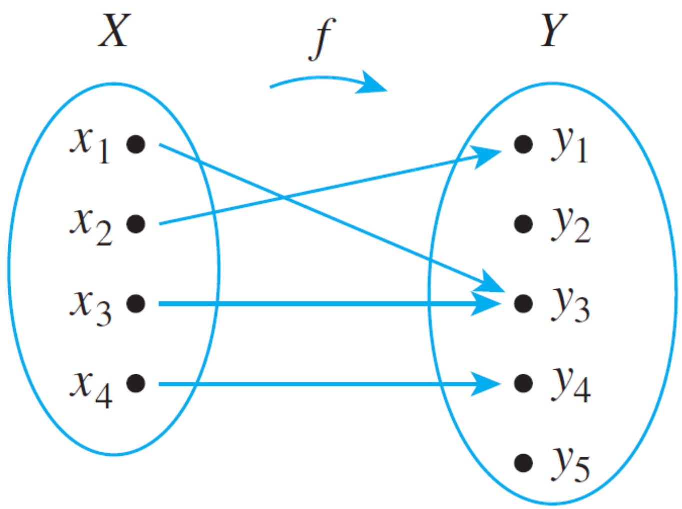
CHAPTER 8

RELATIONS

Recall the Definition of Functions

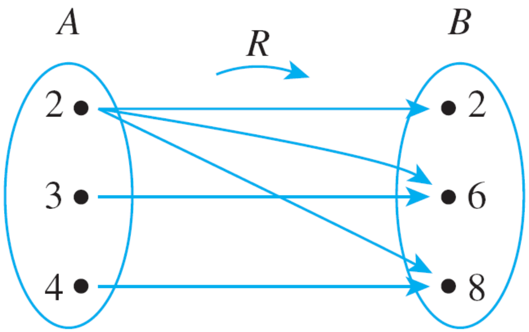
An arrow diagram defines a function if, and only if:

1. Every element of X has an arrow coming out of it.
2. No element of X has two arrows coming out of it that point to two different elements of Y.



Relations

Relations are more general than functions. The key difference is that the **same** element in the Domain **may be related to multiple elements** in the Co-domain; example:



Examples: A number x may be said to be related to a number y if

- $x < y$,
- or if x is a factor of y,
- or if $x^2 + y^2 = 1$.

Notation

- Let us use the notation $x\ R\ y$ as a shorthand for the sentence "*x* is related to *y*."
- Consider the relation x R y if x < y, then we write:

$$
\begin{array}{lll}
0\ R\ 1 & \text{since} & 0 < 1, \\
0\ R\ 2 & \text{since} & 0 < 2, \\
0\ R\ 3 & \text{since} & 0 < 3, \\
1\ R\ 2 & \text{since} & 1 < 2, \\
1\ R\ 3 & \text{since} & 1 < 3, \quad \text{and} \\
2\ R\ 3 & \text{since} & 2 < 3.
\end{array}
$$

- To say that x is not related to y, we use the notation $x \not{R}\ y$

$$
\begin{array}{lll}
1 \not{R}\ 1 & \text{since} & 1 \not< 1, \\
2 \not{R}\ 1 & \text{since} & 2 \not< 1, \quad \text{and} \\
2 \not{R}\ 2 & \text{since} & 2 \not< 2.
\end{array}
$$

Mathematical Definition of Relation

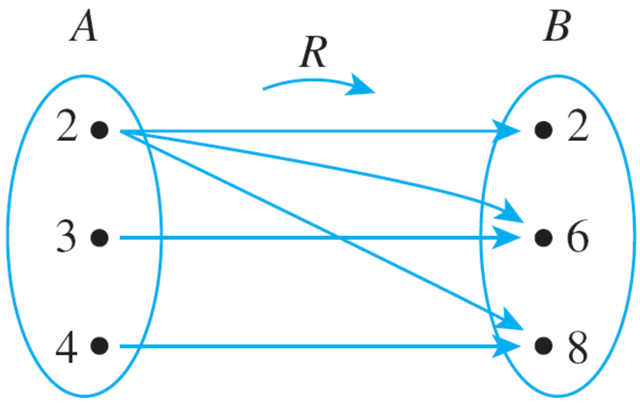
A **relation R from a set A** (domain) **to a set B** (co-domain) is defined as a subset of the Cartesian product A×B:

$$R = \{ (x,y) \in A \times B \mid x \, R \, y \}.$$

When $(x,y) \in R$, we say that x is **related** to y.

