Slides of Discrete Mathematics based on Susanna Epp's Textbook

Moses A. Boudourides[1]

Visiting Associate Professor of Computer Science
Haverford College

[1] Moses.Boudourides@cs.haverford.edu

Chapter 8

Relations

November 8, 10, 12, 15 & 17, 2021

8.1 Relations on Sets

Definition

- If A and B are two sets, a **relation** R from A to B is defined as a subset of the Cartesian product $A \times B$. Moreover, given an ordered pair $(x, y) \in A \times B$, we say that x **is related to** y **by** R, written $x \, R \, y$, if and only if $(x, y) \in R$.
- Given a relation R from A to B, the **inverse relation** R^{-1} is defined as the following relation from B to A:

$$R^{-1} = \{(y, x) \in B \times A \,|\, (x, y) \in R\}.$$

- In other words,

$$x \, R^{-1} \, y \iff y \, R \, x.$$

8.1 Relations on Sets: Exercises

Exercise 8.1.11

Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ and let S be the "divides" relation. This is, for all $(x, y) \in A \times B, x\,S\,y \iff x \mid y$. Find explicitly which ordered pairs belong to S and S^{-1}.

Exercise 8.1.17

Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation T on A as: for all $x, y \in A, x\,T\,y \iff 3 \mid (x - y)$. Find the direct graph of T.

Exercise 8.1.20

Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S as: for all $(x, y) \in A \times B, x\,R\,y \iff |x| = |y|$ and $x\,S\,y \iff x - y$ is even. Find explicitly which ordered pairs belong to $A \times B, R, S, R \cup S$ and $R \cap S$.

Definition

Let R be a relation on a set A.

1. R is **reflexive** if and only if, for all $x \in A, x\,R\,x$.
2. R is **symmetric** if and only if, for all $x, y \in A,$ if $x\,R\,y,$ then $y\,R\,x$.
3. R is **transitive** if and only if, for all $x, y, z \in A,$ if $x\,R\,y$ and $y\,R\,z,$ then $x\,R\,z$.

8.2 Reflexivity, Symmetry and Transitivity: Exercises (a)

Exercise 8.2.17

A relation P is defined on $\mathbb{Z}$ as follows: For all $m, n \in \mathbb{Z}$, $m\,P\,n \iff \exists$ a prime number p such that $p \mid m$ and $p \mid n$. Is P reflexive, symmetric, transitive?

P is not reflexive: Otherwise, there would exist a prime divisor of any integer. Counterexample: there is no prime dividing 1.

P is symmetric: Trivial. **Why?**

P is not transitive: Counterexample: find three integers m, n, k such that both pairs m, n and n, k have a common prime divisor, but the pair m, k does not.

8.2 Reflexivity, Symmetry and Transitivity: Exercises (b)

Exercise 8.2.19

Define a relation I on $\mathbb{R}$ as follows: For all real numbers x and y, $x\,I,y \iff x - y$ is irrational. Is I reflexive, symmetric, transitive?

I is not reflexive: For all $x \in \mathbb{R}, x - x = 0$, which is not irrational.

I is symmetric: Trivial. **Why?**

I is not transitive: Counterexample: find three $x, y, z \in \mathbb{R}$ such that

$$x - y \notin \mathbb{Q}, y - z \notin \mathbb{Q}, \text{ but } x - z \in \mathbb{Q}.$$

8.2 Reflexivity, Symmetry and Transitivity: Exercises (c)

Exercise 8.2.22

Let $X = \{a, b, c\}$ and $\mathscr{P}(X)$ be the power set of X. A relation N is defined on $\mathscr{P}(X)$ as follows: For all $A, B \in \mathscr{P}(X)$, $A \, N \, B \iff$ the number of elements in A is not equal to the number of elements in B. Is N reflexive, symmetric, transitive?

N **is not reflexive**: Denoting by $|S|$ the number of elements of set S, for all $A \in \mathscr{P}(X)$, it is false to say that $|A| \neq |A|$.

N **is symmetric**: Trivial. **Why?**

N **is not transitive**: Counterexample: find three sets such that A, B, C such that $|A| \neq |B|, |B| \neq |C|$, but $|A| = |C|$.

8.3 Equivalence Relations I

Definition

- A **partition** of a set A is a collection of nonempty, mutually disjoint subsets of A, whose union is A.
- Given a partition of A, the **relation induced by the partition**, R, is defined on A as follows: For all $x, y \in A, x\, R\, y \iff$ there is a subset A_i of the partition suth that both x and y are in A_i.
- A relation on a set that satisfies the three properties of reflexivity, symmetry and transitivity is called an **equivalence relation**.

