CHAPTER 8

RELATIONS

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

In fact, the National Security Agency, whose main business is cryptography, is the largest employer of mathematicians in the United States.

With the rise of electronic communication systems, however, especially the Internet, an extremely important current use of cryptography is to make it possible to send private information, such as credit card numbers, banking data, medical records, and so forth, over electronic channels.

Many systems for sending secret messages require both the sender and the receiver to know both the encryption and the decryption procedures.

Modular Arithmetic with Applications to Cryptography

For instance, 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 wrapping around to A, Y to B, and Z to C.

In other words, say each letter of the alphabet is coded by its position relative to the others—so that
A = 01, B = 02, . . . , 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

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

For reference, here are the letters of the alphabet, together with their numeric equivalents:

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

Example 1 – *Encrypting and Decrypting with the Caesar Cipher*

a. Use the Caesar cipher to encrypt the message
HOW ARE YOU.

b. Use the Caesar cipher to decrypt the message
L DP ILQH.

Example 1(a) – *Solution*

First translate the letters of HOW ARE YOU into their numeric equivalents:

08 15 23 01 18 05 25 15 21.

Next encrypt the message by adding 3 to each number. The result is

11 18 26 04 21 08 02 18 24.

Finally, substitute the letters that correspond to these numbers. The encrypted message becomes

KRZ DUH BRX.

Example 1(b) – *Solution*

cont’d

First translate the letters of L DP ILQH into their numeric equivalents:

12 04 16 09 12 17 08.

Next decrypt the message by subtracting 3 from each number:

09 01 13 06 09 14 05.

Then translate back into letters to obtain the original message: I AM FINE.

Properties of Congruence Modulo *n*

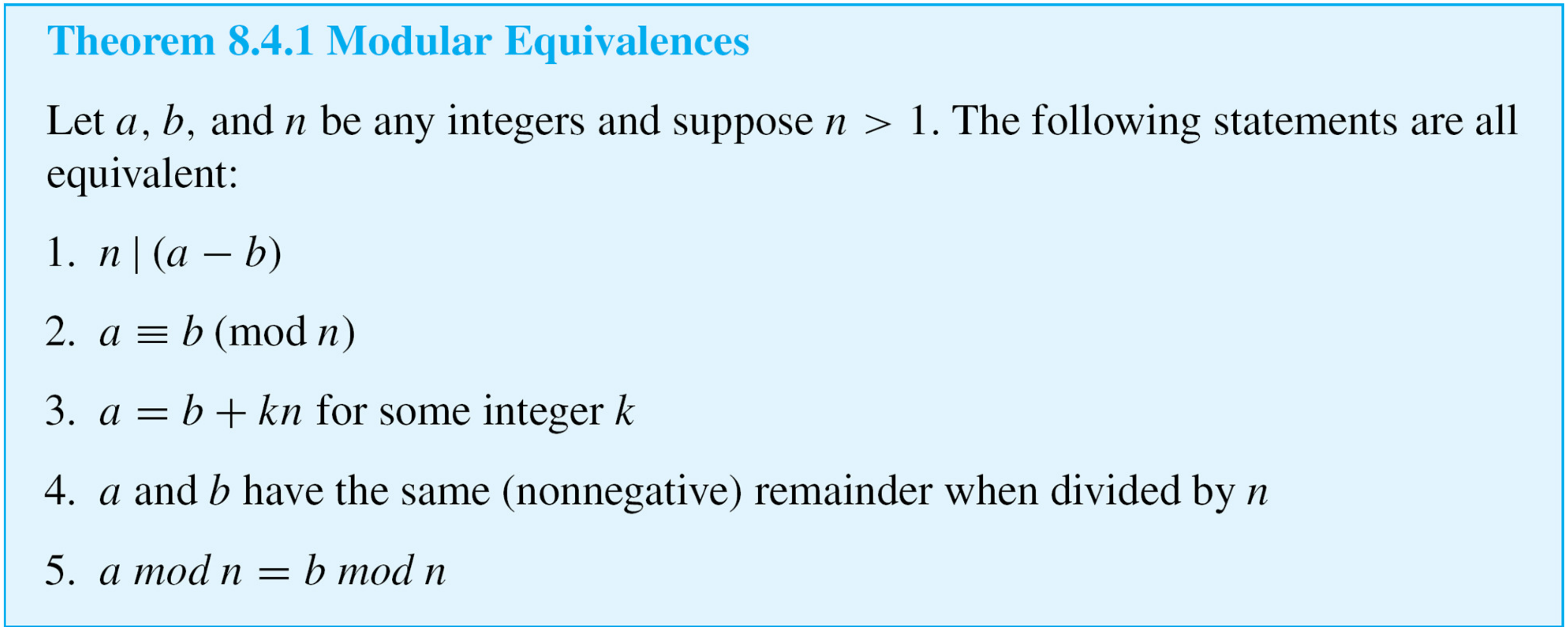
Properties of Congruence Modulo *n*

The first theorem in this section brings together a variety of equivalent ways of expressing the same basic arithmetic fact.

Sometimes one way is most convenient; sometimes another way is best.

You need to be comfortable moving from one to another, depending on the nature of the problem you are trying to solve.