Example: the relation defined in this arrow diagram can also be defined as the set R of ordered pairs:

R = {(2,2),(2,6),(2,8),(3,6),(4,8)}



The Inverse of a Relation

The **inverse** of a relation $\mathbf{R^{-1}}$ **from B to A** is a subset of the Cartesian product B×A defined as follows:

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

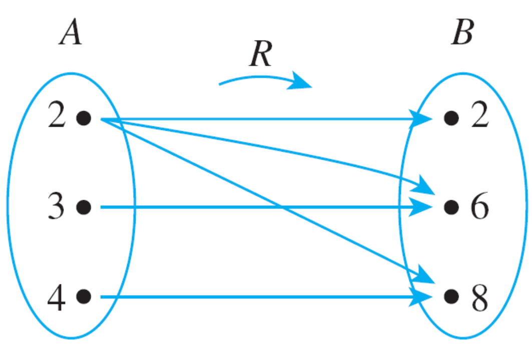
For all $x \in A$ and $y \in B$, $\quad (y, x) \in R^{-1} \quad \Leftrightarrow \quad (x, y) \in R.$

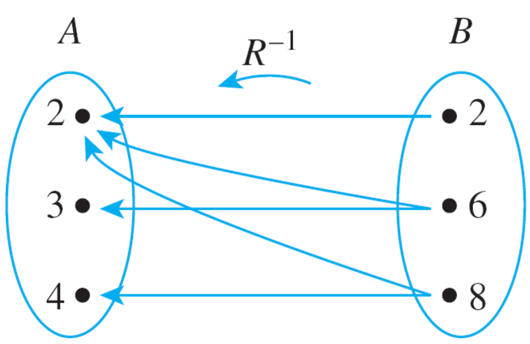
Example – *The Inverse of a Finite Relation*

Let $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$ and let R be the "divides" relation from A to B: For all $(x, y) \in A \times B$,

$$x \; R \; y \quad \Leftrightarrow \quad x \mid y$$

(it reads as "*x divides y*" or "*x is a factor of y*" or "y/x is an integer")





The inverse R^{-1} in this case is: *"y is a* ***multiple of*** *x"*.

Relations defined on the same set

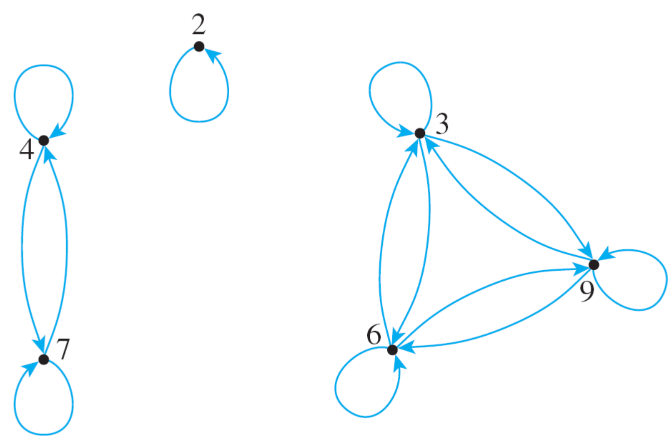
If the co-domain coincides with the domain A, then we call this a **“Relation on a set A”**, and is a subset of $A \times A$

Examples:

1. $R_1 = \{ (x,y) \in \mathbf{R}^2 \mid x^2 + y^2 = 1 \}$
2. $R_2 = \{ (x,y) \in \mathbf{R}^2 \mid x \leq y \}$

Relations on a Finite Set and Directed Graph

- We represent relations on a finite set via a **Directed Graph**: instead of representing *A* as two separate sets of points, we represent *A* only once, and draw an arrow from each point of *A* to each related point (potentially also to itself).
- Example:



Exercise – *Directed Graph of a Relation*

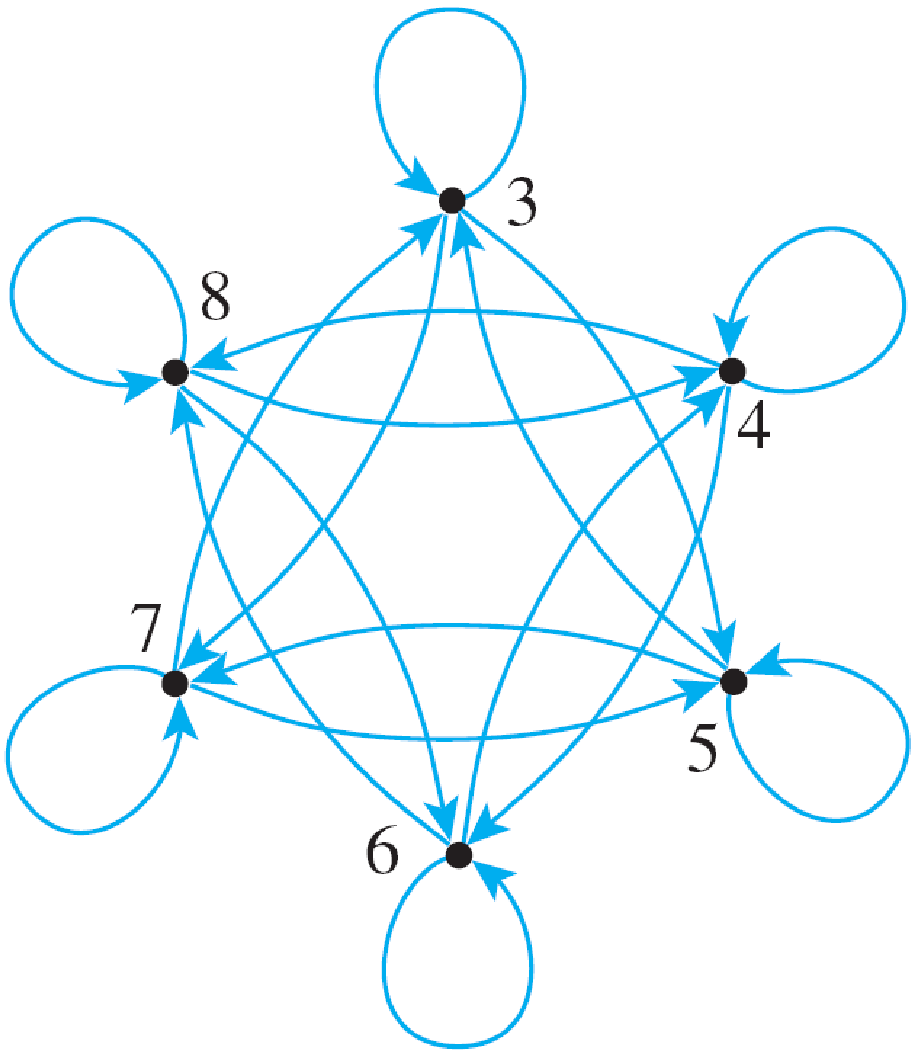
Let $A = \{3, 4, 5, 6, 7, 8\}$ and define a relation R on A as follows: For all $x, y \in A$,