Theorem

Any relation on a set induced by a partition is an equivalence relation.

8.3 Equivalence Relations II

Definition

Let R be an equivalence relation on a set A. Then, for each $a \in A$, the **equivalence class of** a, denoted $[a]$ and called the **class of** a for short, is defined as the set of $x \in A$ such that $x \, R \, a$.

Theorem

Let R be an equivalence relation on a set A. Then the following are true:

- *For any $a, b \in A$, if $a \, R \, b$, then $[a] = [b]$.*
- *For any $a, b \in A$, either $[a] \cap [b] = \varnothing$ or $[a] = [b]$.*
- *The distinct equivalence classes of R form a partition of A.*
- *A* **representative** *of a class S of R is any $a \in A$ such that $[a] = S$.*

8.3 Equivalence Relations: Exercises (a)

Exercise 8.3.2 (b) and (c)

In $A = \{0, 1, 2, 3, 4\}$, find the relation R for the partitions (b) $\{0\}, \{1, 3, 4\}, \{2\}$ and (c) $\{0\}, \{1, 2, 3, 4\}$.

Exercise 8.3.4

Let $A = \{a, b, c, d\}$ be a set and $R = \{(a, a), (b, b), (b, d), (c, c), (d, b), (d, d)\}$ be an equivalence relation on A. Find the distinct equivalence classes of R.

Use the definition $[a] = \{x \in A \mid x\, R\, a\}$ for all $a \in A$.

Exercise 8.3.10

Let $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$ and the equivalence relation R is defined on A as follows: For all $m, n \in \mathbb{Z}$, $m\, R\, n \iff 3 \mid (m^2 - n^2)$. Find the distinct equivalence classes of R.

Use the definition $[a] = \{x \in A \mid x\, R\, a\}$ for all $a \in A$.

8.3 Equivalence Relations: Exercises (b)

Exercise 8.3.22

Let the relation D be defined on $\mathbb{Z}$ as follows: For all $m, n \in \mathbb{Z}$, $m\,D\,n \iff 3 \mid (m^2 - n^2)$. Prove that D is an equivalence relation and find its distinct equivalence classes.

Reflexivity: Trivial. **Why?**
Symmetry: Notice that $3 \mid (m^2 - n^2)$ means that $m^2 - n^2 = 3k$, for some integer k. Then, what about $n^2 - m^2$?
Transitivity: Let $m\,D\,n$ and $n\,D\,p$. Then use the definition of divisibility and some simple manipulation in order to find that $3 \mid (m^2 - p^2)$. **Fill in the details!**

To find the equivalence classes of D, first, notice that $m^2 - n^2 = (m - n)(m + n)$, which would imply that $m\,D\,n \iff$ which two divisibility conditions should occur? Subsequently, using the definition of divisibility, express m in terms of n in two ways, which are going to generate two equivalence classes. Which ones?

8.4 Congruence Modulo n I

In specifying time of day, we equate $10 + 4$ with 2 , we equate $3 - 7$ with 8 and we equate 1+28 with 5. These equivalences hold because the differences $(10 + 4) - 2, (3 - 7) - 8$ and $(1 + 28) - 5$, respectively, are divisible by 12. In the same way, two dates fall on the same day of the week if and only if the number of days by which they differ is divisible by 7. These types of calculations are sometimes called **modular arithmetic** and they are based on the definition of **congruence modulo** n: If $m, n, d \in \mathbb{Z}$ and $d > 0$, we say that m **is congruent to** n **modulo** d and write $m \equiv n \pmod{d}$ if and only if $d \mid (m - n)$.

Definition

Let m and n be integers and let d be a positive integer. We say that m **is congruent to** n **modulo** d and write $m \equiv n \pmod{d}$ if and only if $d \mid (m - n)$.

8.4 Congruence Modulo n II

Theorem (**Modular Equivalences**)

Let $a, b, n \in \mathbb{Z}$ and $n > 1$. The following statements are all equivalent:

1. $a \equiv b \pmod{n}$.
2. $n \mid (a - b)$.
3. $a = b + kn$, *for some* $k \in \mathbb{Z}$.
4. a *and* b *have the same (nonnegative) remainder when divided by* n.
5. $a \bmod n = b \bmod n$.

