

Number Theory and Cryptography


4.1	Divisibility and Modular Arithmetic	251
<hr/>		
4.3	Primes and Greatest Common Divisors	271
4.4	Solving Congruences	290
4.5	Applications of Congruences	303
4.6	Cryptography	310

4.1 Divisibility and Modular Arithmetic

Definition 1

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$ (or equivalently, if $\frac{b}{a}$ is an integer). When a divides b we say that a is a *factor* or *divisor* of b , and that b is a *multiple* of a . The notation $a \mid b$ denotes that a divides b . We write $a \nmid b$ when a does not divide b .

EXAMPLE 1 Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution: We see that $3 \nmid 7$, because $7/3$ is not an integer. On the other hand, $3 \mid 12$ because $12/3 = 4$. 

THEOREM 1

Let a , b , and c be integers, where $a \neq 0$. Then

- (i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- (ii) if $a \mid b$, then $a \mid bc$ for all integers c ;
- (iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

4.1.3 The Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder, as the division algorithm shows.

THEOREM 2 THE DIVISION ALGORITHM Let a be an integer and d a positive integer. Then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$.

Definition 2 In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. This notation is used to express the quotient and remainder:


$$q = a \text{ div } d, \quad r = a \text{ mod } d.$$

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

EXAMPLE 3 What are the quotient and remainder when 101 is divided by 11?

Solution: We have

$$101 = 11 \cdot 9 + 2.$$

Hence, the quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \text{ mod } 11$. 

EXAMPLE 4 What are the quotient and remainder when -11 is divided by 3 ?


Solution: We have

$$-11 = 3(-4) + 1.$$

Hence, the quotient when -11 is divided by 3 is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \text{ mod } 3$.

Note that the remainder cannot be negative. Consequently, the remainder is *not* -2 , even though

$$-11 = 3(-3) - 2,$$

because $r = -2$ does not satisfy $0 \leq r < 3$. 

Remark: A programming language may have one, or possibly two, operators for modular arithmetic, denoted by `mod` (in BASIC, Maple, Mathematica, EXCEL, and SQL), `%` (in C, C++, Java, and Python), `rem` (in Ada and Lisp), or something else. Be careful when using them, because for $a < 0$, some of these operators return $a - m[a/m]$ instead of $a \text{ mod } m = a - m[a/m]$ (as shown in Exercise 24). Also, unlike $a \text{ mod } m$, some of these operators are defined when $m < 0$, and even when $m = 0$.

4.1.4 Modular Arithmetic

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. $a \bmod n = b \bmod n$

THEOREM 5

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

EXAMPLE 6 Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

and that

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}.$$

Evaluating Congruences

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

- a. $12 \equiv 7 \pmod{5}$ b. $6 \equiv -8 \pmod{4}$ c. $3 \equiv 3 \pmod{7}$

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. $55^2 \equiv 3^2 \pmod{4}$

Modular Exponentiation

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

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

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

EXAMPLE 7 Find the value of $(19^3 \bmod 31)^4 \bmod 23$.

$$(19^3 \bmod 31)^4 \bmod 23 = 2.$$

Home work



Computing $a^k \bmod n$ When k Is a Power of 2

Find $144^4 \bmod 713$.

Solution

$$\begin{aligned} 144^4 \bmod 713 &= (144^2)^2 \bmod 713 \\ &= (144^2 \bmod 713)^2 \bmod 713 \\ &= (20736 \bmod 713)^2 \bmod 713 \\ &= 59^2 \bmod 713 \\ &= 3481 \bmod 713 \\ &= 629 \end{aligned}$$

$$(19^3 \bmod 31)^4 \bmod 23,$$

$$19^3 \bmod 31 = 6859 \bmod 31 = 8.$$

$$8^4 = 4096. \text{ Because } 4096 = 178 \cdot 23 + 2,$$

$$4096 \bmod 23 = 2.$$

$$\text{Hence, } (19^3 \bmod 31)^4 \bmod 23 = 2.$$

Computing $a^k \bmod n$ When k Is Not a Power of 2

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

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

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

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

$$12 \bmod 713 = 12$$

$$12^2 \bmod 713 = 144$$

$$12^4 \bmod 713 = 144^2 \bmod 713 = 59$$

$$12^8 \bmod 713 = 59^2 \bmod 713 = 629$$

$$12^{16} \bmod 713 = 629^2 \bmod 713 = 639$$

$$12^{32} \bmod 713 = 639^2 \bmod 713 = 485$$

$$12^{43} = 12^{32+8+2+1} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12^1.$$