$$x \, R \, y \Leftrightarrow 2 \mid (x - y).$$

$$(x, y) \in R \quad \text{means that} \quad \frac{x - y}{2} \text{ is an integer.}$$

Draw the directed graph of R!

Solution – *Directed Graph of a Relation*



SECTION 8.2

Reflexivity, Symmetry, and Transitivity

Reflexivity, Symmetry, and Transitivity

• 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 $x \; R \; z$.

A relation that satisfies all these three properties is called an **Equivalence Relation**.

Reflexivity, Symmetry, and Transitivity

To prove that a relation does **not** have one the properties, find a counterexample or **negate the general statement**:

1. R is **not reflexive** $\Leftrightarrow$ there is a least an element x in A such that $x \not R x$.

2. R is **not symmetric** $\Leftrightarrow$ there are elements x and y in A such that $x \, R \, y$ but $y \not R x$.

3. R is **not transitive** $\Leftrightarrow$ there are elements x, y and z in A such that $x \, R \, y$ and $y \, R \, z$ but $x \not R z$.

Exercise 1

Let $A = \{2, 3, 4, 6, 7, 9\}$ and define a relation R on A as follows: For all $x, y \in A$,

$$x \ R \ y \quad \Leftrightarrow \quad 3 \mid (x - y).$$

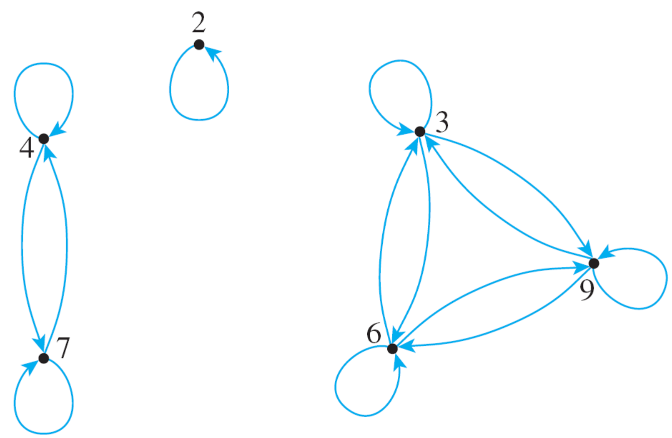
- Is R **reflexive**?
  Yes, because $2\ R\ 2$, $3\ R\ 3$, $4\ R\ 4$, $6\ R\ 6$, $7\ R\ 7$, $9\ R\ 9$.

- Is R **symmetric**?
  Yes, indeed $6\ R\ 3$ and $3\ R\ 6$ (because 3 – 6 = –3, and 3 | –3). We can verify that this applies to any other x, y $\in$ A

- Is R **transitive**?
  Yes, you can verify this.

Exercise 1

Directed graph for *R:*



We observe that:

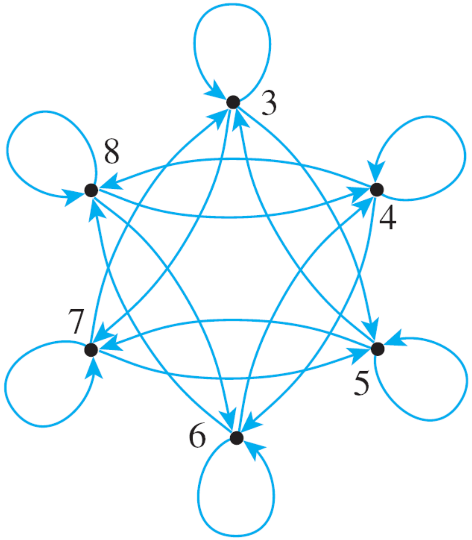
1. Each point has an arrow looping around back to itself, which means that R is **reflexive**.
2. If there is an arrow from A to B, there is an arrow from B to A. This means that R is **symmetric.**
3. If there is an arrow from A to B and from B to C, then there is an arrow from A to C. This means R is **transitive**.

