Discrete Mathematics and Probability **Relations and Modular Arithmetic**
Session 2024/25, Semester 1 Week 5 Tutorial 4 with Solution Notes

Retrieve your submissions from Homework 3 in Week 4 as well as the solution notes on the course website. Compare solutions around the group.

Question 2 from the homework gives three particular functions $f, g, h : \mathbb{R} \to \mathbb{R}$. Question 3 described what it means for a function to be a *section*, with a corresponding *retraction*. Which of f, g, and h is a section? What are suitable corresponding retractions?

Now work together as a group on each of the following tasks, all of which are based on questions in the Epp textbook.

Task A

For this task and the next you will need somewhere to draw diagrams: a whiteboard, pen and paper, an on-screen sketching tool, or similar.

Define relations R and S on $\mathbb{R}$ as follows.

$$\begin{aligned} R &= \{\, (x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 4 \,\} \\ S &= \{\, (x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y \,\} \end{aligned}$$

Graph R, S, $R \cup S$, and $R \cap S$ in the Cartesian plane.

Task B

Let set $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation T as follows.

$$x \; T \; y \quad \Longleftrightarrow \quad 3 \mid (x - y) \qquad \text{for any } x, y \in A$$

Draw a directed graph of T: a node for every element of A and an arrow from node x to node y for every $x \; T \; y$.

This is an equivalence relation. How do the properties of reflexivity, symmetry and transitivity show up in the graph? What are the equivalence classes for the relation T and how do they stand out in the graph?

Task C

A prime number is an integer greater than 1 whose only positive integer factors are itself and 1. Define a relation P as follows:

$$\text{For every } m, n \in \mathbb{Z},\ m \; R \; n \Leftrightarrow \exists \text{a prime number } p \text{ such that } p \mid m \text{ and } p \mid n.$$

For every $m, n \in \mathbb{Z}$, $m \; R \; n$ if and only if there is a prime number p such that $p \mid m$ and $p \mid n$.

Is this relation P reflexive? Symmetric? Transitive? For each of these properties construct a proof or find a counterexample.

Task D

Use the RSA cipher from Examples 8.4.9 and 8.4.10 in Epp to encrypt the following word using modulus 55 and public key 3.

HELLO

The relevant pages from the textbook are at the end of these notes.

Now decrypt the following word.

08 05 15

Task E

Use Theorem 8.4.5 from Epp to prove that for all integers a, b, and c, if $\gcd(a, b) = 1$ with $a \mid c$ and $b \mid c$ then $ab \mid c$.

Task F

Fermat's Little Theorem states that if integer p is a prime number and integer a is not a multiple of p then $a^{p-1} \equiv 1 \pmod{p}$. Verify that this result holds for the following cases.

(a) $a = 15$ and $p = 7$.

(b) $a = 8$ and $p = 11$.

Example 8.4.8 **Finding an Inverse Modulo *n***

a. Find an inverse for 43 modulo 660. That is, find an integer s such that $43s \equiv 1 \pmod{660}$.

b. Find a positive inverse for 3 modulo 40. That is, find a positive integer s such that $3s \equiv 1 \pmod{40}$.

Solution

a. By Example 8.4.7,

$$307 \cdot 43 - 20 \cdot 660 = 1.$$

Adding $20 \cdot 660$ to both sides gives that

$$307 \cdot 43 = 1 + 20 \cdot 660.$$

Thus, by definition of congruence modulo 660,

$$307 \cdot 43 \equiv 1 \pmod{660},$$

so 307 is an inverse for 43 modulo 660.

b. Use the technique of Example 8.4.7 to find a linear combination of 3 and 40 that equals 1.

Step 1: Divide 40 by 3 to obtain $40 = 3 \cdot 13 + 1$. This implies that $1 = 40 - 3 \cdot 13$.

Step 2: Divide 3 by 1 to obtain $3 = 3 \cdot 1 + 0$. This implies that $\gcd(3, 40) = 1$.