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

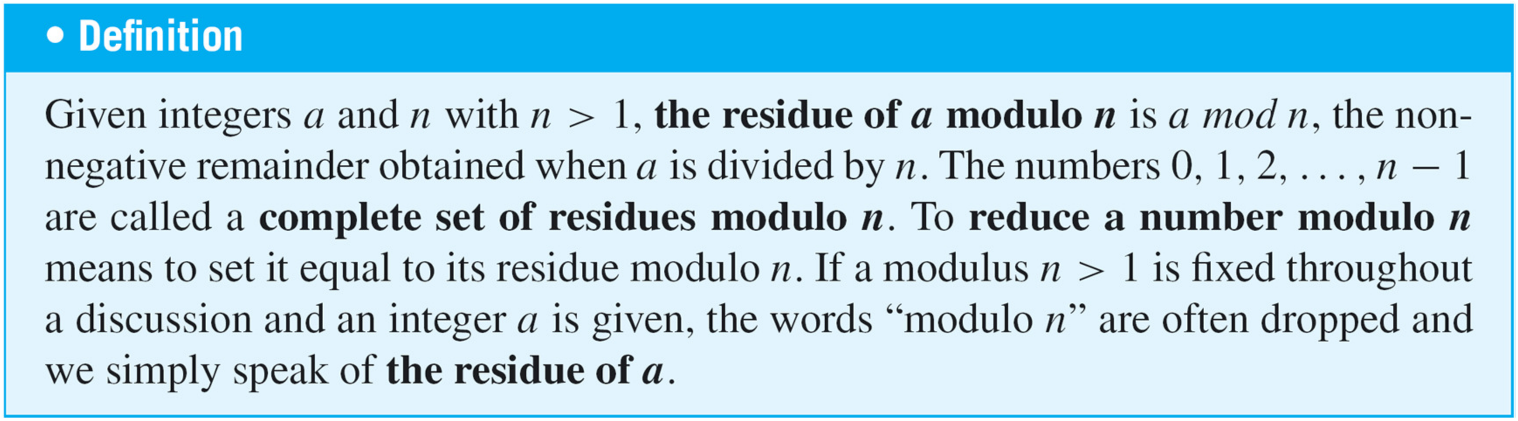
5. $a \; mod \; n = b \; mod \; n$

Properties of Congruence Modulo *n*

Another consequence of the quotient-remainder theorem is this: When an integer a is divided by a positive integer n, a unique quotient q and remainder r are obtained with the property that $a = nq + r$ and $0 \leq r < n$.

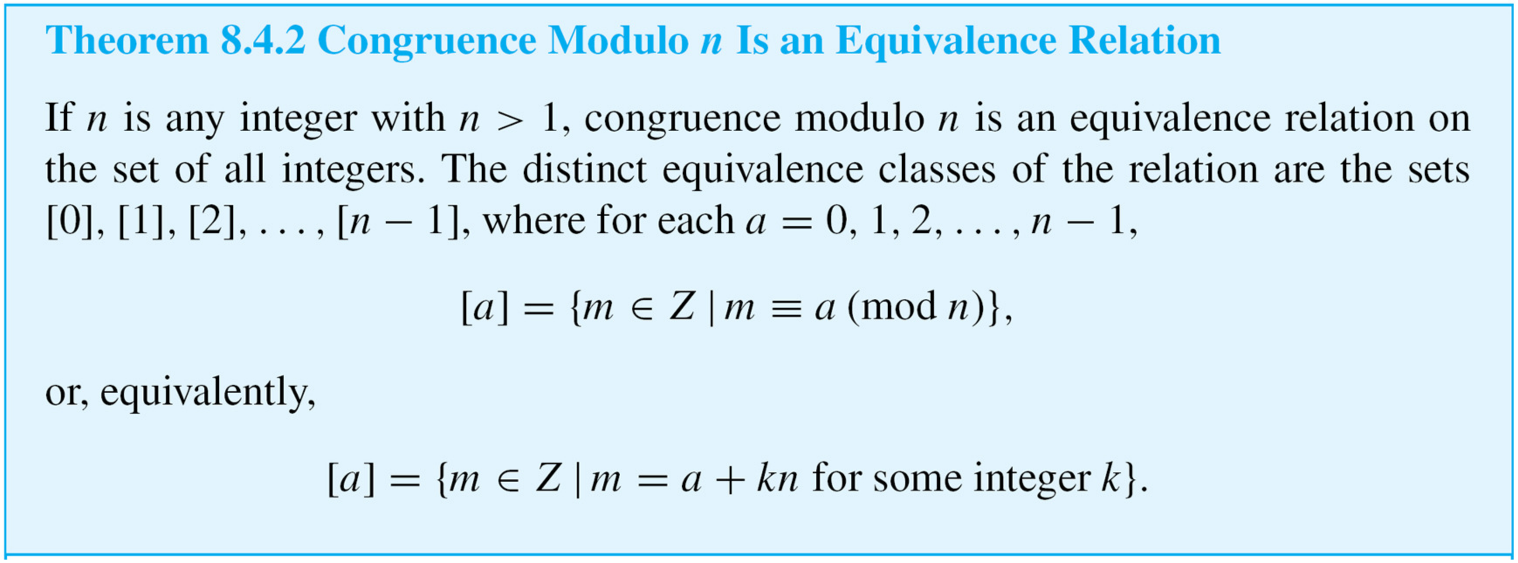
Because there are exactly n integers that satisfy the inequality $0 \leq r < n$ (the numbers from 0 through $n - 1$), there are exactly n possible remainders that can occur. These are called the *least nonnegative residues modulo n* or simply the *residues modulo n*.

Properties of Congruence Modulo *n*



- **Definition**

Given integers a and n with $n > 1$, **the residue of *a* modulo *n*** is a *mod* n, the nonnegative remainder obtained when a is divided by n. The numbers $0, 1, 2, \ldots, n - 1$ are called a **complete set of residues modulo *n***. To **reduce a number modulo *n*** means to set it equal to its residue modulo n. If a modulus $n > 1$ is fixed throughout a discussion and an integer a is given, the words "modulo n" are often dropped and we simply speak of **the residue of *a***.



Theorem 8.4.2 Congruence Modulo *n* Is an Equivalence Relation

If n is any integer with $n > 1$, congruence modulo n is an equivalence relation on the set of all integers. The distinct equivalence classes of the relation are the sets $[0], [1], [2], \ldots, [n - 1]$, where for each $a = 0, 1, 2, \ldots, n - 1$,

$$[a] = \{m \in Z \mid m \equiv a \ (\text{mod } n)\},$$

or, equivalently,

$$[a] = \{m \in Z \mid m = a + kn \text{ for some integer } k\}.$$

Modular Arithmetic

Modular Arithmetic

A fundamental fact about congruence modulo *n* is that if you first perform an addition, subtraction, or multiplication on integers and then reduce the result modulo *n*, you will obtain the same answer as if you had first reduced each of the numbers modulo *n*, performed the operation, and then reduced the result modulo *n*.