$$12^{43} \bmod 713$$

$$= \{(12^{32} \bmod 713) \cdot (12^8 \bmod 713) \cdot (12^2 \bmod 713) \cdot (12 \bmod 713)\} \bmod 713.$$

By substitution,

$$\begin{aligned} 12^{43} \bmod 713 &= (485 \cdot 629 \cdot 144 \cdot 12) \bmod 713 \\ &= 527152320 \bmod 713 \\ &= 48. \end{aligned}$$

Computing the **mod** m Function of Products and Sums

Let m be a positive integer and let a and b be integers. Then

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

4.1.5 Arithmetic Modulo m

We can define arithmetic operations on \mathbf{Z}_m , the set of nonnegative integers less than m , that is, the set $\{0, 1, \dots, m - 1\}$. In particular, we define addition of these integers, denoted by $+_m$ by

$$a +_m b = (a + b) \bmod m,$$

where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, denoted by \cdot_m by

$$a \cdot_m b = (a \cdot b) \bmod m,$$

The operations $+_m$ and \cdot_m are called addition and multiplication modulo m

EXAMPLE 8 Use the definition of addition and multiplication in \mathbf{Z}_m to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution:

$$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5,$$

and

$$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8.$$

Hence, $7 +_{11} 9 = 5$ and $7 \cdot_{11} 9 = 8$.

Closure If a and b belong to \mathbf{Z}_m , then $a +_m b$ and $a \cdot_m b$ belong to \mathbf{Z}_m .

Associativity If a , b , and c belong to \mathbf{Z}_m , then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

Commutativity If a and b belong to \mathbf{Z}_m , then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo m , respectively. That is, if a belongs to \mathbf{Z}_m , then $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$.

Additive inverses If $a \neq 0$ belongs to \mathbf{Z}_m , then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is, $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

Distributivity If a , b , and c belong to \mathbf{Z}_m , then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Properties

4.5 Applications of Congruences

- Hashing Functions
- Pseudorandom Numbers
- Check Digits

4.5.1 Hashing Functions

Definition: A *hashing function* h assigns memory location $h(k)$ to the record that has k as its key.

- A common hashing function is $h(k) = k \bmod m$, where m is the number of memory locations.
- Because this hashing function is onto, all memory locations are possible.

Example: Let $h(k) = k \bmod 111$. This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

$$h(064212848) = 064212848 \bmod 111 = 14$$

$$h(037149212) = 037149212 \bmod 111 = 65$$

$$h(107405723) = 107405723 \bmod 111 = 14, \text{ but since location 14 is already occupied, the record is assigned to the next available position, which is 15.}$$

the record is assigned to the next available position, which is 15.

- The hashing function is not one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a *collision* occurs. Here a collision has been resolved by assigning the record to the first free location.
- For collision resolution, we can use a *linear probing function*:
$$h(k,i) = (h(k) + i) \bmod m, \text{ where } i \text{ runs from } 0 \text{ to } m - 1.$$
- There are many other methods of handling with collisions. You may cover these in a later CS course.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.

The input to the hash function is of arbitrary length but output is always of fixed length.

4.5.2 Pseudorandom Numbers

Pseudorandom Numbers

- Randomly chosen numbers are needed for many purposes, including computer simulations.
- *Pseudorandom numbers* are not truly random since they are generated by systematic methods.
- The *linear congruential method* is one commonly used procedure for generating pseudorandom numbers.
- Four integers are needed: the *modulus* m , the *multiplier* a , the *increment* c , and *seed* x_0 , with $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.
- We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n , by successively using the recursively defined function

$$x_{n+1} = (ax_n + c) \bmod m.$$

- If pseudorandom numbers between 0 and 1 are needed, then the generated numbers are divided by the modulus, x_n/m .

