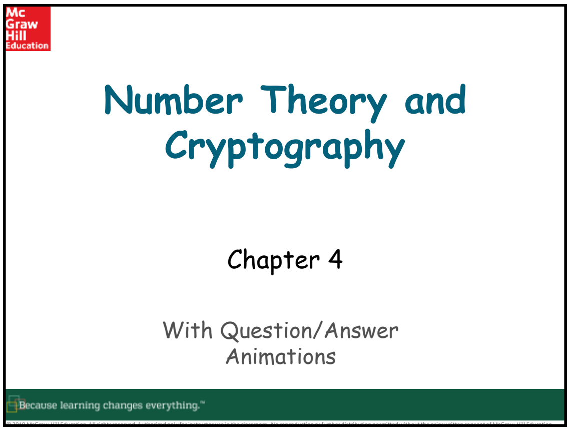


Mc Graw Hill Education

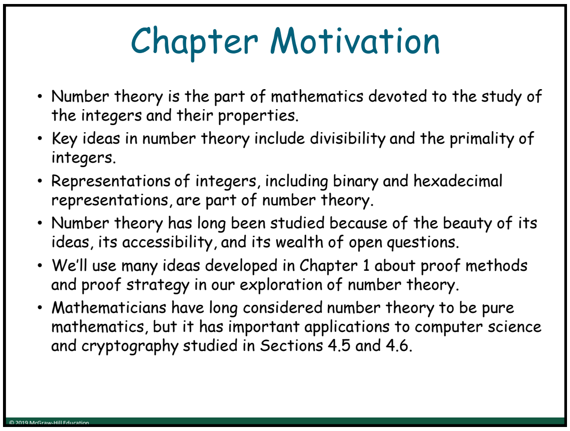
Number Theory and Cryptography

Chapter 4

With Question/Answer Animations

Because learning changes everything.™

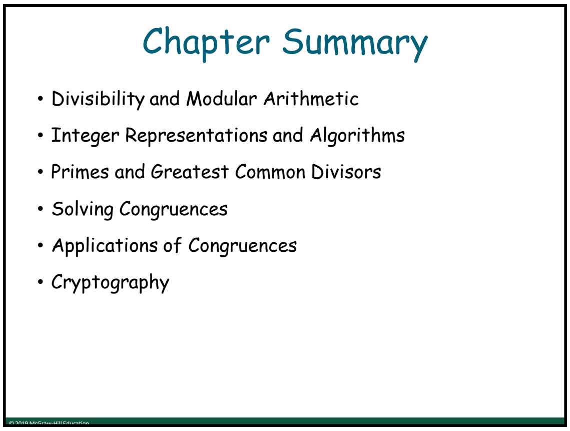
1



Chapter Motivation

- Number theory is the part of mathematics devoted to the study of the integers and their properties.
- Key ideas in number theory include divisibility and the primality of integers.
- Representations of integers, including binary and hexadecimal representations, are part of number theory.
- Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.
- We'll use many ideas developed in Chapter 1 about proof methods and proof strategy in our exploration of number theory.
- Mathematicians have long considered number theory to be pure mathematics, but it has important applications to computer science and cryptography studied in Sections 4.5 and 4.6.

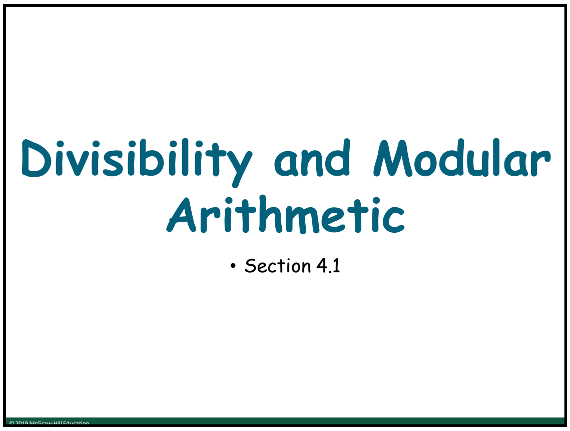
2



Chapter Summary

- Divisibility and Modular Arithmetic
- Integer Representations and Algorithms
- Primes and Greatest Common Divisors
- Solving Congruences
- Applications of Congruences
- Cryptography

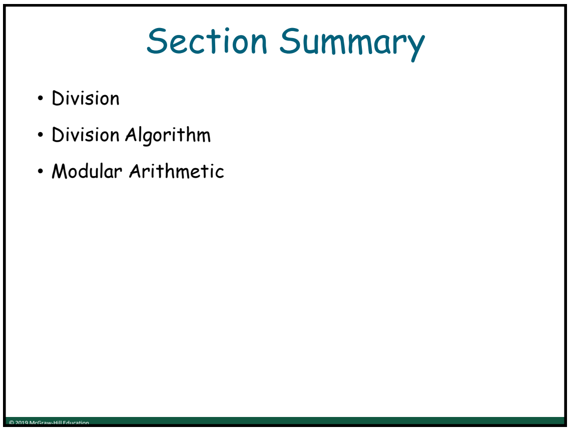
3



Divisibility and Modular Arithmetic

- Section 4.1

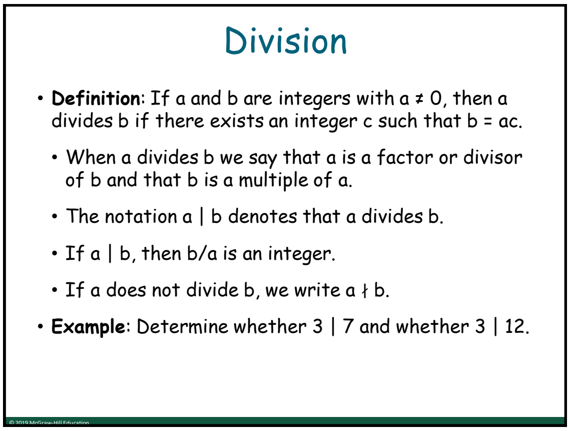
4



Section Summary

- Division
- Division Algorithm
- Modular Arithmetic

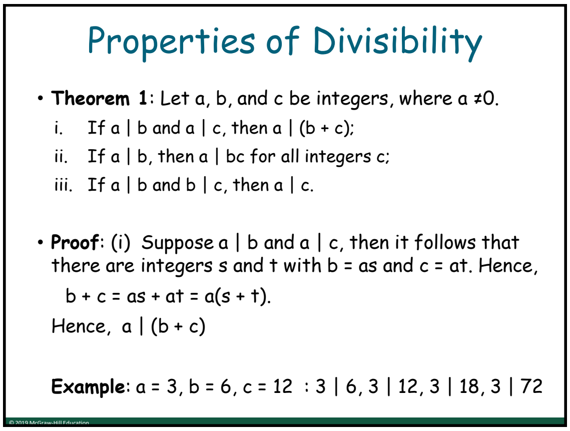
5



Division

- **Definition**: If a and b are integers with a ≠ 0, then a divides b if there exists an integer c such that b = ac.
  - 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 | b denotes that a divides b.
  - If a | b, then b/a is an integer.
  - If a does not divide b, we write a ∤ b.
- **Example**: Determine whether 3 | 7 and whether 3 | 12.

6



Properties of Divisibility

- **Theorem 1**: Let a, b, and c be integers, where $a \neq 0$.
  - 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 $a \mid c$.
- **Proof**: (i) Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

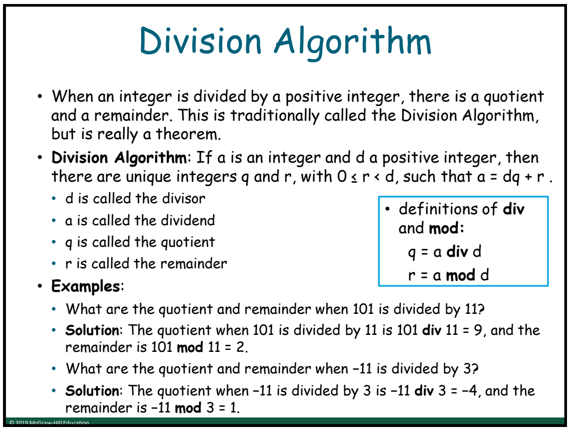
  $b + c = as + at = a(s + t)$.