For instance, instead of computing

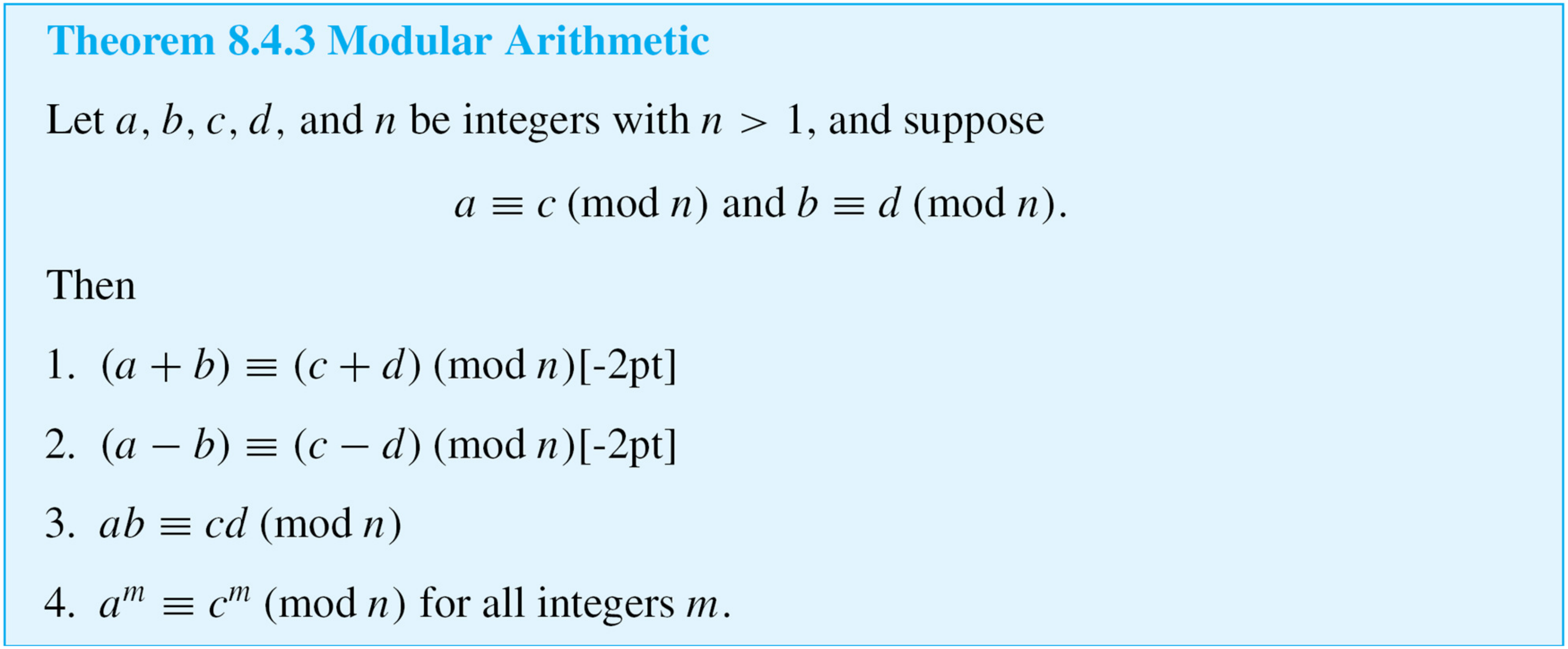
$$(5 \cdot 8) = 40 \equiv 1 \pmod{3}$$

you will obtain the same answer if you compute

$$(5\ \mathit{mod}\ 3)(8\ \mathit{mod}\ 3) = 2 \cdot 2 = 4 \equiv 1 \pmod{3}.$$

Modular Arithmetic

The fact that this process works is a result of the following theorem.



Theorem 8.4.3 Modular Arithmetic

Let a, b, c, d, and n be integers with $n > 1$, and suppose

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}.$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$[-2pt]
2. $(a - b) \equiv (c - d) \pmod{n}$[-2pt]
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$ for all integers m.

Example 2 – *Getting Started with Modular Arithmetic*

The most practical use of modular arithmetic is to reduce computations involving large integers to computations involving smaller ones. For instance, note that $55 \equiv 3 \pmod 4$ because $55 - 3 = 52$, which is divisible by 4, and $26 \equiv 2 \pmod 4$ because $26 - 2 = 24$, which is also divisible by 4. Verify the following statements.

a. $55 + 26 \equiv (3 + 2) \pmod 4$

b. $55 - 26 \equiv (3 - 2) \pmod 4$

c. $55 \cdot 26 \equiv (3 \cdot 2) \pmod 4$

d. $55^2 \equiv 3^2 \pmod 4$

Example 2 – *Solution*

a. Compute 55 + 26 = 81 and 3 + 2 = 5. By definition of congruence modulo *n*, to show that 81 ≡ 5 (mod 4), you need to show that 4 | (81 – 5). But this is true because 81 – 5 = 76, and 4 | 76 since 76 = 4 • 19.

b. Compute 55 – 26 = 29 and 3 – 2 = 1. By definition of congruence modulo *n*, to show that 29 ≡ 1 (mod 4), you need to show that 4 | (29 – 1). But this is true because 29 – 1 = 28, and 4 | 28 since 28 = 4 • 7.

