DMP Tutorial 4 Week 5

Task 1 Share and discuss homework

Task 2 For the task and the next you will need a whiteboard, pencil and paper, or other drawing tool.

> Define relations R and S on $\mathbf{R}$ as follows:
>
> $$R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x^2 + y^2 = 4\} \quad \text{and}$$
> $$S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x = y\}.$$
>
> Graph R, S, $R \cup S$, and $R \cap S$ in the Cartesian plane.

Task 3 Draw a directed graph of the following relation

> Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation T on A as follows: For every $x, y \in A$,
>
> $$x \, T \, y \quad \Leftrightarrow \quad 3 \mid (x - y).$$

Discuss what properties of the relation you can see on your graph.

Task 4 The following text defines a relation *P*.

> Recall that a prime number is an integer that is greater than 1 and has no positive integer divisors other than 1 and itself. (In particular, 1 is not prime.) A relation P is defined on $\mathbf{Z}$ as follows: For every $m, n \in \mathbf{Z}$, $m \, P \, n \Leftrightarrow \exists$ a prime number p such that $p \mid m$ and $p \mid n$.

Is this relation reflexive? symmetric? transitive? None of these? Explain your answer.

Task 5

Use the RSA cipher from Examples 8.4.9 and 8.4.10 to encrypt this word:

HELLO

You can find relevant pages from the textbook at the end of this document.

Now decrypt this message:

13 20 20 09

Task 6

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

Task 7

Fermat's Little Theorem states that if p is a prime number and a and p are relatively prime, then $a^{p-1} \equiv 1 \ (mod\ p)$. Verify that this theorem gives correct results 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:

$$C = M^e \bmod pq. \tag{8.4.5}$$

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

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

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.

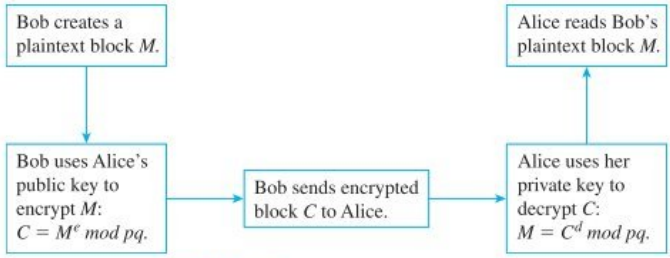

FIGURE 8.4.1 Using RSA cryptography

Euclid's Lemma

Another consequence of Theorem 8.4.5 is known as *Euclid's lemma*. It is the crucial fact behind the unique factorization theorem for the integers and is also of great importance in many other parts of number theory.

Theorem 8.4.8 Euclid's Lemma

For all integers a, b, and c, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

Proof: Suppose a, b, and c are integers, $\gcd(a, c) = 1$, and $a \mid bc$. *[We must show that* $a|b$*.]* By Theorem 8.4.5, there exist integers s and t so that

$$as + ct = 1.$$

Multiply both sides of this equation by b to obtain

$$bas + bct = b. \tag{8.4.7}$$

Since $a|bc$, by definition of divisibility there exists an integer k such that

$$bc = ak. \tag{8.4.8}$$

Substituting (8.4.8) into (8.4.7), rewriting, and factoring out an a gives that

$$b = bas + (ak)t = a(bs + kt).$$

Let $r = bs + kt$. Then r is an integer (because b, s, k, and t are all integers), and $b = ar$. Thus $a|b$ by definition of divisibility.

The unique factorization theorem for the integers states that any integer greater than 1 has a unique representation as a product of prime numbers, except possibly for the order in which the numbers are written. The hint for exercise 13 of Section 5.4 outlined a proof of the existence part of the proof, and the uniqueness of the representation follows quickly from Euclid's lemma. In exercise 41 at the end of this section, we outline a proof for you to complete.

Another application of Euclid's lemma is a cancellation theorem for congruence modulo n. This theorem allows us—under certain circumstances—to divide out a common factor in a congruence relation.

Theorem 8.4.9 Cancellation Theorem for Modular Congruence

For all integers a, b, c, and n with $n > 1$, if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

(continued on page 540)