Exercise 2

Let $A = \{3, 4, 5, 6, 7, 8\}$ and define a relation R on A as follows: For all $x, y \in A$,

$$x \, R \, y \Leftrightarrow 2 \mid (x - y).$$

- Is R an Equivalence Relation?
- Yes, we can inspect directed graph of R and verify the properties.

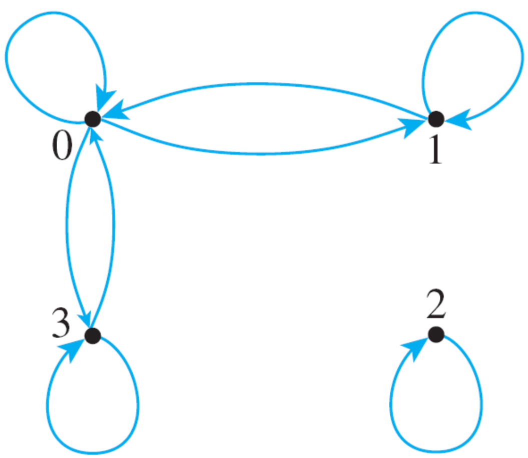


Exercise 3

Let $A = \{0, 1, 2, 3\}$ and define a relation R on A as follows:

$$R = \{(0, 0), (0, 1), (0, 3), (1, 0), (1, 1), (2, 2), (3, 0), (3, 3)\},$$

Is R reflexive? symmetric? transitive?

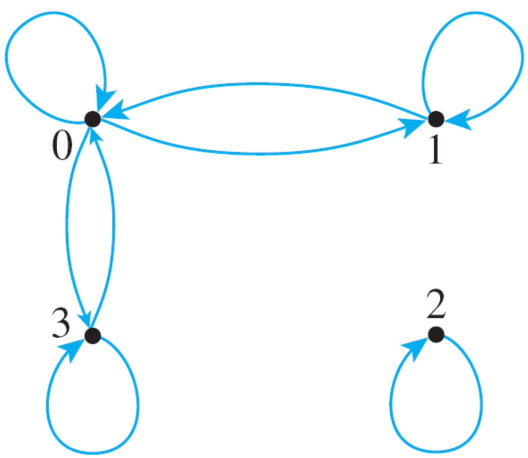


Exercise 3

***R* is reflexive:** There is a loop at each point of the directed graph.

***R* is symmetric:** For each arrow there is an arrow back.

***R* is not transitive:** There is an arrow going from 1 to 0 and an arrow going from 0 to 3, but there is no arrow going from 1 to 3.



More exercises

Prove or disprove that the following relations are **reflexive**, **symmetric**, or **transitive**:

1. For every $x, y \in \boldsymbol{R}$, $\quad x \text{ R } y \quad \Leftrightarrow \quad x < y$

2. For every $m, n \in \boldsymbol{Z}$, $\quad m \text{ R } n \quad \Leftrightarrow \quad 3 \mid (m - n)$

The Transitive Closure of a Relation

A relation R may fail to be transitive if it does not contain certain ordered pairs.

To make it transitive, we need to add ordered pairs.

The relation R^t obtained by adding the least number of ordered pairs to ensure transitivity is called the *transitive closure* of the relation.

Exercise – *Transitive Closure of a Relation*

Let A = {0, 1, 2, 3} and consider the relation R defined on A as follows:

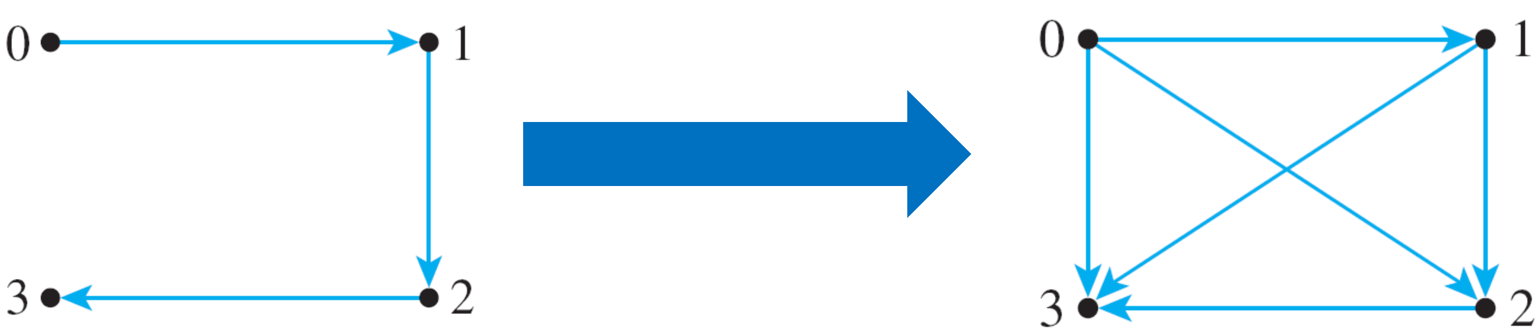
$$R = \{(0, 1), (1, 2), (2, 3)\}.$$

Find the transitive closure of R.