  Hence, $a \mid (b + c)$

  Example: $a = 3, b = 6, c = 12$: $3 \mid 6, 3 \mid 12, 3 \mid 18, 3 \mid 72$

© 2019 McGraw-Hill Education

7



Division Algorithm

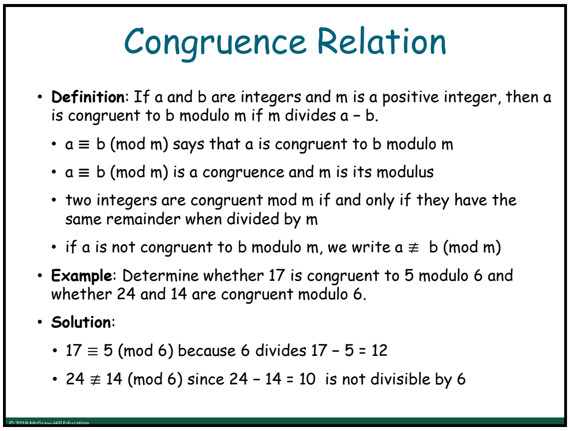
- When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the Division Algorithm, but is really a theorem.
- **Division Algorithm**: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.
  - d is called the divisor
  - a is called the dividend
  - q is called the quotient
  - r is called the remainder

- definitions of **div** and **mod:**
  - q = a **div** d
  - r = a **mod** d

- **Examples**:
  - What are the quotient and remainder when 101 is divided by 11?
  - **Solution**: The quotient when 101 is divided by 11 is 101 **div** 11 = 9, and the remainder is 101 **mod** 11 = 2.
  - What are the quotient and remainder when −11 is divided by 3?
  - **Solution**: The quotient when −11 is divided by 3 is −11 **div** 3 = −4, and the remainder is −11 **mod** 3 = 1.

© 2019 McGraw-Hill Education

8

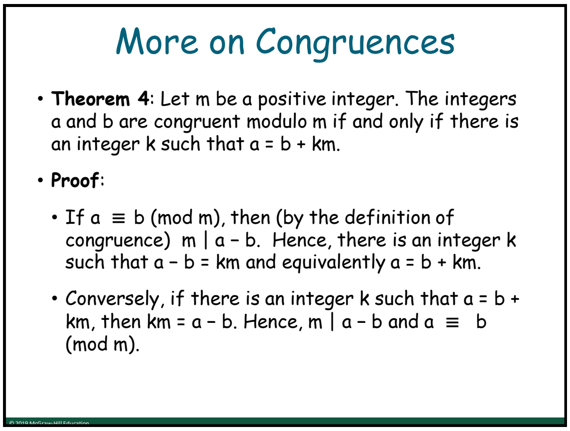


Congruence Relation

- **Definition**: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$.
  - $a \equiv b \pmod{m}$ says that a is congruent to b modulo m
  - $a \equiv b \pmod{m}$ is a congruence and m is its modulus
  - two integers are congruent mod m if and only if they have the same remainder when divided by m
  - if a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$
- **Example**: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.
- **Solution**:
  - $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$
  - $24 \not\equiv 14 \pmod{6}$ since $24 - 14 = 10$ is not divisible by 6

© 2019 McGraw-Hill Education

9

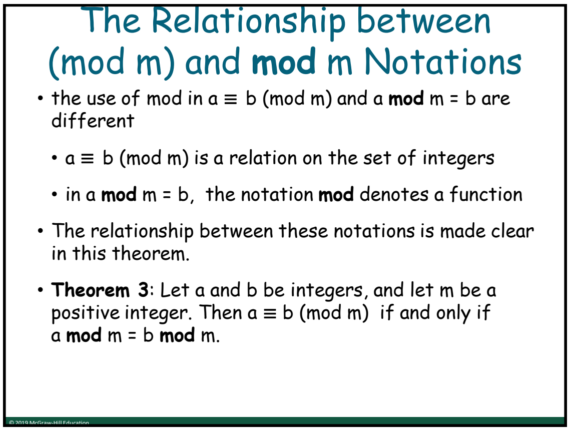


More on Congruences

- **Theorem 4**: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.
- **Proof**:
  - If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
  - Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$.

© 2019 McGraw-Hill Education

10

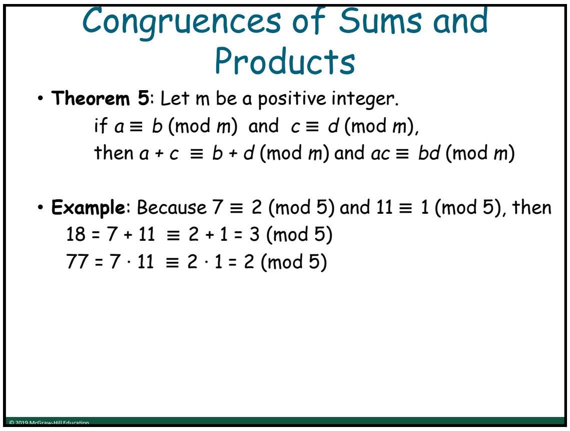


The Relationship between (mod m) and **mod** m Notations

- the use of mod in $a \equiv b$ (mod m) and a **mod** m = b are different
  - $a \equiv b \pmod{m}$ is a relation on the set of integers
  - in a **mod** m = b, the notation **mod** denotes a function
- The relationship between these notations is made clear in this theorem.
- **Theorem 3**: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if a **mod** m = b **mod** m.

© 2019 McGraw-Hill Education

11



Congruences of Sums and Products

- **Theorem 5**: Let m be a positive integer.

  if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,

  then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$
- **Example**: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, then

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

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

© 2019 McGraw-Hill Education

12

Algebraic Manipulation of Congruences

- multiplying both sides of a valid congruence by an integer preserves validity

  if $a \equiv b \pmod{m}$, then $c \cdot a \equiv c \cdot b \pmod{m}$
- adding an integer to both sides of a valid congruence preserves validity

  if $a \equiv b \pmod{m}$, then $c + a \equiv c + b \pmod{m}$
- dividing a congruence by an integer does not always produce a valid congruence
- **Example**: $14 \equiv 8 \pmod{6}$, but dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

13

Integer Representations and Algorithms

- Section 4.2

14

Section Summary

- Integer Representations
  - Base b Expansions
  - Binary Expansions
  - Octal Expansions
  - Hexadecimal Expansions
- Base Conversion Algorithm
- Algorithms for Integer Operations

15

Representations of Integers

- in the modern world, we use decimal, or base 10, notation to represent integers.

  $965 = 9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$
- we can represent numbers using any base b, where b is a positive integer greater than 1
- the bases b = 2 (binary), b = 8 (octal), and b = 16 (hexadecimal) are important for computing and communications
- the ancient Mayans used base 20 and the ancient Babylonians used base 60!