Step 3: Use the result of step 1 to write

$$3 \cdot (-13) = 1 + (-1)40.$$

This result implies that -13 is an inverse for 3 modulo 40. In other words, $3 \cdot (-13) \equiv 1 \pmod{40}$. To find a positive inverse, compute $40 - 13$. The result is 27, and

$$27 \equiv -13 \pmod{40}$$

because $27 - (-13) = 40$. So, by Theorem 8.4.3(3),

$$3 \cdot 27 \equiv 3 \cdot (-13) \equiv 1 \pmod{40},$$

and thus by the transitive property of congruence modulo n, 27 is a positive integer that is an inverse for 3 modulo 40. ■

RSA Cryptography

At this point we have developed enough number theory to explain how to encrypt and decrypt messages using the RSA cipher. The effectiveness of the system is based on the fact that although modern computer algorithms make it quite easy to find two distinct large integers p and q—say on the order of several hundred digits each—that are virtually certain to be prime, even the fastest computers are not currently able to factor their product, an integer with approximately twice that many digits. In order to encrypt a message using the RSA cipher, a person needs to know the value of pq and of another integer e, both of which are made publicly available. But only a person who knows the individual values of p and q can decrypt an encrypted message.

We first give an example to show *how* the cipher works and then discuss some of the theory to explain *why* it works. The example is unrealistic in the sense that because p and q are so small, it would be easy to figure out what they are just by knowing

their product. But working with small numbers conveys the idea of the system, while keeping the computations in a range that can be performed with a hand calculator.

Suppose Alice decides to set up an RSA cipher. She chooses two 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 $e = 3$ because 3 is relatively prime to 40. (In practice, taking e to be small could compromise the secrecy of the cipher, so she would take a larger number than 3. However, the mathematics of the cipher works as well for 3 as for a larger number, and the smaller number makes for easier calculations.)

The number pair (pq, e) is Alice's **public key**, which she may distribute widely. Because the RSA cipher works only on numbers, Alice also informs people how she will interpret the numbers in the messages they send her. Let us suppose that she encodes letters of the alphabet in a similar way as was done for the Caesar cipher:

$$A = 01, B = 02, C = 03, \ldots, Z = 26.$$

Let us also assume that the messages Alice receives consist of blocks, each of which, for simplicity, is taken to be a single, numerically encoded letter of the alphabet.

Someone who wants to send Alice a message breaks the message into blocks, each consisting of a single letter, and finds the numeric equivalent for each block. The plaintext, M, in a block is converted into ciphertext, C, according to the following formula:

$$C = M^e \bmod pq. \qquad 8.4.5$$

Note that because (pq, e) is the public key, anyone who has it and knows modular arithmetic can encrypt a message to send to Alice.

Example 8.4.9 **Encrypting a Message Using RSA Cryptography**

Bob wants to send Alice the message HI. What is the ciphertext for his message?

Solution Bob will send his message in two blocks, one for the H and another for the I. Because H is the eighth letter in the alphabet, it is encoded as 08, or 8. The corresponding ciphertext is computed using formula 8.4.5 as follows:

$$\begin{aligned} C &= 8^3 \bmod 55 \\ &= 512 \bmod 55 \\ &= 17. \end{aligned}$$

Because I is the ninth letter in the alphabet, it is encoded as 09, or 9. The corresponding ciphertext is

$$\begin{aligned} C &= 9^3 \bmod 55 \\ &= 729 \bmod 55 \\ &= 14. \end{aligned}$$

Accordingly, Bob sends Alice the message: 17 14. ■

To decrypt the message, the *decryption key* must be computed. It is a number d that is a positive inverse to e modulo $(p - 1)(q - 1)$. The plaintext M is obtained from the ciphertext C by the formula

$$M = C^d \bmod pq, \text{ where the number pair } (pq, d) \text{ is Alice's } \textbf{private key}. \qquad 8.4.6$$

Note that because $M + kpq \equiv M \pmod{pq}$, M must be taken to be less than pq, as in the above example, in order for the decryption to be guaranteed to produce the original message. But because p and q are normally taken to be so large, this requirement does not cause problems. Long messages are broken into blocks of symbols to meet the restriction and several symbols are included in each block to prevent decryption based on knowledge of letter frequencies.

Example 8.4.10 **Decrypting a Message Using RSA Cryptography**

Imagine that Alice has hired you to help her decrypt messages and has shared with you the values of p and q. Compute Alice's private key (pq, d) and use the formula $M = C^d \bmod pq$ to decrypt the following ciphertext for her: 17 14.