Solution:

R^t contains (at least) the ordered pairs:

{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)}.



SECTION 8.3

Equivalence Relations

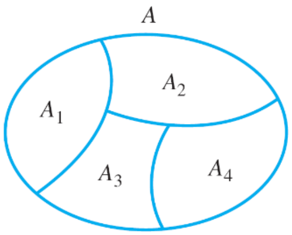
Equivalence Relation

- **Definition**

Let A be a set and R a relation on A. R is an **equivalence relation** if, and only if, R is reflexive, symmetric, and transitive.

The Relation Induced by a Partition

Recall: A partition of a set A is a collection of mutually disjoint subsets A_i whose union is A.



Given a partition, the **relation induced by the partition** of A is a relation where all the element within each subset A_i of the partition are related to one another. Formally:

• Definition

Given a partition of a set A, the **relation induced by the partition,** R, is defined on A as follows: For all $x, y \in A$,

$$x \; R \; y \quad \Leftrightarrow \quad \text{there is a subset } A_i \text{ of the partition such that both } x \text{ and } y \text{ are in } A_i.$$

Exercise – *Relation Induced by a Partition*

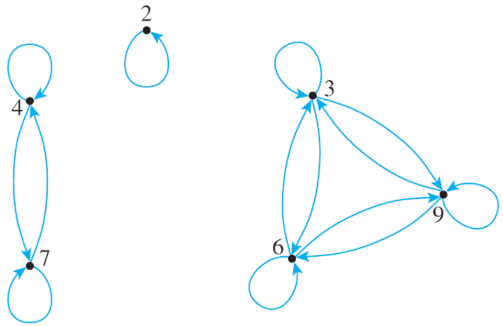
Let A = {2, 3, 4, 6, 7, 9} and consider the following partition of A:

{4, 7}, {2}, {3, 6, 9}.

Find the relation R induced by this partition!

Solution:

All the element within each subset of the partition are related to one another, thus: R = {(4, 4), (4, 7), (7, 4), (7, 7), (2, 2), (3, 3), (3, 6), (3, 9), (6, 6), (6, 3), (6, 9), (9, 9), (9, 6), (9, 3)}.



The Relation Induced by a Partition is an Equivalence Relation

We can observe that **a relation induced by a partition** is **always reflexive**, **symmetric**, and **transitive**. Thus, a relation induced by a partition is always an equivalence relation!

Equivalence Classes of an Equivalence Relation

Given an equivalence relation on a certain set A and any particular element a in A, the subset [a] of all elements related to a under R is called the *equivalence class* of *a*:

$$[a] = \{ x \in A \mid x \, R \, a \} .$$

Distinct equivalence classes of an Equivalence Relation form a partition A.

Suppose that a, b ∈ A, if a R b, then [a] = [b]. This is trivial since, all the elements in [a] are also in [b] and vice versa.

Any element of an equivalent class is called “Class Representative”.

Exercise – *Equivalence Classes*

Consider the relation R induced by the following partition of A = {0, 1, 2, 3, 4}:

{0, 3, 4}, {1}, {2}.

Find the distinct equivalence classes of R.

Solution:

- [0], [1], [2] (or alternatively, [3], [1], [2] or [4], [1], [2]).
- Observe that they are all distinct, mutually disjoint, and their union is the whole set A.
- [0] = [3] = [4] because they represent the same eq. class.

Exercise – *Equivalence Classes of Congruence Modulo 3*

Let *R* be the relation of congruence modulo 3 on the set **Z** of all integers:

$$\boxed{m\ R\ n \quad \Leftrightarrow \quad 3 \mid (m - n) \quad \Leftrightarrow \quad m \equiv n \pmod 3.}$$

Find the distinct equivalence classes of *R*!

(Recall: we showed (slide 20) that the congruence modulo 3 is an equivalence relation)

Solution – *Equivalence Classes of Congruence Modulo* 3

$$[0] = \{x \in \mathbf{Z} \mid x = 3k + 0, \text{ for some integer } k\}$$
$$= \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\},$$
$$[1] = \{x \in \mathbf{Z} \mid x = 3k + 1, \text{ for some integer } k\}$$
$$= \{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\},$$

$$[2] = \{x \in \mathbf{Z} \mid x = 3k + 2, \text{ for some integer } k\}$$
$$= \{\ldots -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

Every integer is in class [0], [1], or [2]. Hence, they are the distinct equivalence classes.