16

Base b Representations

- we can use positive integer b greater than 1 as a base, as in this theorem:
- **Theorem 1**: Let b be a positive integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the base b expansion form:

  $$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$
  - where k is a nonnegative integer, $a_0, a_1, \ldots a_k$ are nonnegative integers less than b, and $a_k \neq 0$
  - the a_j, $j = 0, \ldots, k$ are called the base-b digits of the representation
  - we usually omit the subscript 10 for base 10 expansions

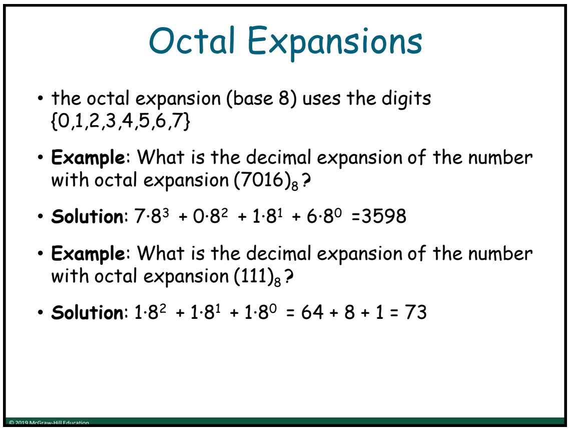
17

Binary Expansions

- most computers represent integers and perform arithmetic with binary (base 2) integers
  - in these expansions, the only digits used are 0 and 1
- **Example**: What is the decimal expansion of the integer that has $(1\,0101\,1111)_2$ as its binary expansion?
- **Solution**:

  $(1\,0101\,1111)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351$
- **Example**: What is the decimal expansion of the integer that has $(11011)_2$ as its binary expansion?
- **Solution**: $(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 27$

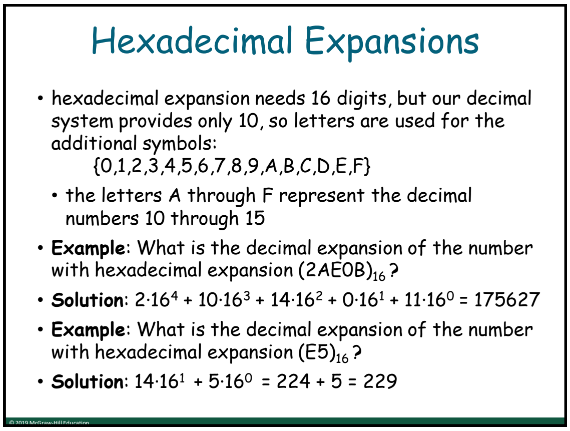
18



Octal Expansions

- the octal expansion (base 8) uses the digits {0,1,2,3,4,5,6,7}
- **Example**: What is the decimal expansion of the number with octal expansion $(7016)_8$?
- **Solution**: $7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$
- **Example**: What is the decimal expansion of the number with octal expansion $(111)_8$?
- **Solution**: $1 \cdot 8^2 + 1 \cdot 8^1 + 1 \cdot 8^0 = 64 + 8 + 1 = 73$

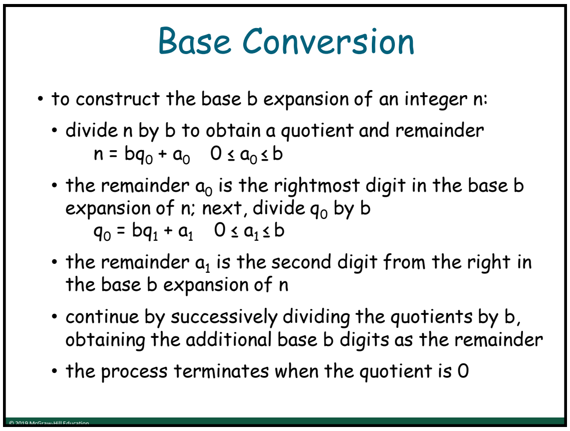
19



Hexadecimal Expansions

- hexadecimal expansion needs 16 digits, but our decimal system provides only 10, so letters are used for the additional symbols:
  {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}
  - the letters A through F represent the decimal numbers 10 through 15
- **Example**: What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?
- **Solution**: $2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627$
- **Example**: What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?
- **Solution**: $14 \cdot 16^1 + 5 \cdot 16^0 = 224 + 5 = 229$

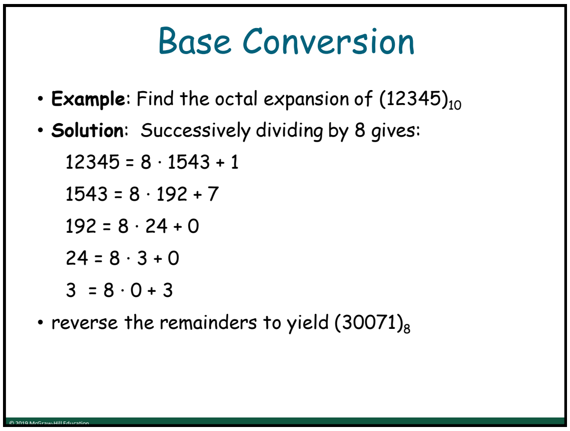
20



Base Conversion

- to construct the base b expansion of an integer n:
  - divide n by b to obtain a quotient and remainder
    $n = bq_0 + a_0 \quad 0 \le a_0 \le b$
  - the remainder a_0 is the rightmost digit in the base b expansion of n; next, divide q_0 by b
    $q_0 = bq_1 + a_1 \quad 0 \le a_1 \le b$
  - the remainder a_1 is the second digit from the right in the base b expansion of n
  - continue by successively dividing the quotients by b, obtaining the additional base b digits as the remainder
  - the process terminates when the quotient is 0

21



Base Conversion

- **Example**: Find the octal expansion of $(12345)_{10}$
- **Solution**: Successively dividing by 8 gives:

  $12345 = 8 \cdot 1543 + 1$

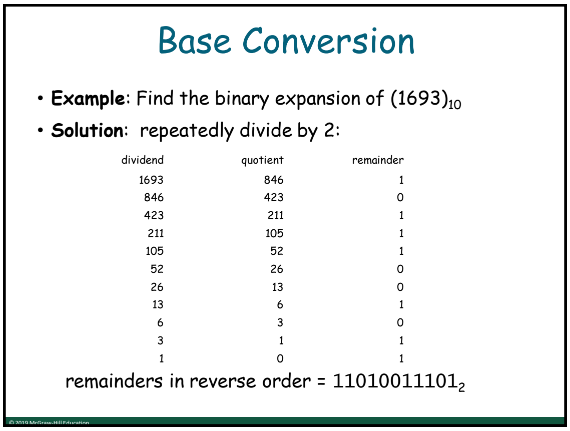
  $1543 = 8 \cdot 192 + 7$

  $192 = 8 \cdot 24 + 0$

  $24 = 8 \cdot 3 + 0$

  $3 = 8 \cdot 0 + 3$
- reverse the remainders to yield $(30071)_8$

22



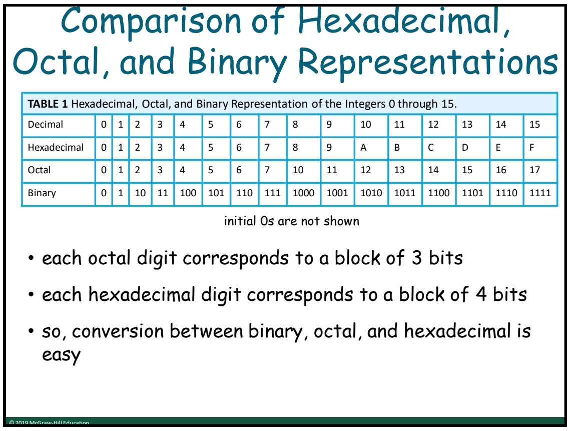
Base Conversion

- **Example**: Find the binary expansion of $(1693)_{10}$
- **Solution**: repeatedly divide by 2:

dividend	quotient	remainder
1693	846	1
846	423	0
423	211	1
211	105	1
105	52	1
52	26	0
26	13	0
13	6	1
6	3	0
3	1	1
1	0	1

remainders in reverse order = 11010011101_2

23



Comparison of Hexadecimal, Octal, and Binary Representations

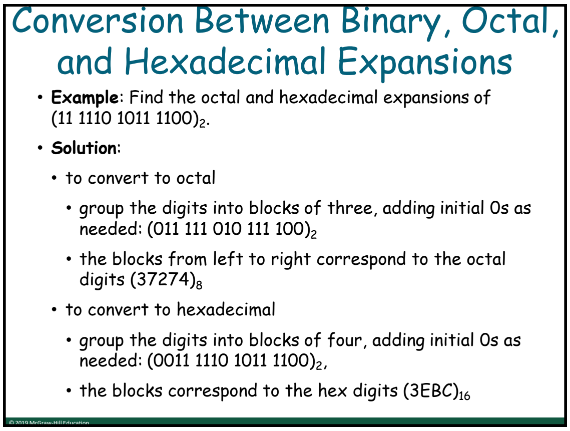
TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

initial 0s are not shown

- each octal digit corresponds to a block of 3 bits
- each hexadecimal digit corresponds to a block of 4 bits
- so, conversion between binary, octal, and hexadecimal is easy

