \cdots \leq p_s$ and $q_1 \leq \cdots \leq q_t$. Removing all the common divisors from the two factorizations, we're left with

$$p_{i_1} \cdots p_{i_u} = q_{j_1} \cdots q_{j_v} \qquad \text{(cont'd...)}$$

gcds as linear combinations

Lemma

If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Proof of the uniqueness of prime factorizations, cont'd

$$p_{i_1} \cdots p_{i_u} = q_{j_1} \cdots q_{j_v},$$

where no prime occurring on the left also occurs on the right. The lemma guarantees p_{i_1} divides q_{j_k} for some k — but no prime divides another prime, so this is impossible. Hence, it is not possible to have two distinct prime factorizations of n.

gcds as linear combinations

Theorem

Let m be a positive integers and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.