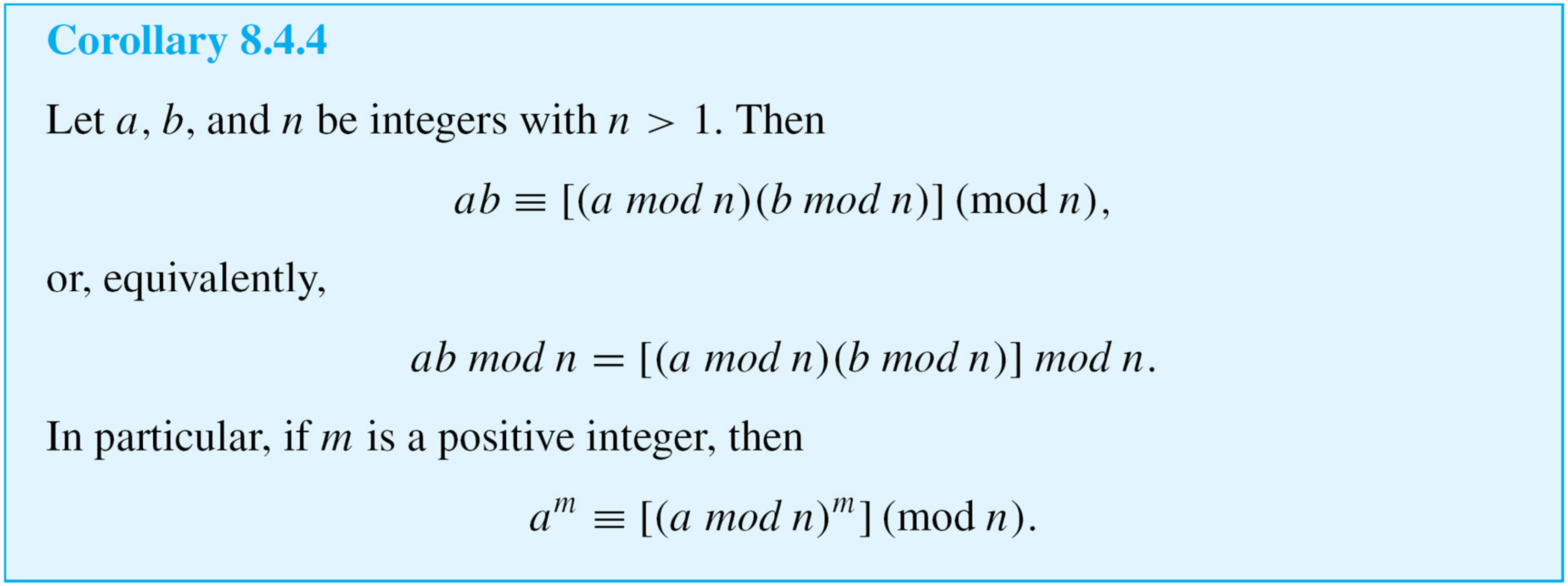
Example 2 – *Solution*

cont'd

c. Compute $55 \cdot 26 = 1430$ and $3 \cdot 2 = 6$. By definition of congruence modulo n, to show that $1430 \equiv 6 \pmod 4$, you need to show that $4 \mid (1430 - 6)$. But this is true because $1430 - 6 = 1424$, and $4 \mid 1424$ since $1424 = 4 \cdot 356$.

d. Compute $55^2 = 3025$ and $3^2 = 9$. By definition of congruence modulo n, to show that $3025 \equiv 9 \pmod 4$, you need to show that $4 \mid (3025 - 9)$. But this is true because $3025 - 9 = 3016$, and $4 \mid 3016$ since $3016 = 4 \cdot 754$.

Modular Arithmetic



Corollary 8.4.4

Let a, b, and n be integers with $n > 1$. Then

$$ab \equiv [(a \; mod \; n)(b \; mod \; n)] \; (\text{mod} \; n),$$

or, equivalently,

$$ab \; mod \; n = [(a \; mod \; n)(b \; mod \; n)] \; mod \; n.$$

In particular, if m is a positive integer, then

$$a^m \equiv [(a \; mod \; n)^m] \; (\text{mod} \; n).$$

Example 3 – *Computing a Product Modulo n*

As in Example 2, note that $55 \equiv 3 \pmod{4}$ and $26 \equiv 2 \pmod{4}$. Because both 3 and 2 are less than 4, each of these numbers is a least nonnegative residue modulo 4. Therefore, $55 \text{ } mod \text{ } 4 = 3$ and $26 \text{ } mod \text{ } 4 = 2$. Use the notation of Corollary 8.4.4 to find the residue of $55 \cdot 26$ modulo 4.

Solution:

We know that to use a calculator to compute remainders, you can use the formula $n \text{ } mod \text{ } d = n - d \cdot \lfloor n/d \rfloor$. If you are using a hand calculator with an "integer part" feature and both *n* and *d* are positive, then $\lfloor n/d \rfloor$ is the integer part of the division of *n* by *d*.

Example 3 – *Solution*

cont'd

When you divide a positive integer *n* by a positive integer *d* with a more basic calculator, you can see $\lfloor n/d \rfloor$ on the calculator display by simply ignoring the digits that follow the decimal point.

By Corollary 8.4.4,

$$\begin{aligned}
(55 \cdot 26)\ mod\ 4 &= \{(55\ mod\ 4)(26\ mod\ 4)\}\ mod\ 4 \\
&\equiv (3 \cdot 2)\ mod\ 4 && \text{because } 55 \bmod 4 = 3 \text{ and } 26 \bmod 4 = 2 \\
&\equiv 6\ mod\ 4 \\
&\equiv 2 && \text{because } 4 \mid (6-2) \text{ and } 2 < 4.
\end{aligned}$$

Modular Arithmetic

When modular arithmetic is performed with very large numbers, as is the case for RSA crytography, computations are facilitated by using two properties of exponents.

The first is

$$\boxed{x^{2a} = (x^a)^2 \quad \text{for all real numbers } x \text{ and } a \text{ with } x \geq 0.} \qquad 8.4.1$$

Modular Arithmetic

Thus, for instance, if *x* is any positive real number, then

$$\begin{aligned} x^4 \mathit{mod}\, n &= (x^2)^2 \mathit{mod}\, n && \text{because } (x^2)^2 = x^4 \\ &= (x^2 \mathit{mod}\, n)^2 \mathit{mod}\, n && \text{by Corollary 8.4.4.} \end{aligned}$$

Hence you can reduce x^4 modulo *n* by reducing x^2 modulo *n* and then reducing the square of the result modulo *n*.