Congruence Modulo *n*

• Definition

Let m and n be integers and let d be a positive integer. We say that $\boldsymbol{m}$ **is congruent to** $\boldsymbol{n}$ **modulo** $\boldsymbol{d}$ and write

$$\boldsymbol{m \equiv n \pmod{d}}$$

if, and only if, $d \mid (m - n)$.

Symbolically: $m \equiv n \pmod{d} \quad \Leftrightarrow \quad d \mid (m - n)$

The "congruence modulo d" is an equivalence relation (the proof is similar to the one we gave to solve the exercise on slide 20 for the "congruence modulo 3").

Exercise – *Evaluating Congruences*

Determine which of the following congruences are true and which are false.

$$12 \equiv 7 \pmod 5 \qquad 6 \equiv -8 \pmod 4 \qquad 3 \equiv 3 \pmod 7$$

Solution:

a. True. $12 - 7 = 5 = 5 \cdot 1$. Hence $5 \mid (12 - 7)$, and so $12 \equiv 7 \pmod 5$.

b. False. $6 - (-8) = 14$, $4 \nmid 14$ because $14 \neq 4 \cdot k$ for any integer k. Consequen $6 \not\equiv -8 \pmod 4$.

c. True. $3 - 3 = 0 = 7 \cdot 0$. Hence $7 \mid (3 - 3)$, and so $3 \equiv 3 \pmod 7$.

Example – *Rational Numbers Are Equivalence Classes*

Let *A* be defined as

$$A = \mathbf{Z} \times (\mathbf{Z} - \{0\}).$$

Define a relation *R* on *A* as follows: For all (*a*, *b*), (*c*, *d*) $\in$ *A*,

$$\boxed{(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad ad = bc.}$$

R is an equivalence relation.

Each equivalence class consists of all ordered pairs (*a*, *b*) where a/b equals a certain value.
Example:

$$[(1, 2)] = \{(1, 2), (-1, -2), (2, 4), (-2, -4), (3, 6), (-3, -6), \ldots\}$$

SECTION 8.4

Modular Arithmetic with Applications to Cryptography

Modular Arithmetic with Applications to Cryptography

Cryptography is the study of methods for sending secret messages.

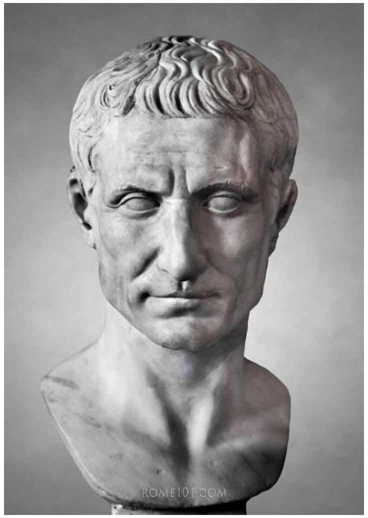
It involves encryption, in which a message, called plaintext, is converted into a form, called ciphertext, that may be sent over channels possibly open to view by outside parties. The receiver of the ciphertext uses decryption to convert the ciphertext back into plaintext.

In the past, the primary use of cryptography was for government and military intelligence, and this use continues to be important.

Modular Arithmetic with Applications to Cryptography

An encryption system once used by Julius Caesar, and now called the Caesar cipher, encrypts messages by changing each letter of the alphabet to the one three places farther along, with X, Y, Z wrapping around to A, B, and C.

Each letter of the alphabet is coded by its position, i.e., A = 1, B = 2, . . . , Z = 26.
If the numerical version of the plaintext for a letter is denoted *M* and the numeric version of the ciphertext is denoted *C*, then



$$\boxed{C = (M + 3)\ mod\ 26.}$$

Modular Arithmetic with Applications to Cryptography

The receiver of such a message can easily decrypt it by using the formula

$$\boxed{M = (C - 3)\ mod\ 26.}$$

Table:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Properties of Congruence Modulo *n*

Theorem 8.4.1 Modular Equivalences

Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent:

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

Modular Arithmetic

The fundamental fact about “Congruence Module n” is that if you first perform an addiction, subtraction, multiplication, of integers and then reduce the result modulo n, you obtain the same result as when the operation is performed on the reduced version of the integers:

1. (a + b) mod n = [(a mod n) + (b mod n)] mod n
2. (a - b) mod n = [(a mod n) - (b mod n)] mod n
3. (a * b) mod n = [(a mod n) * (b mod n)] mod n
4. a^m mod n = (a mod n)^m mod n

Modular Arithmetic

Example:

$$\begin{aligned}(55 \cdot 26)\ mod\ 4 &= \{(55\ mod\ 4)(26\ mod\ 4)\}\ mod\ 4 \\ &\equiv (3 \cdot 2)\ mod\ 4 \\ &\equiv 6\ mod\ 4 \equiv 2\end{aligned}$$

Modular Arithmetic

Cryptography uses large numbers (hundreds/thousands of bits).
When modular arithmetic is performed with large numbers, computations are facilitated by using two properties of exponents:

$$x^{2a} = (x^a)^2 \quad \text{for all real numbers } x \text{ and } a \text{ with } x \geq 0.$$

$$x^{a+b} = x^a x^b \quad \text{for all real numbers } x,\ a, \text{ and } b \text{ with } x \geq 0.$$

Example:

$$x^4 \; mod\; n \;=\; (x^2)^2 \; mod\; n \;=\; (x^2 \; mod\; n)^2 \; mod\; n$$

Example – *Computing a^k mod n When k Is a Power of 2*

Find 144^4 *mod* 713.