Theorem

Let $a, c, n, m \in \mathbb{Z}$ and $n > 1$. Then:

- $ma \equiv mc \pmod{n}$,
- $a^m \equiv c^m \pmod{n}$.

Exercise 8.4.5

Prove the transitivity of modular congruence, i.e., for all $a, b, c, n \in \mathbb{Z}$ with $n > 1$, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, by the definition of congruence modulo n, $n \mid (a-b)$ and $n \mid (b-b)$. Then, by definition of divisibility, $a - b = nk$, for some $k \in \mathbb{Z}$, and $b - c = nl$, for some $l \in \mathbb{Z}$. Therefore, as $a - c = (a-b) + (b-c)$, what do you get and then what does the difinition of divisibility imply?

Exercise 8.3.15 (b)

Prove that, for all integers m and n and any positive integer d, $m \equiv n \pmod{d}$ if and only if $m \bmod d = n \bmod d$.

First, suppose that $m \equiv n \pmod{d}$. By definition of congruence, $d \mid (m-n)$ and, thus, $m - n = dk$, for some integer k. Furthermore, assume that $m \bmod d = r$ or $m = dl + r$, for some integer l. Therefore, after a simple substitution $n = d(l-k) + r$ (**why exactly?**), i.e., $n \bmod d = r = m \bmod d$.

Next, suppose that $m \bmod d = n \bmod d$ and set $r = m \bmod d = n \bmod d$. Then, by definition of mod, $m = dp + r$ and $n = dq + r$, for some integers p and q. Then compute $m - n$ and why would this imply that $d \mid (m-n)$, which is the definition of congruence?

8.4 Congruence Modulo n: Exercises (c)

Exercise 8.4.11

If $a, b, c, n \in \mathbb{Z}$ with $n > 1$, $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then show that $a^m \equiv c^m \pmod{n}$, for all integers $m \geq 1$. (Use strong mathematical induction on m.)

Let property $P(m)$ be the congruence $a^m \equiv c^m \pmod{n}$. $P(1)$ holds by assumption (**why??**). Next, assume that $P(k)$ holds, for all integers $k \geq 1$. (The goal is to prove that $P(k+1)$ holds too). So, assume that, for some integer $k \geq 1$, $a^k \equiv c^k \pmod{n}$. However, the inductive hypothesis $a^k \equiv c^k \pmod{n}$ is translated by the previous Theorem as $a^k = c^k + rn$, for some $r \in \mathbb{Z}$, while, by the same Theorem, $a \equiv c \pmod{n}$ means that $a = c + sn$, for some $s \in \mathbb{Z}$. Therefore, compute $a^{k+1} = a \cdot a^k$ using the previous two equations in order to conclude that $a^{k+1} \equiv c^{k+1} \pmod{n}$. **Fill in all details**.

8.4 Congruence Modulo n: Exercises (d)

Exercise 8.4.12

(a) Prove that for all integers $n \geq 0$, $10^n \equiv (-1)^n \pmod{11}$. (b) Use part (a) to prove that a positive integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

(a) follows directly from the definition of congruence modulo n (**justify!**). For (b), let $a \in \mathbb{Z}, a > 0$. Then the decimal representation of a means that there exists an integer $n \geq 0$ and $n+1$ integers $d_0, d_1, \ldots, d_n$ with $0 \leq d_k < 10$, for $k = 0, 1, \ldots, n$ (the d_k's are the **digits** of a), such that

$$a = \sum_{k=0}^{n} d_k 10^k.$$

Therefore, applying (a) and the Theorem of the properties of modular equivalences,

$$a = \sum_{k=0}^{n} d_k 10^k = \left(\sum_{k=0}^{n} d_k \cdot (-1)^k \right) \pmod{11},$$

which implies that either a or the alternating sum of its digits is divisible by 11 (**because of which property of congruence modulo n??**).

8.4 Congruence Modulo n: Exercises (e)

When an integer is written in ordinary decimal notation, its **units digit** is the digit on its extreme right. For example, the units digit of 247 is 7. The reason 7 is called the "units digit" of 247 is that when 247 is written in expanded form, it becomes $247 = 2 \cdot 100 + 4 \cdot 10 + 7 \cdot 1$. In other words, clearly, the units digit of a number is the remainder of the division with 10.

Exercise 8.4.16

What is the units digit of 3^{1789}?