Modular Arithmetic

Because all the residues are less than *n*, this process limits the size of the computations to numbers that are less than *n*^{2}, which makes them easier to work with, both for humans (when the numbers are relatively small) and for computers (when the numbers are very large).

A second useful property of exponents is

$$\boxed{x^{a+b} = x^a x^b \quad \text{for all real numbers } x, a, \text{ and } b \text{ with } x \geq 0.} \qquad 8.4.2$$

Example 4 – *Computing a^k mod n When k Is a Power of 2*

Find 144^4 *mod* 713.

Solution:

Use property (8.4.1) to write $144^4 = (144^2)^2$. Then

$$\begin{aligned} 144^4 \, mod \, 713 &= (144^2)^2 \, mod \, 713 \\ &= (144^2 \, mod \, 713)^2 \, mod \, 713 \\ &= (20736 \, mod \, 713)^2 \, mod \, 713 \qquad \text{because } 144^2 = 20736 \end{aligned}$$

Example 4 – *Solution*

cont'd

$= \quad 59^2 \; mod \; 713$ because $20736 \; mod \; 713 = 59$

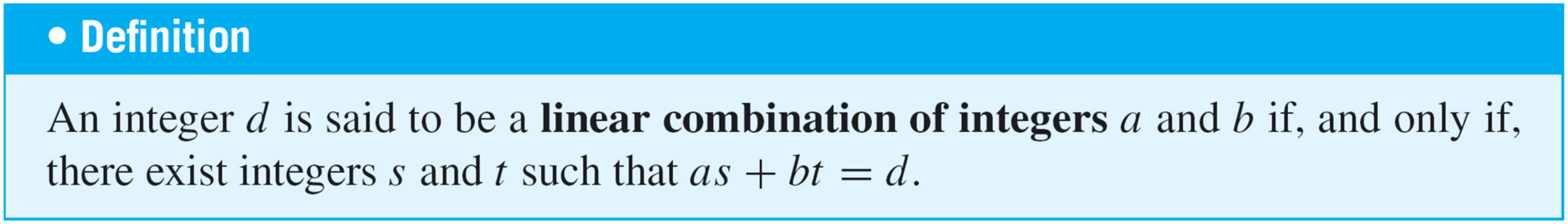
$= \quad 3481 \; mod \; 713$ because $59^2 = 3481$

$= \quad 629$ because $3481 \; mod \; 713 = 629$.

Extending the Euclidean Algorithm

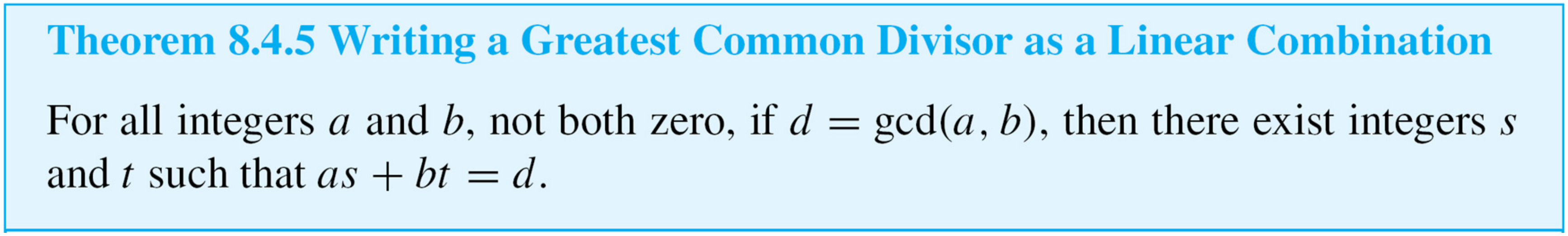
Extending the Euclidean Algorithm

An extended version of the Euclidean algorithm can be used to find a concrete expression for the greatest common divisor of integers *a* and *b.*



● **Definition**

An integer d is said to be a **linear combination of integers** a and b if, and only if, there exist integers s and t such that $as + bt = d$.



Theorem 8.4.5 Writing a Greatest Common Divisor as a Linear Combination

For all integers a and b, not both zero, if $d = \gcd(a, b)$, then there exist integers s and t such that $as + bt = d$.

Example 6 – *Expressing a Greatest Common Divisor as a Linear Combination*

Use Euclidean algorithm to express gcd(330, 156) as a linear combination of 330 and 156.

Solution:

The first four steps of the solution were obtained by successive applications of the quotient-remainder theorem.

The fifth step shows how to find the coefficients of the linear combination by substituting back through the results of the previous steps.

Example 6 – *Solution*

cont'd

Step 1: 330 = 156 · 2 + 18, which implies that
18 = 330 – 156 · 2.

Step 2: 156 = 18 · 8 + 12, which implies that
12 = 156 – 18 · 8.

Step 3: 18 = 12 · 1 + 6, which implies that 6 = 18 – 12 · 1.

Step 4: 12 = 6 · 2 + 0, which implies that gcd(330, 156) = 6.

Step 5: By substituting back through steps 3 to 1:

$$\begin{aligned} 6 &= 18 - 12 \cdot 1 && \text{from step 3} \\ &= 18 - (156 - 8 \cdot 18) \cdot 1 && \text{by substitution from step 2} \end{aligned}$$

Example 6 – *Solution*

cont'd

$$
\begin{aligned}
&= 9 \cdot 18 + (-1) \cdot 156 && \text{by algebra} \\
&= 9 \cdot (330 - 156 \cdot 2) + (-1) \cdot 156 && \text{by substitution from step 1} \\
&= 9 \cdot 330 + (-19) \cdot 156 && \text{by algebra.}
\end{aligned}
$$

Thus gcd(330, 156) = 9 • 330 + (–19) • 156. (It is always a good idea to check the result of a calculation like this to be sure you did not make a mistake. In this case, you find that 9 • 330 + (–19) • 156 does indeed equal 6.)