Pseudorandom Numbers

- **Example:** Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.

Solution: Compute the terms of the sequence by successively using the congruence $x_{n+1} = (7x_n + 4) \bmod 9$, with $x_0 = 3$.

$$x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,$$

$$x_2 = 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,$$

$$x_3 = 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,$$

$$x_4 = 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,$$

$$x_5 = 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,$$

$$x_6 = 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,$$

$$x_7 = 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,$$

$$x_8 = 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,$$

$$x_9 = 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.$$

The sequence generated is 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, ...

It repeats after generating 9 terms.

4.5.3 Check Digits

- A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

Example: Retail products are identified by their *Universal Product Codes (UPCs)*. Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

- EXAMPLE 5**
- a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?
 - b. Is 041331021641 a valid UPC?

Solution:

- a. $3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 7 + 3 + 3 \cdot 4 + 3 + 3 \cdot 1 + 0 + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10}$
 $21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$
 $98 + x_{12} \equiv 0 \pmod{10}$
 $x_{12} \equiv 0 \pmod{10}$ So, the check digit is 2.
- b. $3 \cdot 0 + 4 + 3 \cdot 1 + 3 + 3 \cdot 3 + 1 + 3 \cdot 0 + 2 + 3 \cdot 1 + 6 + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10}$
 $0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + x_{12} \equiv 0 \pmod{10}$
 $44 + x_{12} \equiv 0 \pmod{10}$
Hence, 041331021641 is not a valid UPC.

Books are identified by an *International Standard Book Number* (ISBN-10), a 10 digit code. The first 9 digits identify the language, the publisher, and the book. The tenth digit is a check digit, which is determined by the following congruence

$$x_{10} \equiv \sum_{i=1}^9 ix_i \pmod{11}.$$

The validity of an ISBN-10 number can be evaluated with the equivalent $\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}.$

EXAMPLE 6

- Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?
- Is 084930149X a valid ISBN10?

Solution:

$$\text{a. } X_{10} \equiv 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 8 \pmod{11}.$$

$$X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}.$$

$$X_{10} \equiv 189 \equiv 2 \pmod{11}. \text{ Hence, } X_{10} = 2.$$

$$\begin{aligned} \text{b. } 1 \cdot 0 + 2 \cdot 8 + 3 \cdot 4 + 4 \cdot 9 + 5 \cdot 3 + 6 \cdot 0 + 7 \cdot 1 + 8 \cdot 4 + 9 \cdot 9 + 10 \cdot 10 &= \\ 0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 &= 299 \equiv 2 \not\equiv 0 \pmod{11} \end{aligned}$$

Hence, 084930149X is not a valid ISBN-10.

X is used
for the digit
10.

Primes and Greatest Common Divisors

Section 4.3

Section Summary

- Prime Numbers and their Properties
- Greatest Common Divisors and Least Common Multiples
- The Euclidian Algorithm
- GCDs as Linear Combinations

Primes

Definition: A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p . A positive integer that is greater than 1 and is not prime is called *composite*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.

Examples:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

The Sieve of Eratosthenes

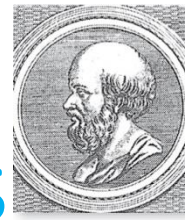
TABLE 1 The Sieve of Eratosthenes.