Solution Because $p = 5$ and $q = 11$, $(p-1)(q-1) = 40$, the decryption key d is a positive inverse for 3 modulo 40. Knowing that you would need this number, we computed it in Example 8.4.8(b) and found it to be 27. Thus to decrypt the ciphertext 17, you need to compute

$$M = 17^d \bmod pq = 17^{27} \bmod 55.$$

To do so, note that

$$27 = 16 + 8 + 2 + 1.$$

Next, find the residues obtained when 17 is raised to successively higher powers of 2, up to $2^4 = 16$:

$$\begin{aligned}
17 \bmod 55 &= 17 \bmod 55 &&= 17\\
17^2 \bmod 55 &= 17^2 \bmod 55 &&= 14\\
17^4 \bmod 55 &= (17^2)^2 \bmod 55 &&= 14^2 \bmod 55 = 31\\
17^8 \bmod 55 &= (17^4)^2 \bmod 55 &&= 31^2 \bmod 55 = 26\\
17^{16} \bmod 55 &= (17^8)^2 \bmod 55 &&= 26^2 \bmod 55 = 16
\end{aligned}$$

Then use the fact that

$$17^{27} = 17^{16+8+2+1} = 17^{16} \cdot 17^8 \cdot 17^2 \cdot 17^1$$

to write

$$\begin{aligned}
17^{27} \bmod 55 &= (17^{16} \cdot 17^8 \cdot 17^2 \cdot 17) \bmod 55\\
&\equiv [(17^6 \bmod 55)(17^8 \bmod 55)(17^2 \bmod 55)(17 \bmod 55)] \pmod{55}\\
&\qquad \text{by Corollary 8.4.4}\\
&\equiv (16 \cdot 26 \cdot 14 \cdot 17) \pmod{55}\\
&\equiv 99008 \pmod{55}\\
&\equiv 8 \pmod{55}.
\end{aligned}$$

Hence $17^{27} \bmod 55 = 8$, and thus the plaintext of the first part of Bob's message is 8, or 08. In the last step, you find the letter corresponding to 08, which is *H*. In exercises 14 and 15 at the end of this section, you are asked to show that when you decrypt 14, the result is 9, which corresponds to the letter I, so you can tell Alice that Bob's message is HI. ■

Figure 8.4.1 illustrates the process of sending and receiving a message using RSA cryptography.

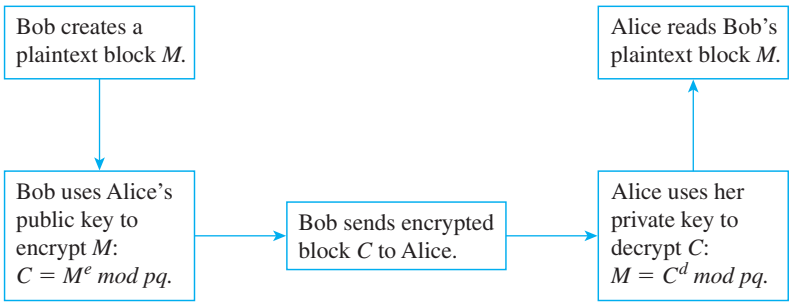


FIGURE 8.4.1 Using RSA cryptography

Solution Notes

For Homework 3 see the solution notes on the course web pages.

Function $f(x) = -x$ is a bijection, which means it is also a section with its inverse as a retraction. It also happens to be self-inverse, so is a section for itself. This is a rather unusual case.

Function $g(x) = 2^x$ is not a bijection, but we can still find a retraction which has g as a section. For example, the following:

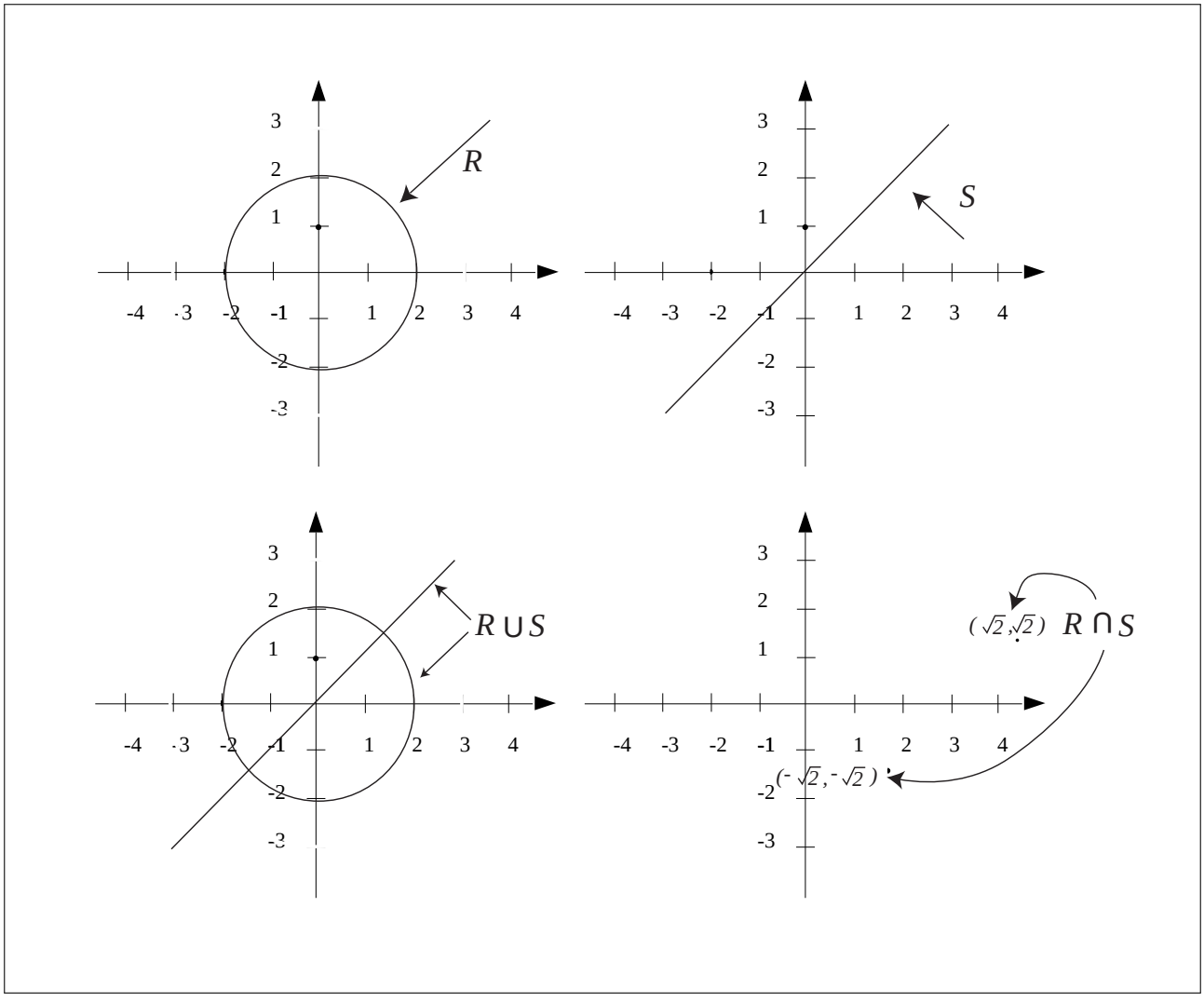
$$j(x) \;=\; \begin{cases} \log_2(y) & \text{if } y > 0 \\ 0 & \text{if } y \leq 0. \end{cases}$$

This has $(j \circ g) = I_{\mathbb{R}}$, the identity on real numbers as $\log_2(2^x) = x$ for all $x \in \mathbb{R}$.

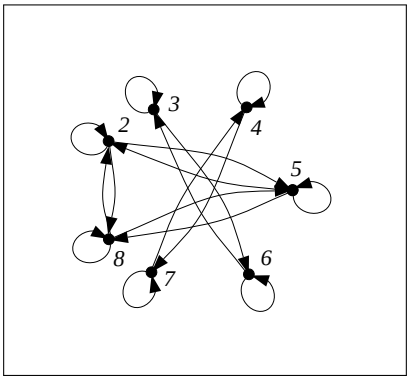
Function $h(x) = (x^3 - x)$ is not injective and that means it is not a section: there is no function $k : \mathbb{R} \to \mathbb{R}$ such that $(k \circ h) = I_{\mathbb{R}}$. To demonstrate this, note that $h(-1) = h(0) = h(1) = 0$: if $(k \circ h)$ was the identity then we would need $k(0)$ to equal -1, 0, and 1 all at the same time.

Task A

This and other boxed notes are taken from the Instructor's Manual for the Epp textbook.



Task B



Reflexivity of T appears as self-loops on every node. Symmetry shows up as every arrow having a reverse arrow. Transitivity is that for any chain of arrows leading in to one another their composition is also an arrow in the graph.

The equivalence classes are $\{2, 5, 8\}$, $\{3, 6\}$, and $\{4, 7\}$. These appear as *connected components* of the graph: groups of nodes where you can get from one to another inside the group by following arrows, but not from one group to another. For more on these see the sections on *Subgraphs* and *Connectedness* in Chapter 10 of Epp, pages 682–683.

