Theorem:

If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A; that is, the union of the equivalence classes is all of A, and the intersection of any two distinct classes is empty.

Definition

Suppose R is an equivalence relation on a set A and S is an equivalence class of R. A **representative** of the class S is any element a such that $[a]=S$.

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

$$m \equiv n(mod\ d)$$

if, and only if,

$$d\ |(m\ -\ n).$$

Symbolically:

$$m \equiv n(mod\ d) \Leftrightarrow d|(m - n)$$

Properties of Congruence Modulo n

Theorem:

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

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

Definition:

- Given integers *a* and *n* with *n* > 1, **the residue of *a* modulo *n*** is *a mod n*, the non-negative remainder obtained when *a* is divided by *n*.
- The numbers 0, 1, 2, . . . , *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:

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 $a = 0, 1, 2, \ldots, n-1$,

or, equivalently,

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

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

Theorem:

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

$$a \equiv c \ (mod\ n) \text{ and } b \equiv d \ (mod\ n).$$

Then

1. $(a + b) \equiv (c + d) \ (mod\ n)$
2. $(a - b) \equiv (c - d) \ (mod\ n)$
3. $ab \equiv cd \ (mod\ n)$
4. $a^m \equiv c^m \ (mod\ n)$ for every positive integer m.

Example:

Note that

$$55 \equiv 3\ (mod\ 4) \text{ and } 26 \equiv 2\ (mod\ 4)$$

Verify the following statements.

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

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

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

d. $55^2 \equiv 3^2\ (mod\ 4)$

Corollary:

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

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n},$$

or, equivalently,

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

In particular, if *m* is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}.$$

Example:

Computing a Product Modulo n find the residue of 55·26 modulo 4.

$$55 \equiv 3\ (mod\ 4) \text{ and } 26 \equiv 2\ (mod\ 4)$$

$$55.26\ mod\ 4 = [(55\ mod\ 4)(26\ mod\ 4)]mod\ 4$$

$$= [3.2]mod\ 4$$

$$= 6\ mod\ 4 = 2$$

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

$$x^{2a} = (x^a)^2$$

for all real numbers x and a with $x \geq 0$.

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

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

- A second useful property of exponents is

$$x^{a+b} = x^a x^b$$

  for all real numbers x, a, and b with $x \geq 0$.

- For instance, because $7 = 4 + 2 + 1$, $x^7 = x^4 x^2 x^1$.
- Thus,

$$x^7 \bmod n = \{(x^4 \bmod n)(x^2 \bmod n)(x^1 \bmod n)\} \bmod n.$$

Example: Find $144^4 \ mod \ 713$.

$$144^4 \ mod \ 713 = (144^2)^2 \ mod \ 713$$

$$= (144^2 \ mod \ 713)^2 \ mod \ 713$$

$$= (20736 \ mod \ 713)^2 \ mod \ 713$$

$$= \ 59^2 \ mod \ 713$$

$$= 3481 \ mod \ 713$$

$$= \ 629$$

Example: Find $12^{43}\ mod\ 713$.

First write the exponent as a sum of powers of 2:

$$43 = 2^5 + 2^3 + 2^1 + 1 = 32 + 8 + 2 + 1.$$

Next compute 12^{2^k} for $k = 0, 1, 2, 3, 4, and\ 5$.

$$12\ mod\ 713 = 12$$
$$12^2\ mod\ 713 = 144$$
$$12^{2^2}\ mod\ 713 = 12^4\ mod\ 713 = 144^2 mod\ 713 = 59$$
$$12^{2^3}\ mod\ 713 = 12^8\ mod\ 713 = 59^2\ mod\ 713 = \ 629$$
$$12^{2^4}\ mod\ 713 = 12^{16}\ mod\ 713 = 629^2\ mod\ 713 = \ 639$$
$$12^{2^5}\ mod\ 713 = 12^{32}\ mod\ 713 = \ 639^2\ mod\ 713 = \ 485$$
$$12^{43} = 12^{32+8+2+1} = 12^{32}.12^8.12^2.12^1.$$

Thus, by the previous corollary,

$$12^{43}\ \ mod\ 713$$
$$= \ \{(12^{32}\ mod\ 713).(12^8\ mod\ 713).(12^2\ mod\ 713).(12\ mod\ 713)\}\ mod\ 713.$$

By substitution,

$$12^{43}\ mod\ 713 = (485.629.144.12) mod\ 713$$
$$= 527152320\ mod\ 713$$
$$= 48.$$

Extending the Euclidean Algorithm

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

$$as + bt = d.$$

Extending the Euclidean Algorithm

Theorem: 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:$\gcd(330,156) = 6$ then show that $6 = 9 \cdot 330 + (-19) \cdot 156$