<i>Integers divisible by 2 other than 2 receive an underline.</i>										<i>Integers divisible by 3 other than 3 receive an underline.</i>									
1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	9	<u>10</u>	1	2	3	<u>4</u>	5	<u>6</u>	7	8	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	15	<u>16</u>	17	<u>18</u>	19	<u>20</u>	11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	27	<u>28</u>	29	<u>30</u>	21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>
31	<u>32</u>	33	<u>34</u>	35	<u>36</u>	37	<u>38</u>	39	<u>40</u>	31	<u>32</u>	<u>33</u>	<u>34</u>	35	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u>42</u>	43	<u>44</u>	45	<u>46</u>	47	<u>48</u>	49	<u>50</u>	41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>
51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	57	<u>58</u>	59	<u>60</u>	51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
61	<u>62</u>	63	<u>64</u>	65	<u>66</u>	67	<u>68</u>	69	<u>70</u>	61	<u>62</u>	<u>63</u>	<u>64</u>	65	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u>72</u>	73	<u>74</u>	75	<u>76</u>	77	<u>78</u>	79	<u>80</u>	71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>
81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	87	<u>88</u>	89	<u>90</u>	81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
91	<u>92</u>	93	<u>94</u>	95	<u>96</u>	97	<u>98</u>	99	<u>100</u>	91	<u>92</u>	<u>93</u>	<u>94</u>	95	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>
<i>Integers divisible by 5 other than 5 receive an underline.</i>										<i>Integers divisible by 7 other than 7 receive an underline; integers in color are prime.</i>									
1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	<u>9</u>	<u>10</u>	1	2	3	4	5	6	7	8	9	<u>10</u>
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>	11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
21	<u>22</u>	23	<u>24</u>	<u>25</u>	<u>26</u>	27	<u>28</u>	29	<u>30</u>	21	<u>22</u>	23	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>
31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>	31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>	41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>
51	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>	51	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>	61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>	71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	<u>77</u>	<u>78</u>	79	<u>80</u>
81	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	87	<u>88</u>	89	<u>90</u>	81	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
91	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>	91	<u>92</u>	93	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>

If an integer n is a composite integer, then it has a prime divisor less than or equal to \sqrt{n} .

To see this, note that if $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $i \leq \sqrt{n}$ and see if n is divisible by i .



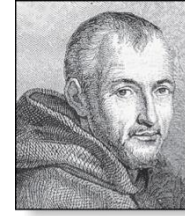
Eratosthenes
(276-194 B.C.)

The Sieve of Eratosthenes

- The *Sieve of Eratosthenes* can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.
 - a. Delete all the integers, other than 2, divisible by 2.
 - b. Delete all the integers, other than 3, divisible by 3.
 - c. Next, delete all the integers, other than 5, divisible by 5.
 - d. Next, delete all the integers, other than 7, divisible by 7.
 - e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

Mersenne Primes



Marin Mersenne
(1588-1648)

Definition: Prime numbers of the form $2^p - 1$, where p is prime, are called *Mersenne primes*.

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, and $2^7 - 1 = 127$ are Mersenne primes.
- $2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.
- There is an efficient test for determining if $2^p - 1$ is prime.
- The largest known prime numbers are Mersenne primes.
- As of mid 2011, 47 Mersenne primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.
- The *Great Internet Mersenne Prime Search (GIMPS)* is a distributed computing project to search for new Mersenne Primes.

<http://www.mersenne.org/>

Greatest Common Divisor

Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b . The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

One can find greatest common divisors of small numbers by inspection.

Example: What is the greatest common divisor of 24 and 36?

Solution: $\gcd(24, 36) = 12$

Example: What is the greatest common divisor of 17 and 22?

Solution: $\gcd(17, 22) = 1$

Greatest Common Divisor

Definition: The integers a and b are *relatively prime* if their greatest common divisor is 1.

Example: 17 and 22

Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution: Because $\gcd(10,17) = 1$, $\gcd(10,21) = 1$, and $\gcd(17,21) = 1$, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because $\gcd(10,24) = 2$,
10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

- This formula is valid since the integer on the right (of the equals sign) divides both a and b . No larger integer can divide both a and b .

Example: $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$

$$\gcd(120, 500) = 2^{\min(3, 2)} \cdot 3^{\min(1, 0)} \cdot 5^{\min(1, 3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

- Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

Definition: The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b . It is denoted by $\text{lcm}(a,b)$.

- The least common multiple can also be computed from the prime factorizations.

$$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

This number is divided by both a and b and no smaller number is divided by a and b .

Example: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$

- The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

$$ab = \text{gcd}(a,b) \cdot \text{lcm}(a,b)$$



Euclid

(325 B.C.E. – 265 B.C.E.)