Finding an Inverse Modulo *n*

Finding an Inverse Modulo *n*

Suppose you want to solve the following congruence for x:

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

Note that $3 \cdot 2 = 6 \equiv 1 \pmod{5}$. So you can think of 3 as a kind of inverse for 2 modulo 5 and multiply both sides of the congruence to be solved by 3 to obtain

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

But $6 \equiv 1 \pmod{5}$, and so by Theorem 8.4.3(3),
$6x \equiv 1x \pmod{5} \equiv x \pmod{5}$.

Finding an Inverse Modulo *n*

Thus, by the symmetric and transitive properties of modular congruence,

$$x \equiv 4 \pmod{5},$$

and hence a solution is $x = 4$. (You can check that $2 \cdot 4 = 8 \equiv 3 \pmod{5}$.)

Unfortunately, it is not always possible to find an “inverse” modulo an integer *n*.

Finding an Inverse Modulo *n*

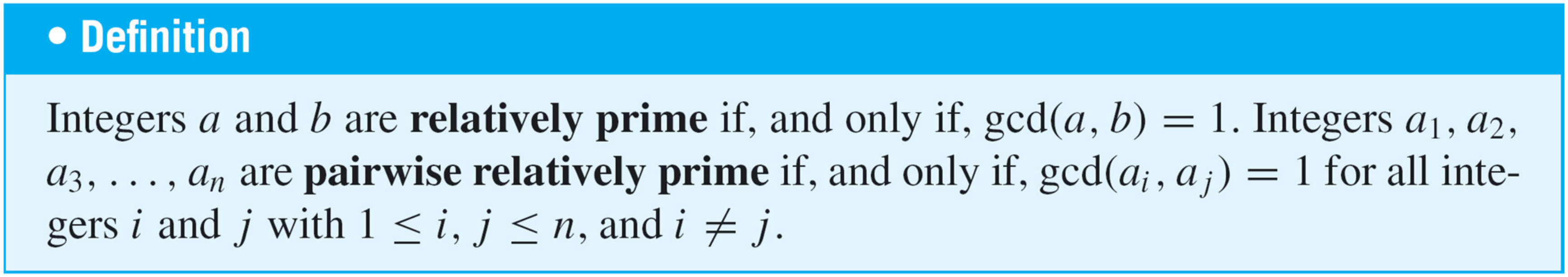
For instance, observe that

$$\begin{aligned} 2\cdot 1 &\equiv 2 \pmod 4) \\ 2\cdot 2 &\equiv 0 \pmod 4) \\ 2\cdot 3 &\equiv 2 \pmod 4). \end{aligned}$$

By Theorem 8.4.3, these calculations suffice for us to conclude that the number 2 does not have an inverse modulo 4.

Describing the circumstances in which inverses exist in modular arithmetic requires the concept of relative primeness.

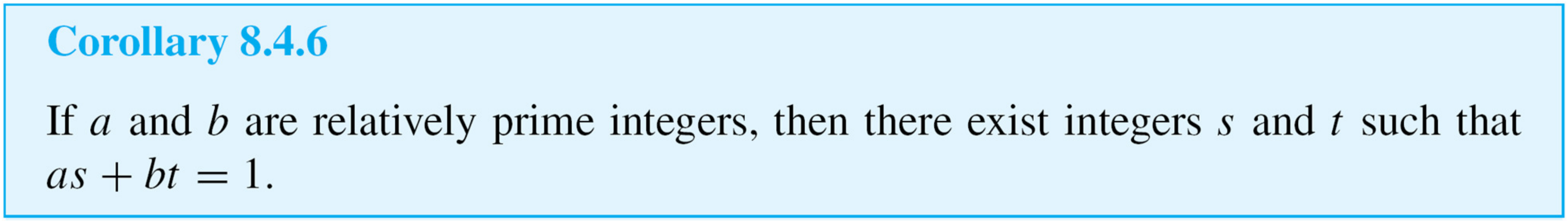
Finding an Inverse Modulo *n*



- **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 $1 \le i, j \le n$, and $i \ne j$.

Given the definition of relatively prime integers, the following corollary is an immediate consequence of theorem 8.4.5.



Corollary 8.4.6

If a and b are relatively prime integers, then there exist integers s and t such that $as + bt = 1$.

Example 7 – *Expressing* 1 *as a Linear Combination of Relatively Prime Integers*

Show that 660 and 43 are relatively prime, and find a linear combination of 660 and 43 that equals 1.

Solution:

Step 1: Divide 660 by 43 to obtain $660 = 43 \cdot 15 + 15$, which implies that $15 = 660 - 43 \cdot 15$.

Step 2: Divide 43 by 15 to obtain $43 = 15 \cdot 2 + 13$, which implies that $13 = 43 - 15 \cdot 2$.

Step 3: Divide 15 by 13 to obtain $15 = 13 \cdot 1 + 2$, which implies that $2 = 15 - 13$.

Example 7 – *Solution*

cont'd

Step 4: Divide 13 by 2 to obtain 13 = 2 • 6 + 1, which implies that 1 = 13 – 2 • 6.

Step 5: Divide 2 by 1 to obtain 2 = 1 • 2 + 0, which implies that gcd(660, 43) = 1 and so 660 and 43 are relatively prime.