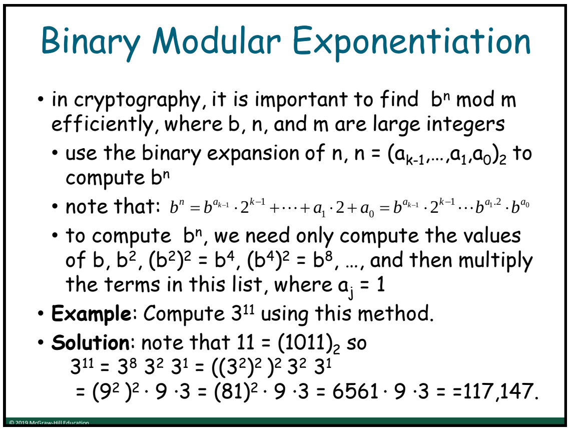
24



Conversion Between Binary, Octal, and Hexadecimal Expansions

- **Example**: Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$.
- **Solution**:
  - to convert to octal
    - group the digits into blocks of three, adding initial 0s as needed: $(011\ 111\ 010\ 111\ 100)_2$
    - the blocks from left to right correspond to the octal digits $(37274)_8$
  - to convert to hexadecimal
    - group the digits into blocks of four, adding initial 0s as needed: $(0011\ 1110\ 1011\ 1100)_2$,
    - the blocks correspond to the hex digits $(3EBC)_{16}$

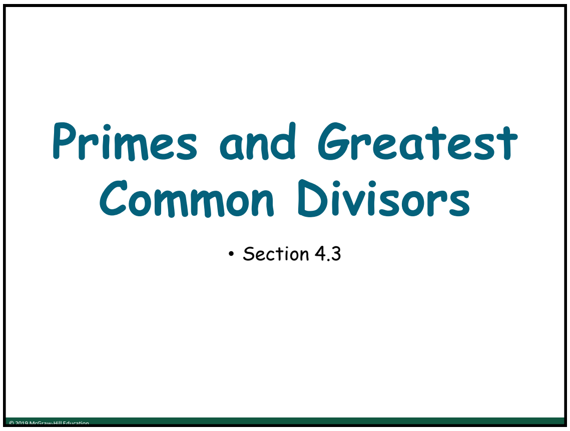
25



Binary Modular Exponentiation

- in cryptography, it is important to find b^n mod m efficiently, where b, n, and m are large integers
  - use the binary expansion of n, $n = (a_{k-1},\ldots,a_1,a_0)_2$ to compute b^n
  - note that: $b^n = b^{a_{k-1}\cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0} = b^{a_{k-1}\cdot 2^{k-1}} \cdots b^{a_1 \cdot 2} \cdot b^{a_0}$
  - to compute b^n, we need only compute the values of b, b^2, $(b^2)^2 = b^4$, $(b^4)^2 = b^8$, …, and then multiply the terms in this list, where $a_j = 1$
- **Example**: Compute 3^{11} using this method.
- **Solution**: note that $11 = (1011)_2$ so
  $3^{11} = 3^8\ 3^2\ 3^1 = ((3^2)^2)^2\ 3^2\ 3^1$
  $= (9^2)^2 \cdot 9 \cdot 3 = (81)^2 \cdot 9 \cdot 3 = 6561 \cdot 9 \cdot 3 = =117{,}147.$

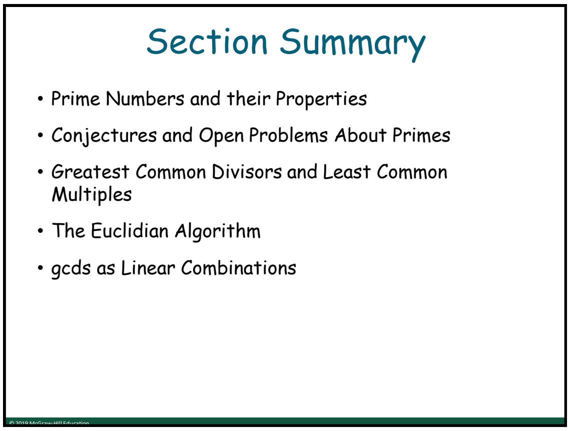
26



Primes and Greatest Common Divisors

- Section 4.3

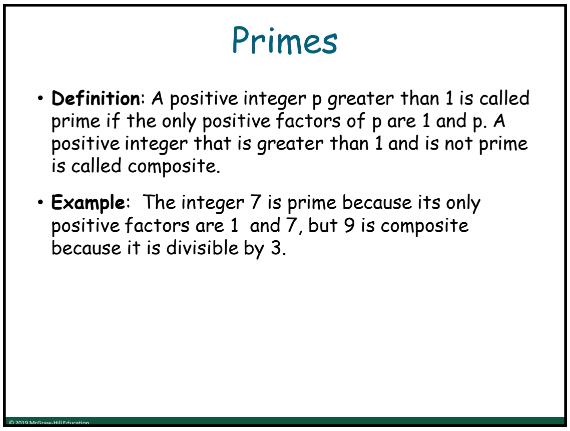
27



Section Summary

- Prime Numbers and their Properties
- Conjectures and Open Problems About Primes
- Greatest Common Divisors and Least Common Multiples
- The Euclidian Algorithm
- gcds as Linear Combinations

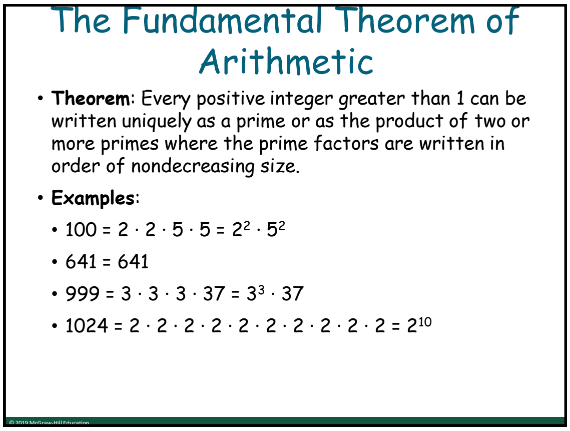
28



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.

29



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 nondecreasing size.
- **Examples**:
  - $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
  - $641 = 641$
  - $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
  - $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

30

The Sieve of Eratosthenes

Eratosthenes

(276-194 B.C.)

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.s

a. Delete all the integers, other than 2, divisible by 2.
b. Delete all the integers, other than 3, divisible by 3.
c. Delete all the integers, other than 5, divisible by 5.
d. Delete all the integers, other than 7, divisible by 7.
e. Since all 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}

31

The Sieve of Eratosthenes$_2$

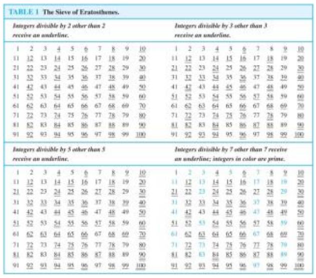


TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

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

Integers divisible by 3 other than 3 receive an underline.

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

Integers divisible by 5 other than 5 receive an underline.

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

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

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

- If an integer n is composite, then it has a prime divisor less than or equal to √n.
- To see this, note that if n = ab, then a ≤ √n or b ≤ √n.
- Trial division, a very inefficient method of determining if a number n is prime, is to try every integer i ≤ √n to see if n is divisible by i.

32

Infinitude of Primes

Euclid

(325 B.C. – 265 B.C.)