Euclidean Algorithm

- The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that $\gcd(a,b)$ is equal to $\gcd(a,c)$ when $a > b$ and c is the remainder when a is divided by b .

Example: Find $\gcd(91, 287)$:

- $287 = 91 \cdot 3 + 14$ Divide 287 by 91
- $91 = 14 \cdot 6 + 7$ Divide 91 by 14
- $14 = 7 \cdot 2 + 0$ Divide 14 by 7

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

continued →



GCDs as Linear Combinations

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b . The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity*.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b .
 - $\gcd(6,14) = (-2) \cdot 6 + 1 \cdot 14$

Finding gcds as Linear Combinations

Example: Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show $\gcd(252, 198) = 18$

i. $252 = 1 \cdot 198 + 54$

ii. $198 = 3 \cdot 54 + 36$

iii. $54 = 1 \cdot 36 + 18$

iv. $36 = 2 \cdot 18$

- Now working backwards, from **iii** and **i** above
 - $18 = 54 - 1 \cdot 36$
 - $36 = 198 - 3 \cdot 54$
- Substituting the 2nd equation into the 1st yields:
 - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting $54 = 252 - 1 \cdot 198$ (from **i**)) yields:
 - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

Dividing Congruencies by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).
- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

Theorem 7: Let m be a positive integer and let a , b , and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.



Solving Congruencies

Section 4.4

- Linear Congruencies
- The Chinese Remainder Theorem
- Fermat's Little Theorem

Linear Congruencies

Definition: A congruence of the form

$$ax \equiv b \pmod{m},$$

where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

- The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Definition: An integer \bar{a} such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *inverse* of a modulo m .

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1 \pmod{7}$

- One method of solving linear congruencies makes use of an inverse \bar{a} , if it exists. Although we can not divide both sides of the congruence by a , we can multiply by \bar{a} to solve for x .

EXAMPLE 1 Find an inverse of 3 modulo 7 by first finding Bézout coefficients of 3 and 7.

Solution: Because $\gcd(3, 7) = 1$, Theorem 1 tells us that an inverse of 3 modulo 7 exists.

Euclidean algorithm

$$7 = 2 \cdot 3 + 1.$$

From this equation we see that

$$-2 \cdot 3 + 1 \cdot 7 = 1.$$

This shows that -2 and 1 are Bézout coefficients of 3 and 7.

We see that -2 is an inverse of 3 modulo 7.

4. By inspection (as discussed prior to Example 1), find an inverse of 2 modulo 17.

We need a number that when multiplied by 2 gives a number congruent to 1 modulo 17.

Since $18 \equiv 1 \pmod{17}$

and $2 \cdot 9 = 18$,

it follows that 9 is an inverse of 2 modulo 17.

Inverse of a modulo m

- The following theorem guarantees that an inverse of a modulo m exists whenever a and m are relatively prime. Two integers a and b are relatively prime when

$$\gcd(a,b) = 1.$$

Theorem 1: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m . (This means that there is a unique positive integer \bar{a} less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to \bar{a} modulo m .)

Finding Inverses

- The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

Example: Find an inverse of 3 modulo 7.

Solution: Because $\gcd(3,7) = 1$, by Theorem 1, an inverse of 3 modulo 7 exists.

- Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.
- From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that -2 and 1 are **Bézout coefficients** of 3 and 7.
- Hence, -2 is an inverse of 3 modulo 7.

Finding Inverses

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that $\gcd(101, 4620) = 1$.

$$4620 = 45 \cdot 101 + 75$$

$$101 = 1 \cdot 75 + 26$$

$$75 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$23 = 7 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

Since the last nonzero remainder is 1,
 $\gcd(101, 4260) = 1$

Working Backwards:

$$1 = 3 - 1 \cdot 2$$

$$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$

$$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$

$$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$$

$$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$$

$$= 26 \cdot 101 - 35 \cdot 75$$

$$1 = 26 \cdot 101 - 35 \cdot (42620 - 45 \cdot 101)$$

$$= -35 \cdot 42620 + 1601 \cdot 101$$

Bézout coefficients : -35 and 1601

1601 is an inverse of
101 modulo 42620

Finding an Inverse Modulo n

Home work

- 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)

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

so 307 is an inverse for 43 modulo 660.