Step 6: To express 1 as a linear combination of 660 and 43, substitute back through steps 4 to 1:

$$\begin{aligned} 1 &= 13 - 2 \cdot 6 && \text{from step 4} \\ &= 13 - (15 - 13) \cdot 6 && \text{by substitution from step 3} \end{aligned}$$

Example 7 – *Solution*

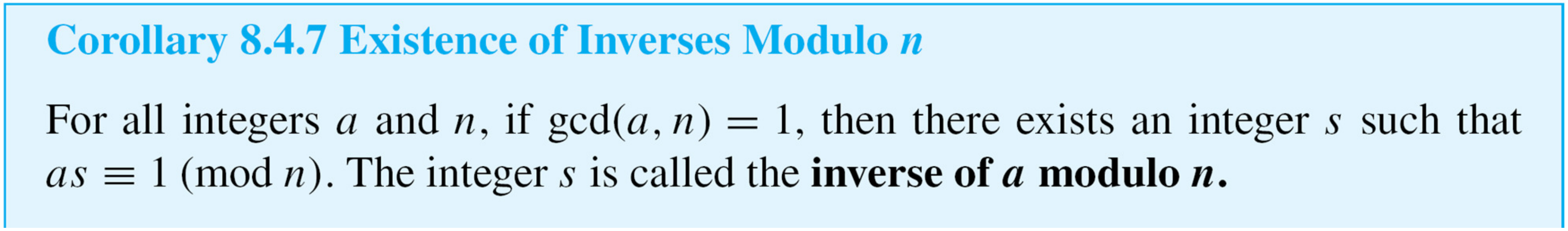
cont'd

$$
\begin{aligned}
&= 7\cdot 13 - 6\cdot 15 && \text{by algebra}\\
&= 7\cdot(43 - 15\cdot 2) - 6\cdot 15 && \text{by substitution from step 2}\\
&= 7\cdot 43 - 20\cdot 15 && \text{by algebra}\\
&= 7\cdot 43 - 20\cdot(660 - 43\cdot 15) && \text{by substitution from step 1}\\
&= 307\cdot 43 - 20\cdot 660 && \text{by algebra}
\end{aligned}
$$

Thus gcd(660, 43) = 1 = 307 • 43 – 20 • 660. (And a check by direct computation confirms that 307 • 43 – 20 • 660 does indeed equal 1.)

Finding an Inverse Modulo *n*

A consequence of Corollary 8.4.6 is that under certain circumstances, it is possible to find an inverse for an integer modulo *n*.



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.**

RSA Cryptography

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.

RSA Cryptography

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.

RSA Cryptography

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.

RSA Cryptography

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.

RSA Cryptography

The two numbers $pq = 55$ and $e = 3$ are the **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 the same way as was done for the Caesar cipher:

$$A = 1, B = 2, C = 3, \ldots, Z = 26.$$

RSA Cryptography

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.

RSA Cryptography

The plaintext, *M*, in a block is converted into ciphertext, *C*, according to the following formula:

$$\boxed{C = M^e \; mod \; pq.} \qquad 8.4.5$$

Note that because both *pq* and *e* are public keys, anyone who is given the keys and knows modular arithmetic can encrypt a message to send to Alice.

Example 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:

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

Example 9 – *Solution*

cont'd

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

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

Accordingly, Bob sends Alice the message: 17 14.

RSA Cryptography

To decrypt the message, Alice needs to compute the decryption key, a number *d* that is a positive inverse to *e* modulo (p – 1)(q – 1).

She obtains the plaintext *M* from the ciphertext *C* by the formula

$$\boxed{M = C^d \; mod \; pq.} \qquad 8.4.6$$

RSA Cryptography

Note that because $M + kpq \equiv M \pmod{pq}$, M must be taken to be less than pq, as in the Example 9, 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 present decryption based on knowledge of letter frequencies.

Example 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. Decrypt the following ciphertext for her: 17 14.

Solution:

Because $p = 5$ and $q = 11$, $(p - 1)(q - 1) = 40$, and so you first need to find the decryption key, which is a positive inverse for 3 modulo 40.

Use the technique of Example 7 to find a linear combination of 3 and 40 that equals 1.

Example 10 – *Solution*

cont'd

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

To find a positive inverse, compute 40 – 13. The result is 27, and

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

Example 10 – *Solution*

cont'd

Thus you need to compute $M = 17^{27}$ *mod* 55. To do so, note that 27 = 16 + 8 + 2 + 1 = $2^4 + 2^3 + 2 + 1$.

Thus you will find the residues obtained when 17 is raised to successively higher powers of 2, up to $2^4 = 16$.

$$\begin{aligned}
17 \; mod \; 55 &= 17 \; mod \; 55 &&= 17 \\
17^2 \; mod \; 55 &= 17^2 \; mod \; 55 &&= 14 \\
17^4 \; mod \; 55 &= (17^2)^2 \; mod \; 55 &&= 14^2 \; mod \; 55 = 31
\end{aligned}$$

Example 10 – *Solution*

cont'd

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

Then you will use the fact that

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

to write

$$\begin{aligned}
17^{27} \, mod \, 55 &= (17^{16} \cdot 17^8 \cdot 17^2 \cdot 17) \, mod \, 55 \\
&\equiv [(17^{16} \, mod \, 55)(17^8 \, mod \, 55)(17^2 \, mod \, 55)(17 \, mod \, 55)] \, (\text{mod } 55)
\end{aligned}$$

by Corollary 8.4.4

$$\equiv (16 \cdot 26 \cdot 14 \cdot 17) \, (\text{mod } 55)$$

Example 10 – *Solution*

cont'd

$$\equiv \quad 99008 \pmod{55}$$

$$\equiv \quad 8 \pmod{55}.$$

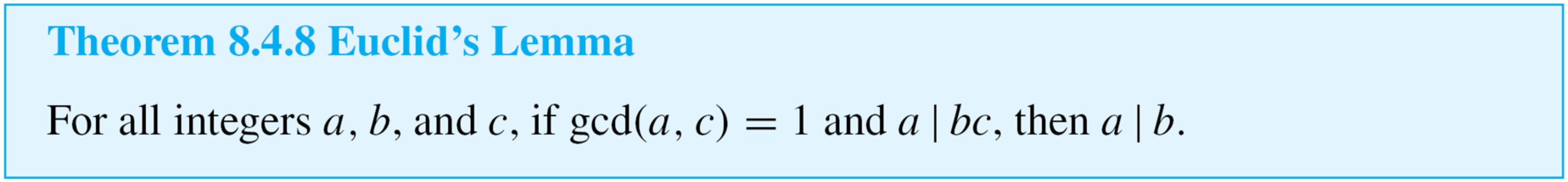
Hence 17^{27} *mod* 55 = 8, and thus the plaintext of the first part of Bob's message is 8, or 08.