Theorem: There are infinitely many primes. (Euclid)

Proof: Assume finitely many primes: $p_1, p_2, \ldots\ldots, p_n$

- let $q = p_1p_2\cdots p_n + 1$
- either q is prime or by the fundamental theorem of arithmetic, it is a product of primes
- but none of the primes p_j divides q since if $p_j \mid q$, then p_j divides $q - p_1p_2\cdots p_n = 1$
- hence, there is a prime not on the list $p_1, p_2, \ldots\ldots, p_n$; it is either q, or if q is composite, it is a prime factor of q, but this contradicts the assumption that $p_1, p_2, \ldots\ldots, p_n$ are all the primes
- consequently, there are infinitely many primes

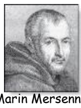
This proof was given by Euclid in *The Elements*. The proof is considered to be one of the most beautiful in all mathematics. It is the first proof in *The Book*, inspired by the famous mathematician Paul Erdős' imagined collection of perfect proofs maintained by God.

Paul Erdős

(1913-1996)

33

Representing Functions



Marin Mersenne

(1588-1648)

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

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, 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/

34

Distribution of Primes

- mathematicians have been interested in the distribution of prime numbers among the positive integers
- in the nineteenth century, the prime number theorem was proved which gives an asymptotic estimate for the number of primes not exceeding x
  - the number of primes not exceeding x, can be approximated by x/ln x

35

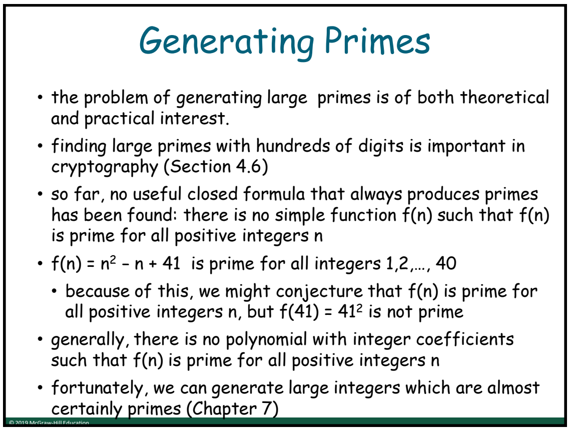
Primes and Arithmetic Progressions (optional)*

- Euclid's proof that there are infinitely many primes can be easily adapted to show that there are infinitely many primes in the following 4k + 3, k = 1,2,… (See Exercise 55)
- In the 19th century G. Lejuenne Dirichlet showed that every arithmetic progression ka + b, k = 1,2, …, where a and b have no common factor greater than 1 contains infinitely many primes. (The proof is beyond the scope of the text.)
- Are there long arithmetic progressions made up entirely of primes?
  - 5, 11, 17, 23, 29 is an arithmetic progression of five primes.
  - 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 is an arithmetic progression of ten primes.
- In the 1930s, Paul Erdős conjectured that for every positive integer n greater than 1, there is an arithmetic progression of length n made up entirely of primes. This was proven in 2006, by Ben Green and Terrence Tau.

Terence Tao

(Born 1975)

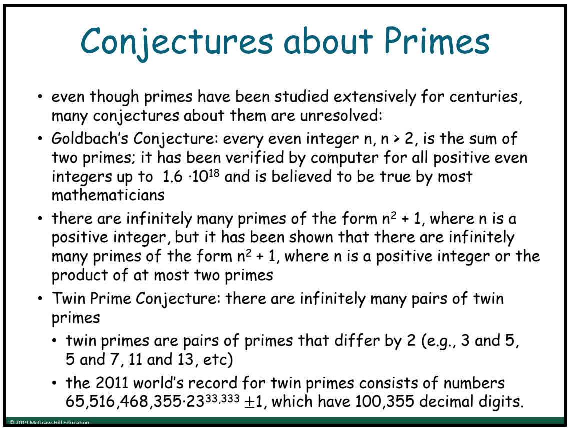
36



Generating Primes

- the problem of generating large primes is of both theoretical and practical interest.
- finding large primes with hundreds of digits is important in cryptography (Section 4.6)
- so far, no useful closed formula that always produces primes has been found: there is no simple function f(n) such that f(n) is prime for all positive integers n
- $f(n) = n^2 - n + 41$ is prime for all integers 1,2,…, 40
  - because of this, we might conjecture that f(n) is prime for all positive integers n, but $f(41) = 41^2$ is not prime
- generally, there is no polynomial with integer coefficients such that f(n) is prime for all positive integers n
- fortunately, we can generate large integers which are almost certainly primes (Chapter 7)

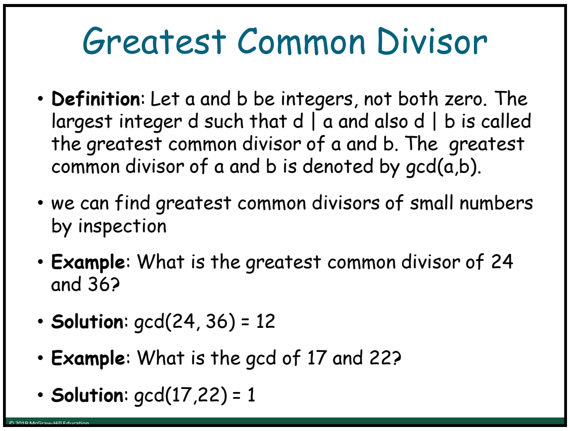
37



Conjectures about Primes

- even though primes have been studied extensively for centuries, many conjectures about them are unresolved:
- Goldbach's Conjecture: every even integer n, n > 2, is the sum of two primes; it has been verified by computer for all positive even integers up to $1.6 \cdot 10^{18}$ and is believed to be true by most mathematicians
- there are infinitely many primes of the form $n^2 + 1$, where n is a positive integer, but it has been shown that there are infinitely many primes of the form $n^2 + 1$, where n is a positive integer or the product of at most two primes
- Twin Prime Conjecture: there are infinitely many pairs of twin primes
  - twin primes are pairs of primes that differ by 2 (e.g., 3 and 5, 5 and 7, 11 and 13, etc)
  - the 2011 world's record for twin primes consists of numbers $65{,}516{,}468{,}355 \cdot 2^{333{,}333} \pm 1$, which have 100,355 decimal digits.

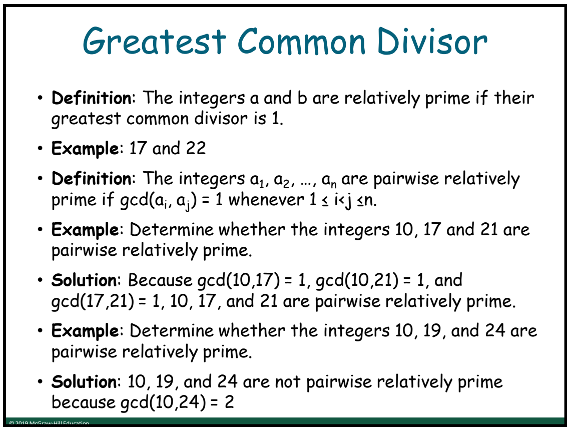
38



Greatest Common Divisor

- **Definition**: Let a and b be integers, not both zero. The largest integer d such that d | a and also d | 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).
- we 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 gcd of 17 and 22?
- **Solution**: gcd(17,22) = 1

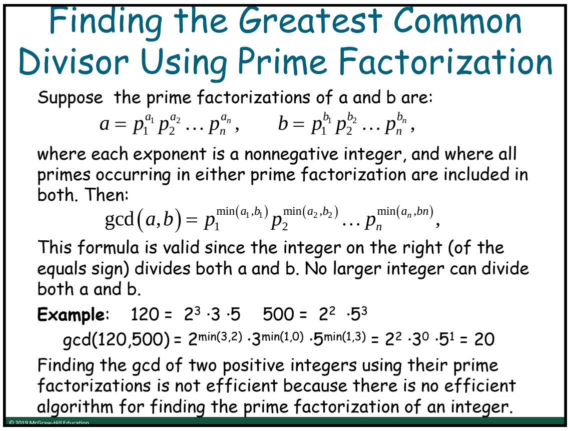
39



Greatest Common Divisor

- **Definition**: The integers a and b are relatively prime if their greatest common divisor is 1.
- **Example**: 17 and 22
- **Definition**: The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
- **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**: 10, 19, and 24 are not pairwise relatively prime because gcd(10,24) = 2