Solution: b)

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

12. Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 6.

- a) $34x \equiv 77 \pmod{89}$
- b) $144x \equiv 4 \pmod{233}$

Solution:

a) We found that 55 is an inverse of 34 modulo 89,
so $x \equiv 77 \cdot 55 = 4235 \equiv 52 \pmod{89}$.

b) We found that 89 is an inverse of 144 modulo 233,
 $x \equiv 4 \cdot 89 = 356 \equiv 123 \pmod{233}$.

6. Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.

Class Activity

b) $a = 34, m = 89$

Solution:

the Euclidean algorithm computation that $\gcd(34, 89) = 1$:

$$89 = 2 \cdot 34 + 21$$

$$34 = 21 + 13$$

$$21 = 13 + 8$$

$$13 = 8 + 5$$

$$8 = 5 + 3$$

$$5 = 3 + 2$$

$$3 = 2 + 1$$

Then we reverse our steps and write 1 as the desired linear combination:

$$1 = 3 - 2$$

$$= 3 - (5 - 3) = 2 \cdot 3 - 5$$

$$= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5$$

$$= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13$$

$$= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13$$

$$= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34$$

$$= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 34 \cdot 34$$

an inverse of 34 modulo 89 is -34 ,

which can also be written as 55

The Chinese Remainder Theorem

Theorem 2: (*The Chinese Remainder Theorem*) Let m_1, m_2, \dots, m_n be pairwise relatively prime positive integers greater than one and a_1, a_2, \dots, a_n arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

.

.

.

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

(That is, there is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.)

- **Proof:** We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo m is Exercise 30.

continued →

The Chinese Remainder Theorem

To construct a solution first let $M_k = m/m_k$ for $k = 1, 2, \dots, n$ and $m = m_1 m_2 \cdots m_n$.

Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer y_k , an inverse of M_k modulo m_k , such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \pmod{m}$$

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the k th term in this sum are congruent to 0 modulo m_k .

Because $M_k y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1, 2, \dots, n$.

Hence, x is a simultaneous solution to the n congruences.

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

.

.

.

$$x \equiv a_n \pmod{m_n}$$



The Chinese Remainder Theorem

Example: Consider the 3 congruences from Sun-Tsu's problem:

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}.$$

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.
- We see that
 - 2 is an inverse of $M_1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod{3}$
 - 1 is an inverse of $M_2 = 21$ modulo 5 since $21 \equiv 1 \pmod{5}$
 - 1 is an inverse of $M_3 = 15$ modulo 7 since $15 \equiv 1 \pmod{7}$
- Hence,

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{m} \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105} \end{aligned}$$

- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

Use the Chinese Remainder Theorem to find an x such that

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

$$x \equiv 3 \pmod{7}$$

$$x \equiv 10 \pmod{11}$$

Solution. Set $N = 5 \times 7 \times 11 = 385$. Following the notation of the theorem, we have $m_1 = N/5 = 77$, $m_2 = N/7 = 55$, and $m_3 = N/11 = 35$.

We now seek a multiplicative inverse for each m_i modulo n_i . First: $m_1 \equiv 77 \equiv 2 \pmod{5}$, and hence an inverse to $m_1 \pmod{n_1}$ is $y_1 = 3$.

Second: $m_2 \equiv 55 \equiv 6 \pmod{7}$, and hence an inverse to $m_2 \pmod{n_2}$ is $y_2 = 6$.

Third: $m_3 \equiv 35 \equiv 2 \pmod{11}$, and hence an inverse to $m_3 \pmod{n_3}$ is $y_3 = 6$.

Therefore, the theorem states that a solution takes the form:

$$x = y_1 b_1 m_1 + y_2 b_2 m_2 + y_3 b_3 m_3 = 3 \times 2 \times 77 + 6 \times 3 \times 55 + 6 \times 10 \times 35 = 3552.$$

Since we may take the solution modulo $N = 385$, we can reduce this to 87, since $3552 \equiv 87 \pmod{385}$.