Solution:

$$\begin{aligned}
144^4 \textit{ mod } 713 &= (144^2)^2 \textit{ mod } 713 \\
&= (144^2 \textit{ mod } 713)^2 \textit{ mod } 713 \\
&= (20736 \textit{ mod } 713)^2 \textit{ mod } 713 && \text{because } 144^2 = 20736 \\
&= 59^2 \textit{ mod } 713 && \text{because } 20736 \textit{ mod } 713 = 59 \\
&= 3481 \textit{ mod } 713 && \text{because } 59^2 = 3481 \\
&= 629 && \text{because } 3481 \textit{ mod } 713 = 629.
\end{aligned}$$

Finding an Inverse Modulo n

Suppose you want to solve the following congruence:

$$2x \equiv 3 \pmod 5$$

Since $3 \cdot 2 = 6 \equiv 1 \pmod 5$, you can think of 3 as an inverse for 2 modulo 5, multiply both sides by 3:

$$6x = 3 \cdot 2x \equiv 3 \cdot 3 \pmod 5 \equiv 9 \pmod 5 \equiv 4 \pmod 5.$$

Since $6 \equiv 1 \pmod 5$, we get that

$$x \equiv 4 \pmod 5.$$

Finding an Inverse Modulo *n*

It is not always possible to find an inverse:

$$2 \cdot 1 \equiv 2 \pmod{4}$$
$$2 \cdot 2 \equiv 0 \pmod{4}$$
$$2 \cdot 3 \equiv 2 \pmod{4}.$$

The number 2 does not have an inverse modulo 4!

When do inverses exist?
→ We need to understand the concept of relative primeness to answer this question.

Finding an Inverse Modulo *n*

• Definition

Integers a and b are **relatively prime** if, and only if, $\gcd(a, b) = 1$. Integers $a_1, a_2, a_3, \ldots, a_n$ are **pairwise relatively prime** if, and only if, $\gcd(a_i, a_j) = 1$ for all integers i and j with $1 \leq i, j \leq n$, and $i \neq j$.

Corollary 8.4.7 Existence of Inverses Modulo *n*

For all integers a and n, if $\gcd(a, n) = 1$, then there exists an integer s such that $as \equiv 1 \pmod{n}$. The integer s is called the **inverse of *a* modulo *n*.**

Finding an Inverse Modulo *n*

The extended Euclidean algorithm can be used to find the inverse of number a modulo m efficiently:

Given a and b the algorithm finds x and y such that
$ax + by = \gcd(a,b)$

If a and m are relatively prime, $\gcd(a, m) = 1$ by definition.

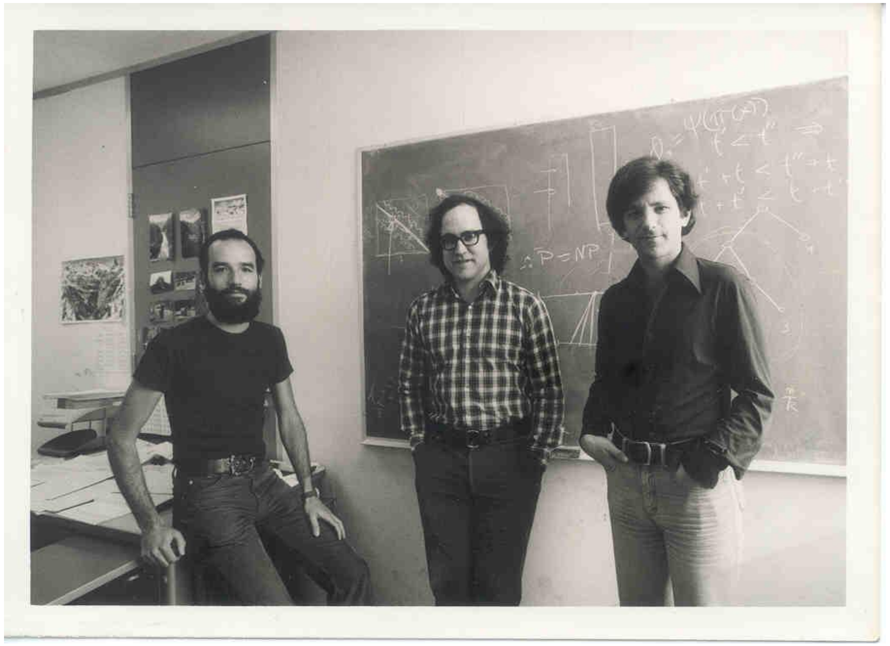
Given a and m, the algorithm returns
$ax + my = \gcd(a,m) = 1$

Since $my \equiv 0 \pmod{m}$, x is the inverse of $a \pmod{m}$!