Task C

P is not reflexive: P is reflexive $\Leftrightarrow$ for every integer n, $n\ P\ n$. By definition of P this means that for every integer n, $\exists$ a prime number p such that $p \mid n$ and $p \mid n$. This is false. As a counterexample, take $n = 1$. There is no prime number that divides 1.

P is symmetric: *[We must show that for all integers m and n, if $m\ P\ n$ then $n\ P\ m$.]* Suppose m and n are integers such that $m\ P\ n$. By definition of P this means that there exists a prime number p such that $p \mid m$ and $p \mid n$. But to say that "$p \mid m$ and $p \mid n$" is logically equivalent to saying that "$p \mid n$ and $p \mid m$." Hence there exists a prime number p such that $p \mid n$ and $p \mid m$, and so by definition of P, $n\ P\ m$.

P is not transitive: P is transitive $\Leftrightarrow$ for all integers m, n, and p, if $m\ P\ n$ and $n\ P\ p$ then $m\ P\ p$. This is false. As a counterexample, take $m = 2$, $n = 6$, and $p = 9$. Then $m\ P\ n$ because the prime number 2 divides both 2 and 6 and $n\ P\ p$ because the prime number 3 divides both 6 and 9, but m is not related to p by P because the numbers 2 and 9 have no common prime factor.

Task D

The letters in HELLO translate numerically into 08, 05, 12, 12, and 15. By Example 8.4.9, the H is encrypted as 17. To encrypt E, we compute $5^3\ mod\ 55 = 15$. To encrypt L, we compute $12^3\ mod\ 55 = 23$. And to encrypt O, we compute $15^3\ mod\ 55 = 20$. Thus the ciphertext is 17 15 23 23 20. (In practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words.)

By Example 8.4.10, the decryption key is 27. Thus the residues modulo 55 for 8^{27}, 5^{27}, and 15^{27} must be found and then translated into letters of the alphabet. Because $27 = 16+8+2+1$, we first perform the following computations:

$8^1 \equiv 8 \pmod{55}$	$5^1 \equiv 5 \pmod{55}$	$15^1 \equiv 15 \pmod{55}$
$8^2 \equiv 9 \pmod{55}$	$5^2 \equiv 25 \pmod{55}$	$15^2 \equiv 5 \pmod{55}$
$8^4 \equiv 9^2 \equiv 26 \pmod{55}$	$5^4 \equiv 25^2 \equiv 20 \pmod{55}$	$15^4 \equiv 5^2 \equiv 25 \pmod{55}$
$8^8 \equiv 26^2 \equiv 16 \pmod{55}$	$5^8 \equiv 20^2 \equiv 15 \pmod{55}$	$15^8 \equiv 25^2 \equiv 20 \pmod{55}$
$8^{16} \equiv 16^2 \equiv 36 \pmod{55}$	$5^{16} \equiv 15^2 \equiv 5 \pmod{55}$	$15^{16} \equiv 20^2 \equiv 15 \pmod{55}$

Then we compute

$8^{27}\ mod\ 55 = (36 \cdot 16 \cdot 9 \cdot 8)\ mod\ 55 = 2,$

$5^{27}\ mod\ 55 = (5 \cdot 15 \cdot 25 \cdot 5)\ mod\ 55 = 25,$

$15^{27}\ mod\ 55 = (15 \cdot 20 \cdot 5 \cdot 15)\ mod\ 55 = 5.$

Finally, because 2, 25, and 5 translate into letters as B, Y, and E, we see that the message is BYE.

Task E

Proof: Suppose a, b, and c are integers such that $\gcd(a, b) = 1$, $a \mid c$, and $b \mid c$. We will show that $ab \mid c$.

By Corollary 8.4.6 (or by Theorem 8.4.5), there exist integers s and t such that $as + bt = 1$.

Also, by definition of divisibility, $c = au = bv$, for some integers u and v. Hence, by substitution,

$$c = asc + btc = as(bv) + bt(au) = ab(sv + tu).$$

But $sv + tu$ is an integer, and so, by definition of divisibility, $ab \mid c$ *[as was to be shown]*.

Task F

a. When $a = 15$ and $p = 7$,

$$a^{p-1} = 15^6 = 11390625 \equiv 1 \pmod{7} \text{ because } 11390625 - 1 = 7 \cdot 1627232.$$

b. When $a = 8$ and $p = 11$,

$$a^{p-1} = 8^{10} = 1073741824 \equiv 1 \pmod{11} \text{ because } 1073741824 - 1 = 11 \cdot 97612893.$$