The Chinese Remainder Theorem

$x \equiv 4 \pmod{5}$, $x \equiv 6 \pmod{8}$, $x \equiv 8 \pmod{9}$.

- Let $m = 5 \cdot 8 \cdot 9 = 360$, $M_1 = 360/5 = 72$, $M_2 = 360/8 = 45$, $M_3 = 360/9 = 40$.
- We see that
 - 3 is an inverse of $M_1 = 72$ modulo 5
 - 5 is an inverse of $M_2 = 45$ modulo 8
 - 7 is an inverse of $M_3 = 40$ modulo 9
- Hence,

$$\begin{aligned}x &= (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \pmod{m} \\&= (4 \cdot 72 \cdot 3 + 6 \cdot 45 \cdot 5 + 8 \cdot 40 \cdot 7) \pmod{360} \\&= 4454 \pmod{360} \\&= 134\end{aligned}$$

- We have shown that 134 is the smallest positive integer that is a simultaneous solution. Check it!

Cryptography

- Classical Cryptography
- Cryptosystems
- Public Key Cryptography
- RSA Cryptosystem
- Fermat's Little theorem



Caesar Cipher

Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet (sending the last three letters to the first three letters.) For example, the letter B is replaced by E and the letter X is replaced by A. This process of making a message secret is an example of *encryption*.

Here is how the encryption process works:

- Replace each letter by an integer from \mathbf{Z}_{26} , that is an integer from 0 to 25 representing one less than its position in the alphabet.
- The encryption function is $f(p) = (p + 3) \bmod 26$. It replaces each integer p in the set $\{0, 1, 2, \dots, 25\}$ by $f(p)$ in the set $\{0, 1, 2, \dots, 25\}$.
- Replace each integer p by the letter with the position $p + 1$ in the alphabet.

Example: Encrypt the message “MEET YOU IN THE PARK” using the Caesar cipher.

Solution: 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3) \bmod 26$.

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating the numbers back to letters produces the encrypted message

“PHHW BRX LQ WKH SDUN.”

Caesar Cipher

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

- To recover the original message, use $f^{-1}(p) = (p-3) \bmod 26$. So, each letter in the coded message is shifted back three letters in the alphabet, with the first three letters sent to the last three letters. This process of recovering the original message from the encrypted message is called *decryption*.
- The Caesar cipher is one of a family of ciphers called *shift ciphers*. Letters can be shifted by an integer k , with 3 being just one possibility. The encryption function is
$$f(p) = (p + k) \bmod 26$$
and the decryption function is
$$f^{-1}(p) = (p - k) \bmod 26$$
The integer k is called a *key*.

Shift Cipher

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: Encrypt the message “STOP GLOBAL WARMING” using the shift cipher with $k = 11$.

Solution: Replace each letter with the corresponding element of \mathbf{Z}_{26} .

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.

Apply the shift $f(p) = (p + 11) \bmod 26$, yielding

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating the numbers back to letters produces the ciphertext

“DEZA RWZMLW HLCXTYR.”

Shift Cipher

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 2: Decrypt the message “LEWLYPLUJL PZ H NYLHA ALHJOLY” that was encrypted using the shift cipher with $k = 7$.

Solution: Replace each letter with the corresponding element of \mathbf{Z}_{26} .

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Shift each of the numbers by $-k = -7$ modulo 26, yielding

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.

Translating the numbers back to letters produces the decrypted message

“EXPERIENCE IS A GREAT TEACHER.”

Encrypting and Decrypting with the Caesar Cipher

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

- Use the Caesar cipher to encrypt the message HOW ARE YOU.
- Use the Caesar cipher to decrypt the message L DP ILQH.

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.

$$C = (M + 3) \bmod 26.$$

$$M = (C - 3) \bmod 26.$$

- 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.

Number Theory in Cryptography

Terminology: Two parties **Alice** and **Bob** want to communicate securely s.t. a third party **Eve** who intercepts messages cannot learn the content of the messages.