RSA Cryptography

We now understand enough number theory to explain the RSA (Rivest, Shamir, Adleman) cipher.

The security of RSA is based on the hardness of factoring: It is easy to generate large prime numbers but it is hard to factor their product!



RSA Cryptography

Suppose Alice decides to set up an RSA cipher. She chooses two random prime numbers, say $p = 5$ and $q = 11$, and computes $pq = 55$.

She then chooses a positive integer e that is relatively prime to $(p - 1)(q - 1)$. In this case, $(p - 1)(q - 1) = 4 \cdot 10 = 40$, so she may take $e = 3$.

The numbers $pq = 55$ and $e = 3$ are the public key (everybody can know these numbers).

She then computes d, such that $ed \equiv 1 \pmod{(p-1)(q-1)}$. The numbers pq and d are the private key.

RSA Cryptography

The plaintext M is converted into ciphertext C according to the following formula:

$$\boxed{C = M^e \; mod \; pq.}$$

Since pq and e are public, anyone can encrypt messages!

RSA Cryptography

The plaintext M for a ciphertext C is recovered as follows:

$$M = C^d \; mod \; pq.$$

Note that because $M + kpq \equiv M \pmod{pq}$, M must be less than pq.

Because p and q are large in practice, this is not a severe limitation. Long messages are broken into blocks of symbols to meet this restriction.

Example – *Encrypting a Message Using RSA Cryptography*

Given the public key (pq=55,e=3), what is the ciphertext corresponding to the plaintext 8?

$C = 8^3 \bmod 55$

$= 64 \cdot 8 \bmod 55$

$= (64 \bmod 55) \cdot 8 \bmod 55$

$= 9 \cdot 8 \bmod 55$

$= 72 \bmod 55$

$= 17$

Example – *Decrypting a Message Using RSA Cryptography*

Note that $d = 27$, since $ed = 27 \cdot 3 \equiv 1 \pmod{40}$.

Decrypting the ciphertext 17:

$$
\begin{aligned}
M &= 17^{27} \bmod 55 \\
&= 17^{16} \cdot 17^{8} \cdot 17^{2} \cdot 17 \bmod 55 \\
&= 16 \cdot 26 \cdot 14 \cdot 17 \bmod 55 \\
&= 31 \cdot 14 \cdot 17 \bmod 55 \\
&= 49 \cdot 17 \bmod 55 \\
&= 8
\end{aligned}
$$

$17^2 \bmod 55 = 289 \bmod 55 = 14$

$17^4 \bmod 55 = 14 \cdot 14 \bmod 55 = 31$

$17^8 \bmod 55 = 31 \cdot 31 \bmod 55 = 26$

$17^{16} \bmod 55 = 26 \cdot 26 \bmod 55 = 16$

Why Does the RSA Cipher Work?

Fermat's Little Theorem provides the theoretical underpinning for RSA cryptography:

Theorem 8.4.10 Fermat's Little Theorem

If p is any prime number and a is any integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

We must verify that:

$$M = C^d \; mod \; pq$$

Why Does the RSA Cipher Work?

By substitution

$$M = C^d \; mod \; pq$$

$$C^d \; mod \; pq = (M^e \; mod \; pq)^d \; mod \; pq.$$

$$(M^e \; mod \; pq)^d \equiv M^{ed} \pmod{pq}.$$

Thus, it suffices to show that

$$M \equiv M^{ed} \pmod{pq}.$$

Why Does the RSA Cipher Work?

We have that

$$ed \equiv 1 \pmod{(p-1)(q-1)},$$

and therefore

$$ed = 1 + k(p-1)(q-1) \quad \text{for some positive integer } k.$$

Thus,

$$M^{ed} = M^{1+k(p-1)(q-1)} = M(M^{p-1})^{k(q-1)} = M(M^{q-1})^{k(p-1)}$$

Since $p \nmid M$, $M^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem, and so

$$M^{ed} = M(M^{p-1})^{k(q-1)} \equiv M(1)^{k(q-1)} \pmod{p} = M \pmod{p}.$$

Why Does the RSA Cipher Work?

Similarly, since $q \nmid M$, $M^{q-1} \equiv 1 \pmod{q}$, and so

$$M^{ed} = M(M^{q-1})^{k(p-1)} \equiv M(1)^{k(p-1)} = M \pmod{q}.$$

Thus,

$$M^{ed} \equiv M \pmod{p} \quad \text{and} \quad M^{ed} \equiv M \pmod{q}.$$

Since gcd(p,q) = 1, these two formulas imply that

$$M \equiv M^{ed} \pmod{pq}.$$

If $M < pq$, this last congruence implies that

$$M = M^{ed} \ mod \ pq,$$

and thus the RSA cipher gives the correct result.