40



Finding the Greatest Common Divisor Using Prime Factorization

Suppose the prime factorizations of a and b are:

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

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

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

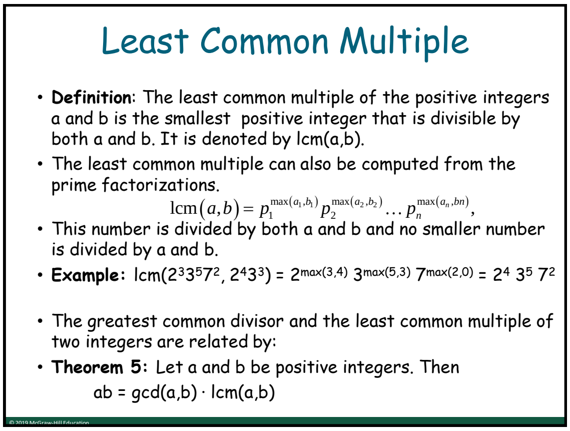
This formula is valid since the integer on the right (of the equals sign) divides both a and b. No larger integer can divide both a and b.

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

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

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 an integer.

41



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 lcm(a,b).
- The least common multiple can also be computed from the prime factorizations.

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,bn)},$$

- This number is divided by both a and b and no smaller number is divided by a and b.
- **Example:** $\operatorname{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$
- 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

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

42

Euclidean Algorithm

- the Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers

Example: Find gcd(91, 287):

- 287 = 91 · 3 + 14 — Divide 287 by 91
- 91 = 14 · 6 + 7 — Divide 91 by 14
- 14 = 7 · 2 + 0 — Divide 14 by 7

Stopping condition

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

43

gcd's as Linear Combinations

Étienne Bézout (1730-1783)

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)·6 + 1·14

44

gcd's 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 · 198 + 54
  - ii. 198 = 3 · 54 + 36
  - iii. 54 = 1 · 36 + 18
  - iv. 36 = 2 · 18
  - Now working backwards, from iii and ii above:
    - 18 = 54 − 1 · 36
    - 36 = 198 − 3 · 54
  - Substituting the 2nd equation into the 1st yields:
    - 18 = 54 − 1 · (198 − 3 · 54) = 4 · 54 − 1 · 198
  - Substituting 54 = 252 − 1 · 198 (from i) yields:
    - 18 = 4 · (252 − 1 · 198) − 1 · 198 = 4 · 252 − 5 · 198
- This method illustrated above is a two-pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers.

45

Solving Congruences

- Section 4.4

46

Section Summary 4

- Linear Congruences
- The Chinese Remainder Theorem
- Computer Arithmetic with Large Integers (*not currently included in slides, see text*)
- Fermat's Little Theorem
- Pseudoprimes
- Primitive Roots and Discrete Logarithms

47

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

$a^p \equiv a \pmod{p}$

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

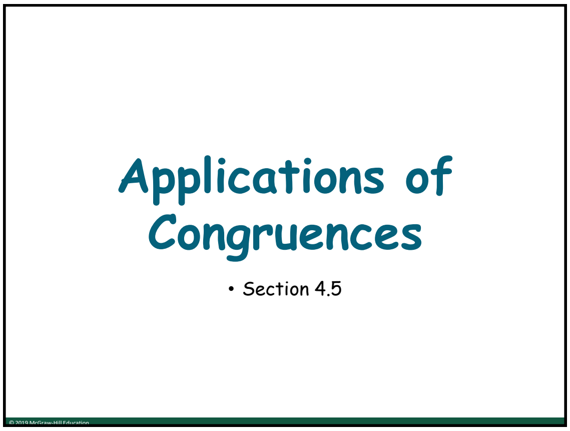
Example: Find 7^{222} **mod** 11.

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} **mod** 11 = 5.

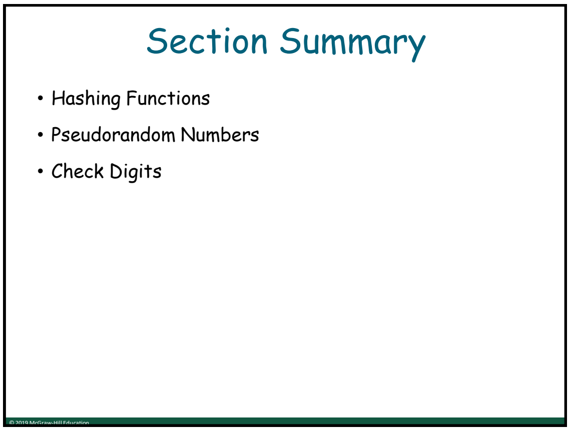
48



Applications of Congruences

- Section 4.5

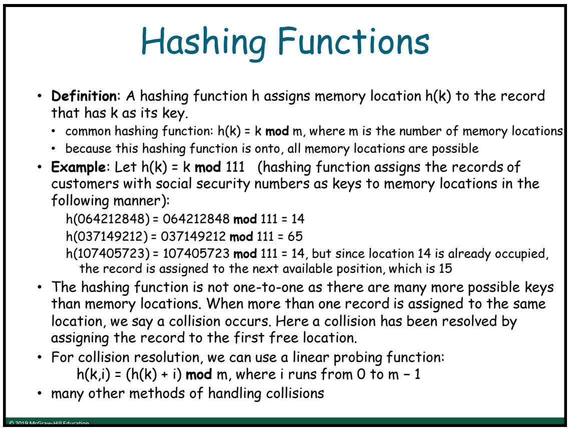
49



Section Summary

- Hashing Functions
- Pseudorandom Numbers
- Check Digits

50



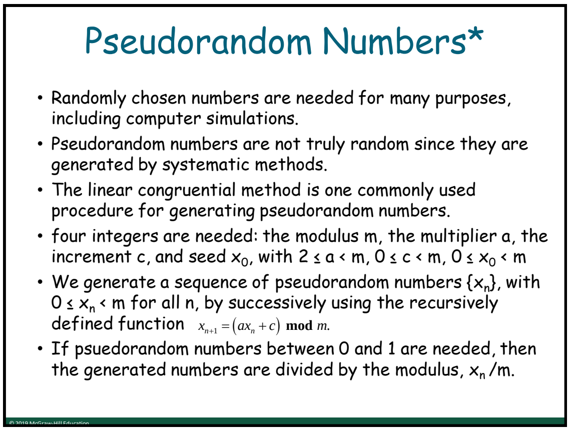
Hashing Functions

- **Definition**: A hashing function h assigns memory location h(k) to the record that has k as its key.
  - common hashing function: h(k) = k **mod** 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 **mod** 111 (hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner):

  h(064212848) = 064212848 **mod** 111 = 14
  h(037149212) = 037149212 **mod** 111 = 65
  h(107405723) = 107405723 **mod** 111 = 14, but since location 14 is already occupied, 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) **mod** m, where i runs from 0 to m – 1
- many other methods of handling collisions

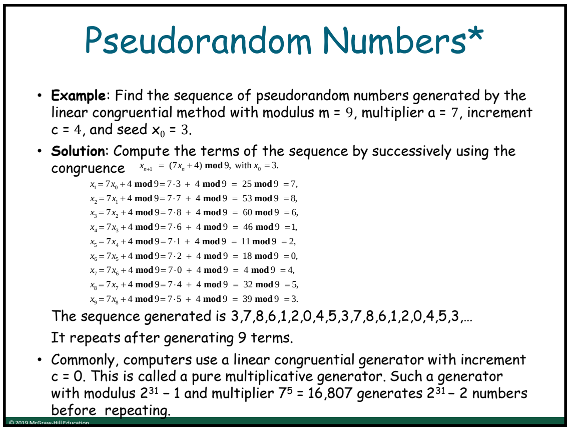
51



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 $2 \le a < m$, $0 \le c < m$, $0 \le x_0 < m$
- We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \le x_n < m$ for all n, by successively using the recursively defined function $x_{n+1} = (ax_n + c) \ \mathbf{mod}\ m.$
- If psuedorandom numbers between 0 and 1 are needed, then the generated numbers are divided by the modulus, x_n /m.