Symmetric Cryptosystems: Alice and Bob share a secret. Only they know a secret key K that is used to encrypt and decrypt messages. Given a message M , Alice encodes it (possibly with padding) into m , and then sends the ciphertext $encrypt(m, K)$ to Bob. Then Bob uses K to decrypt it and obtains $decrypt(encrypt(m, K), K) = m$.

Example: AES.

Public Key Cryptosystems: Alice and Bob do a-priori **not** share a secret. How can they establish a shared secret when others are listening to their messages?

Idea: Have a two-part key, i.e., a key pair. A public key that is used to encrypt messages, and a secret key to decrypt them. Alice uses Bob's public key to encrypt a message (everyone can do that). Only Bob can decrypt the message with his secret key.

Description of RSA: Key generation

- Choose two distinct prime numbers p and q . Numbers p and q should be chosen at random, and be of similar bit-length. Prime integers can be efficiently found using a primality test.
- Let $n = pq$ and $k = (p - 1)(q - 1)$. (In particular, $k = |Z_n^*|$).
- Choose an integer e such that $1 < e < k$ and $\gcd(e, k) = 1$; i.e., e and k are coprime.
 e (for encryption) is released as the public key exponent.
(e must not be very small.)
- Let d be the multiplicative inverse of e modulo k , i.e., $de \equiv 1 \pmod{k}$. (Computed using the extended Euclidean algorithm.) d (for decryption) is the private key and kept secret.

The public key is (n, e) and the private key is (n, d) .

RSA: Encryption and Decryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret.

Encryption: Bob then wishes to send message M to Alice. He first turns M into an integer m , such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \pmod{n}$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Decryption: Alice can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \pmod{n}$$

Given m , she can recover the original message M by reversing the padding scheme.

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, 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

$$M = C^d \bmod pq.$$

Using RSA

Given $\text{pubKey} = \langle e, n \rangle$ and $\text{privKey} = \langle d, n \rangle$

If Message = m

Then:

encryption: $c = m^e \bmod n, m < n$

decryption: $m = c^d \bmod n$

signature: $s = md \bmod n, m < n$

verification: $m = se \bmod n$

Example of RSA (1)

Choose $p = 7$ and $q = 17$.

Compute $n = p \cdot q = 119$.

Compute $f(n) = (p-1)(q-1) = 96$.

Select $e = 5$, (a relatively prime to $f(n)$.)

Compute $d = \underline{77}$ such that $e \cdot d = 1 \pmod{f(n)}$.

- Public key: $\langle 5, 119 \rangle$
- Private key: $\langle 77, 119 \rangle$
- Message = 19
- Encryption: $19^5 \pmod{119} = 66$
- Decryption: $66^{77} \pmod{119} = 19$

Example of RSA (2)

$p = 7, q = 11, n = 77$

Alice chooses $e = 17$, making $d = 53$

Bob wants to send Alice secret message

HELLO (07 04 11 11 14)

- $07^{17} \bmod 77 = 28$; $04^{17} \bmod 77 = 16$
- $11^{17} \bmod 77 = 44$; – $11^{17} \bmod 77 = 44$
- $14^{17} \bmod 77 = 42$
- Bob sends **28 16 44 44 42**

Example of RSA (3)

Alice receives **28 16 44 44 42**

Alice uses private key, $d = 53$, to decrypt message:

– $28^{53} \bmod 77 = 07$; $16^{53} \bmod 77 = 04$

– $44^{53} \bmod 77 = 11$; $44^{53} \bmod 77 = 11$

– $42^{53} \bmod 77 = 14$

- Alice translates **07 04 11 11 14** to ***HELLO***

No one else could read it, as only Alice knows her private key (needed for decryption)

Fermat's Little Theorem

Pierre de Fermat
(1601-1665)



Theorem 3: (*Fermat's Little Theorem*) If p is prime and a is an integer not divisible by p , then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$

(*proof outlined in Exercise 19*)

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

Example: Find $7^{222} \bmod 11$.

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k . Therefore,

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

Hence, $7^{222} \bmod 11 = 5$.