In the last step, you find the letter corresponding to 08, which is *H*. Similarly 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.

Euclid’s Lemma

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

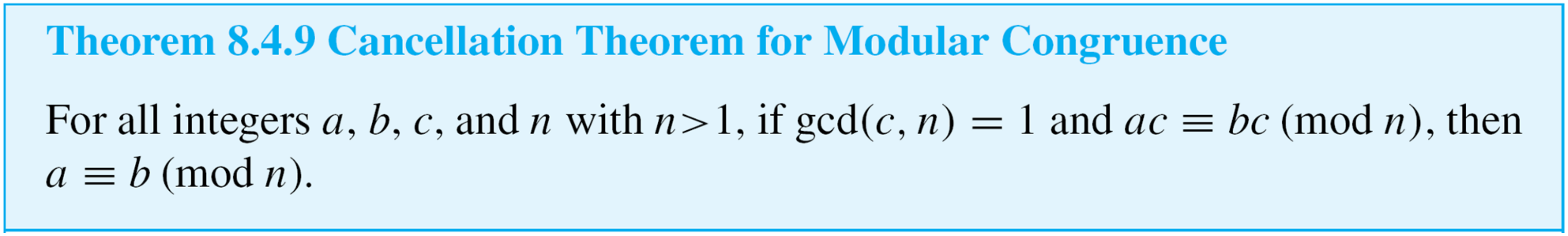
For all integers a, b, and c, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

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.

Euclid’s Lemma

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

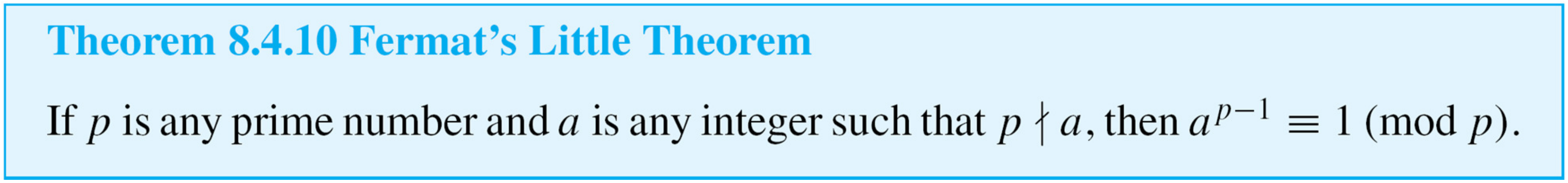
For all integers a, b, c, and n with $n > 1$, if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Fermat’s Little Theorem

Fermat’s Little Theorem

Fermat’s little theorem was given that name to distinguish it from Fermat’s last theorem, which we have discussed.

It 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 $a^{p-1} \equiv 1 \pmod{p}$.

Why Does the RSA Cipher Work?

Why Does the RSA Cipher Work?

For the RSA cryptography method, the formula

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

is supposed to produce the original plaintext message, *M*, when the encrypted message is *C*. How can we be sure that it always does so? We know that we require that $M < pq$, and we know that $C = M^e \, mod \; pq$. So, by substitution,

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

By Theorem 8.4.3(4),

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

Why Does the RSA Cipher Work?

Thus C^d *mod pq* ≡ M^{ed} (mod *pq*), and so it suffices to show that

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

We know that *d* was chosen to be a positive inverse for *e* modulo (p – 1)(q – 1), which exists because gcd(e, (p – 1)(q – 1)) = 1.

In other words,

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

or, equivalently,

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

Why Does the RSA Cipher Work?

Therefore,

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

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

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

Thus, if M is relatively prime to pq,

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

If M is not relatively prime to pq, then either $p \mid M$ or $q \mid M$. Without loss of generality, assume $p \mid M$.

Why Does the RSA Cipher Work?

It follows that $M^{ed} \equiv 0 \equiv M$ (*mod p*). Moreover, because $M < pq$, $q \mid M$, and thus, as above, $M^{ed} \equiv M$ (*mod q*). Therefore, in this case also,

$$M^{ed} \equiv M \; (mod\ p) \quad \text{and} \quad M^{ed} \equiv M \; (mod\ q).$$

By Theorem 8.4.1,

$$p \mid (M^{ed} - M) \quad \text{and} \quad q \mid (M^{ed} - M),$$

and, by definition of divisibility,

$$M^{ed} - M = pt \text{ for some integer } t.$$

Why Does the RSA Cipher Work?

By substitution,

$$q \mid pt,$$

and since *q* and *p* are distinct prime numbers, Euclid’s lemma applies to give

$$q \mid t.$$

Thus $t = qu$ for some integer *u* by definition of divisibility.

By substitution,

$$M - M^{ed} = pt = p(qu) = (pq)u,$$

where *u* is an integer, and so,

$$pq \mid (M - M^{ed})$$

by definition of divisibility.

Why Does the RSA Cipher Work?

Thus

$$M - M^{ed} \equiv 0 \pmod{pq}$$

by definition of congruence, or, equivalently,

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

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

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

and thus the RSA cipher gives the correct result.

Additional Remarks on Number Theory and Cryptography

Additional Remarks on Number Theory and Cryptography

The famous British mathematician G. H. Hardy (1877–1947) was fond of comparing the beauty of pure mathematics, especially number theory, to the beauty of art.

Indeed, the theorems in this section have many beautiful and striking consequences beyond those we have had the space to describe, and the subject of number theory extends far beyond these theorems.

Hardy also enjoyed describing pure mathematics as useless.

Additional Remarks on Number Theory and Cryptography

Hence it is ironic that there are now whole books devoted to applications of number theory to computer science, RSA cryptography being just one such application.

Furthermore, as the need for public-key cryptography has developed, techniques from other areas of mathematics, such as abstract algebra and algebraic geometry, have been used to develop additional cryptosystems.