52



Pseudorandom Numbers*

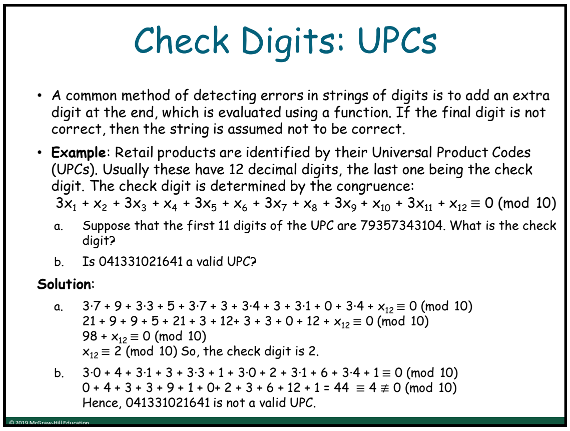
- **Example**: Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus m = 9, multiplier a = 7, increment c = 4, and seed x_0 = 3.
- **Solution**: Compute the terms of the sequence by successively using the congruence $x_{n+1} = (7x_n + 4) \ \mathbf{mod}\ 9, \text{ with } x_0 = 3.$

$$
\begin{aligned}
x_1 &= 7x_0 + 4 \ \mathbf{mod}\ 9 = 7\cdot 3 + 4 \ \mathbf{mod}\ 9 = 25 \ \mathbf{mod}\ 9 = 7,\\
x_2 &= 7x_1 + 4 \ \mathbf{mod}\ 9 = 7\cdot 7 + 4 \ \mathbf{mod}\ 9 = 53 \ \mathbf{mod}\ 9 = 8,\\
x_3 &= 7x_2 + 4 \ \mathbf{mod}\ 9 = 7\cdot 8 + 4 \ \mathbf{mod}\ 9 = 60 \ \mathbf{mod}\ 9 = 6,\\
x_4 &= 7x_3 + 4 \ \mathbf{mod}\ 9 = 7\cdot 6 + 4 \ \mathbf{mod}\ 9 = 46 \ \mathbf{mod}\ 9 = 1,\\
x_5 &= 7x_4 + 4 \ \mathbf{mod}\ 9 = 7\cdot 1 + 4 \ \mathbf{mod}\ 9 = 11 \ \mathbf{mod}\ 9 = 2,\\
x_6 &= 7x_5 + 4 \ \mathbf{mod}\ 9 = 7\cdot 2 + 4 \ \mathbf{mod}\ 9 = 18 \ \mathbf{mod}\ 9 = 0,\\
x_7 &= 7x_6 + 4 \ \mathbf{mod}\ 9 = 7\cdot 0 + 4 \ \mathbf{mod}\ 9 = 4 \ \mathbf{mod}\ 9 = 4,\\
x_8 &= 7x_7 + 4 \ \mathbf{mod}\ 9 = 7\cdot 4 + 4 \ \mathbf{mod}\ 9 = 32 \ \mathbf{mod}\ 9 = 5,\\
x_9 &= 7x_8 + 4 \ \mathbf{mod}\ 9 = 7\cdot 5 + 4 \ \mathbf{mod}\ 9 = 39 \ \mathbf{mod}\ 9 = 3.
\end{aligned}
$$

  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.
- Commonly, computers use a linear congruential generator with increment c = 0. This is called a pure multiplicative generator. Such a generator with modulus 2^{31} – 1 and multiplier 7^5 = 16,807 generates 2^{31} – 2 numbers before repeating.

53



Check Digits: UPCs

- 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:

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

  a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

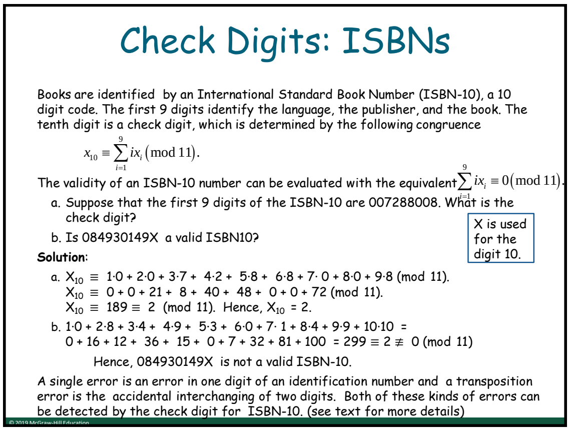
  b. Is 041331021641 a valid UPC?

Solution:

a. $3\cdot7 + 9 + 3\cdot3 + 5 + 3\cdot7 + 3 + 3\cdot4 + 3 + 3\cdot1 + 0 + 3\cdot4 + x_{12} \equiv 0 \pmod{10}$
$21 + 9 + 9 + 5 + 21 + 3 + 12+ 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$
$98 + x_{12} \equiv 0 \pmod{10}$
$x_{12} \equiv 2 \pmod{10}$ So, the check digit is 2.

b. $3\cdot0 + 4 + 3\cdot1 + 3 + 3\cdot3 + 1 + 3\cdot0 + 2 + 3\cdot1 + 6 + 3\cdot4 + 1 \equiv 0 \pmod{10}$
$0 + 4 + 3 + 3 + 9 + 1 + 0+ 2 + 3 + 6 + 12 + 1 = 44 \equiv 4 \not\equiv 0 \pmod{10}$
Hence, 041331021641 is not a valid UPC.

54



Check Digits: ISBNs

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

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

The validity of an ISBN-10 number can be evaluated with the equivalent $\sum_{i=1}^{9} i x_i \equiv 0 \pmod{11}$.

a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

b. Is 084930149X a valid ISBN10?

X is used for the digit 10.

Solution:

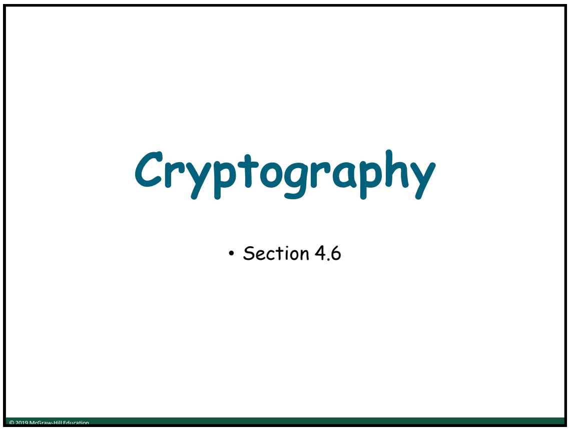
a. $X_{10} \equiv 1\cdot0 + 2\cdot0 + 3\cdot7 + 4\cdot2 + 5\cdot8 + 6\cdot8 + 7\cdot0 + 8\cdot0 + 9\cdot8 \pmod{11}$.
$X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$.
$X_{10} \equiv 189 \equiv 2 \pmod{11}$. Hence, $X_{10} = 2$.

b. $1\cdot0 + 2\cdot8 + 3\cdot4 + 4\cdot9 + 5\cdot3 + 6\cdot0 + 7\cdot1 + 8\cdot4 + 9\cdot9 + 10\cdot10 =$
$0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$

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

A single error is an error in one digit of an identification number and a transposition error is the accidental interchanging of two digits. Both of these kinds of errors can be detected by the check digit for ISBN-10. (see text for more details)