First, we compute the powers of 3 until the found units digits are repeated: $3^0 = 1$ (i.e., the units digit of 3^0 is 1), $3^1 = 3$ (i.e., the units digit of 3^1 is 3), $3^2 = 9$ (i.e., the units digit of 3^2 is 9), $3^3 = 27$ (i.e., the units digit of 3^3 is 7), $3^4 = 81$ (i.e., the units digit of 3^4 is 1), which terminates the process, because the first units digit is repeated. Hence, $3^4 = 1 (\text{mod } 10)$. Next, we observe that $1789 = 4 \cdot 447 + 1$. Therefore,

$$3^{1789} = 3^{4 \cdot 447 + 1} = (3^4)^{447} \cdot 3^1 \equiv 1^{447} \cdot 3 \equiv 3 \pmod{10}.$$

So, the units digit of 3^{1789} is 3 (**why??**).

Exercise 8.4.19

Reduce the following two equations by modulo 6 to show that they do not have a simultaneous integer solution:

$$43x + 24y = 39,$$
$$-11x + 48y = 53.$$

We have $43 \equiv 1 \pmod 6, 24 \equiv 0 \pmod 6, 39 \equiv 3 \pmod 6,$ $-11 \equiv 1 \pmod 6, 48 \equiv 0 \pmod 6, 53 \equiv 5 \pmod 6$. **Explain the derivation of these congruences**. Thus, what is the reduced system of equations and why do we get two contradictory congruences?

8.5 The Greatest Common Divisor of Two Integers

Definition

Given integers a and b not both zero, their **greatest common divisor**, denoted $\gcd a, b$, is the unique integer d such that:

1. $d > 0$,
2. $d \mid a$ and $d \mid b$,
3. for all positive integers c, if $c \mid a$ and $c \mid b$, then $c \leq d$.

Definition

Two integers a and b are called **realatively prime** if and only if $\gcd(a, b) = 1$.

Examples

- $\gcd(14, 35) = 7$.
- 21 and 8 are relative prime, since $\gcd(21, 8) = 1$.
- Any two successive integers are relatively prime!
- Given integer $k \neq 0, \gcd(k, 0) = |k|$.

8.5 Euclid's Algorithm

Theorem (GCD Reduction)

Let a and b two integers such that $a \geq b > 0$. Write $a = bq + r$, where $q, r \in \mathbb{Z}$ with $0 \leq q < b$. Then

$$\gcd(a, b) = \gcd(b, r).$$

Example

$$\begin{aligned} \gcd(48, 18) &= \gcd(18, 12) && \text{since } 48 = 18 \cdot 2 + 12 \\ &= \gcd(12, 6) && \text{since } 18 = 12 \cdot 1 + 6 \\ &= \gcd(6, 0) && \text{since } 12 = 6 \cdot 2 + 0 \\ &= 6 \end{aligned}$$

8.5 Euclid's Algorithm: Exercises

Exercise 8.5.7 and 8.5.8

$\gcd(832, 10, 933) = ?, \gcd(4, 131, 2, 431) = ?$.

Exercise 8.5.19

Find $\gcd(2583, 349)$ and express it as a linear combination of two numbers.

Start with $2583 = 349q + r$ and find q, r such that $r = 2583 - 349r$. Then do the same for 349 and r as many consecutive time it is needed to reach $r = 0$. Then substitute back the expressions for the remainder r until you reach the wanted linear combination.

8.5 Factoring

Theorem (Euclid's Lemma)

For all integers a, b and c, if a and c are relatively prime and $a \mid bc$, then $a \mid b$.

Corollary

Let a, b and p integers with p prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Example

Show that, when a, b, n are integers with $n > 0$, if a and b are relatively prime, then a and b^n are relatively prime too.

Let $d = \gcd(a, b^n)$. Suppose $d > 1$. Then, by the prime factorization Theorem, there is a prime p such that $p \mid d$. Hence $p \mid a$ and $p \mid b^n$. So $p \mid \gcd(a, b)$. However, a and b are relatively prime, i.e., $\gcd(a, b) = 1$, and it is impossible to have a prime $p \mid 1$. Therefore, $d = 1$.

8.5 GCD as a Linear Combination

Theorem

Given integers a and b not both 0, there exist integers x and y such that

$$gcd(a, b) = ax + by.$$

Corollary

Two integers a and b are relatively prime if and only if there exist integers x and y such that

$$ax + by = 1.$$

Example

$\gcd(18, 30) = 6$ and $6 = 18 \cdot (-3) + 30 \cdot 2$.

Exercise 8.5.7 and 8.5.23

Find one intger solution of the Diophantine equation $1456x + 693y = 4760$.