$330 = 156.2 + 18$

$156 = 18.8 + 12$

$18 = 12.1 + 6$

$12 = 6.2 + 0$

$\gcd(330,156) = 6$

Example:$\gcd(330,156) = 6$ then show that $6 = 9 \cdot 330 + (-19) \cdot 156$

$330 = 156.2 + 18$

$156 = 18.8 + 12$

$18 = 12.1 + 6$

$12 = 6.2 + 0$

$\gcd(330,156) = 6$

$6 = 18 - 12.1$

$= 18 - (156 - 18.8).1$

$= 9.18 - 156$

$= 9(330 - 156.2) - 156$

$= 9.330 + (-19).156$

Finding an Inverse Modulo n

Given any integer *a* and any positive integer *n*, if there exists an integer *s* such that

$$as \equiv 1 \ (mod\ n),$$

then *s* is called **an inverse for *a* modulo *n***.

Example: Find the inverse of 2 modulo 5.

Observe that

$$2.3 = 6$$

And

$$2.3 = 6 \equiv 1 \ (mod \ 5)$$

Therefore,

3 is the inverse of 2 modulo 5.

Note:

- The method shown above cannot always be used to solve congruences because not every integer has an inverse modulo *n*. For instance, observe that

$$2.1 \equiv 2 \ (mod\ 4)$$
$$2.2 \equiv 0 \ (mod\ 4)$$
$$2.3 \equiv 2 \ (mod\ 4).$$

- By Theorem 8.4.3, these calculations suffice to show 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.

Relatively Prime

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

If a and b are relatively prime integers, then there exist integers *s* and *t* such that

$$as + bt = 1.$$

Proof:

Suppose a and n are integers and $\gcd(a, n) = 1$. By Corollary 8.4.6, there exist integers *s* and *t* such that

$$as + nt = 1.$$

Subtracting *nt* from both sides gives that

$$as = 1 - nt = 1 + (-t)n.$$

Thus, by definition of congruence modulo *n*,

$$as \equiv 1 \ (mod\ n).$$

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

To show that relatively prime,

We need to show gcd(660,43)=1

660=43(15)+15

43=15(2)+13

15=13(1)+2

13=2(6)+1

2=1(2)+0

gcd(660,43)=gcd(1,0)=1

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

To show that relatively prime,

We need to show gcd(660,43)=1

660=43(15)+15

43=15(2)+13

15=13(1)+2

13=2(6)+1

2=1(2)+0

gcd(660,43)=gcd(1,0)=1

But

1=13-2(6)

=13-(15-13)(6)

=13(1+6)-15(6)

=(43-15(2))(7)-15(6)

=43(7)-15(14+6)

=43(7)-(660-43(15))(20)

=43(7)-660(20)+43(300)

=43(307)-660(20)

Existence of Inverses Modulo *n*

For all integers a and n, if $\gcd(a, n) = 1$, then there exists an integer *s* such that

$$as \equiv 1 \ (mod\ n),$$

and so s is an inverse for a modulo n.

Example:

Find an inverse for 43 modulo 660. That is, find an integer *s* such that $43s \equiv 1(mod\ 660)$.

Since,

$$43(307) - 660(20) = 1$$
$$43(307) = 1 + 660(20)$$

That is

$$43(307) \equiv 1\ (mod\ 660).$$

This means 307 is an inverse of 43.

Example:

Find a positive inverse for 3 modulo 40. That is, find a positive integer *s* such that $3s \equiv 1 \ (mod\ 40)$.

Since

$$40 = 3(13) + 1$$

We get

$$3(-13) = 1 + 40(-1)$$

Therefore, the inverse of 3 modulo 40 is -13. But are required to find a positive inverse, so

$$-13 \equiv -13 + 40 \ (mod\ 40)$$

Or

$$-13 \equiv 27 \ (mod\ 40)$$

So a positive inverse of 3 modulo 40 is 27.

RSA Cryptography

- 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.

Example:

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, $(p-1)(q-1) = 4.10 = 40$, 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, . . . , 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:

$$C \equiv M^e \ (mod\ pq).$$

Example:

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

Answer

Bob sends Alice the message: 17 14.

Decryption Key

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

$$M \equiv C^d \ (mod\ pq),$$

where the number pair (pq, d) is Alice's **private key**

Example:

Compute Alice's private key (*pq*, *d*) and use the formula $M \equiv C^d \ (mod\ pq)$, to decrypt the following ciphertext for her: 17 14.

Euclid's Lemma

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