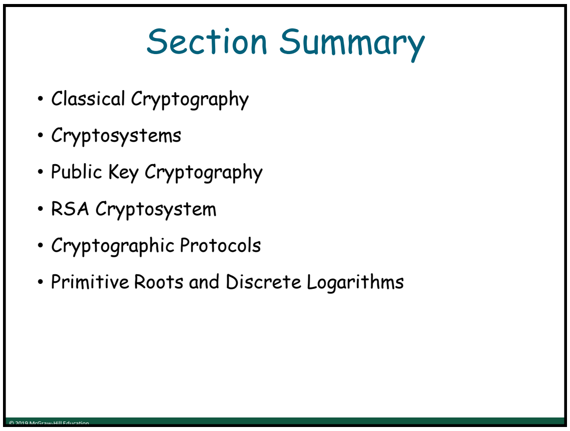
55



Cryptography

- Section 4.6

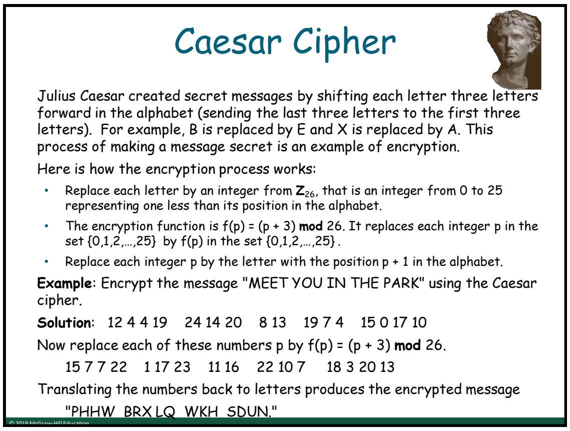
56



Section Summary

- Classical Cryptography
- Cryptosystems
- Public Key Cryptography
- RSA Cryptosystem
- Cryptographic Protocols
- Primitive Roots and Discrete Logarithms

57



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, B is replaced by E and 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) **mod** 26. It replaces each integer p in the set {0,1,2,…,25} by f(p) in the set {0,1,2,…,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

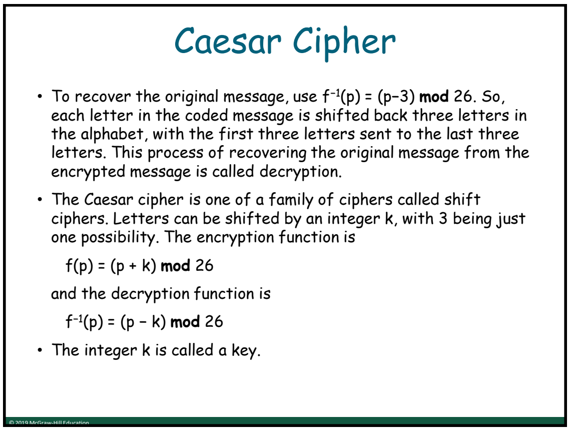
Now replace each of these numbers p by f(p) = (p + 3) **mod** 26.

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."

58



Caesar Cipher

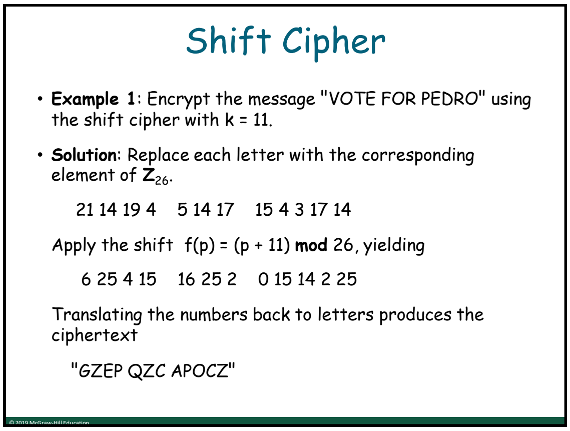
- To recover the original message, use $f^{-1}(p) = (p-3)$ **mod** 26. So, each letter in the coded message is shifted back three letters in the alphabet, with the first three letters sent to the last three letters. This process of recovering the original message from the encrypted message is called 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) **mod** 26

  and the decryption function is

  $f^{-1}(p) = (p - k)$ **mod** 26
- The integer k is called a key.

59



Shift Cipher

- **Example 1**: Encrypt the message "VOTE FOR PEDRO" using the shift cipher with k = 11.
- **Solution**: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

  21 14 19 4 5 14 17 15 4 3 17 14

  Apply the shift f(p) = (p + 11) **mod** 26, yielding

  6 25 4 15 16 25 2 0 15 14 2 25

  Translating the numbers back to letters produces the ciphertext

  "GZEP QZC APOCZ"

60

Shift Cipher

- **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 1   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"

61

Affine Ciphers

- Shift ciphers are a special case of affine ciphers which use functions of the form $f(p) = (ap + b)$ **mod** 26, where a and b are integers, chosen so that f is a bijection.

  The function is a bijection if and only if gcd(a,26) = 1.
- **Example**: What letter replaces the letter K when the function $f(p) = (7p + 3)$ **mod** 26 is used for encryption.
- **Solution**: Since 10 represents K, $f(10) = (7{\cdot}10 + 3)$ **mod** 26 =21, which is then replaced by V.

  To decrypt a message encrypted by a shift cipher, the congruence $c \equiv ap + b \pmod{26}$ needs to be solved for p.
  - Subtract b from both sides to obtain $c - b \equiv ap \pmod{26}$.
  - Multiply both sides by the inverse of a modulo 26, which exists since gcd(a,26) = 1.
  - $\bar{a}(c- b) \equiv \bar{a}ap \pmod{26}$, which simplifies to $\bar{a}(c- b) \equiv p \pmod{26}$.
  - $p \equiv \bar{a}(c- b) \pmod{26}$ is used to determine p in $\mathbf{Z}_{26}$.s

62

Cryptanalysis of Affine Ciphers

- The process of recovering plaintext from ciphertext without knowledge both of the encryption method and the key is known as cryptanalysis or breaking codes.
- An important tool for cryptanalyzing ciphertext produced with affine ciphers is the relative frequencies of letters. The nine most common letters in the English texts are E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, and R 6%.
- To analyze ciphertext:
  - Find the frequency of the letters in the ciphertext.
  - Hypothesize that the most frequent letter is produced by encrypting E.
  - If the value of the shift from E to the most frequent letter is k, shift the ciphertext by $-k$ and see if it makes sense.
  - If not, try T as a hypothesis and continue.
- **Example**: We intercepted the message "ZNK KGXRE HOXJ MKZY ZNK CUXS' that we know was produced by a shift cipher. Let's try to cryptanalyze.
- **Solution**: The most common letter in the ciphertext is K. So perhaps the letters were shifted by 6 since this would then map E to K. Shifting the entire message by -6 gives us "THE EARLY BIRD GETS THE WORM"

63

Block Ciphers

- Ciphers that replace each letter of the alphabet by another letter are called character or monoalphabetic ciphers.
- They are vulnerable to cryptanalysis based on letter frequency. Block ciphers avoid this problem, by replacing blocks of letters with other blocks of letters.
- A simple type of block cipher is called the transposition cipher. The key is a permutation σ of the set {1,2,…,m}, where m is an integer, that is a one-to-one function from {1,2,…,m} to itself.
- To encrypt a message, split the letters into blocks of size m, adding additional letters to fill out the final block. We encrypt $p_1,p_2,…,p_m$ as $c_1,c_2,…,c_m = p_{\sigma(1)},p_{\sigma(2)},…,p_{\sigma(m)}$.
- To decrypt the $c_1,c_2,…,c_m$ transpose the letters using the inverse permutation σ^{-1}.

64

Block Ciphers

- **Example**: Using the transposition cipher based on the permutation σ of the set {1,2,3,4} with σ(1) = 3, σ(2) = 1, σ(3) = 4, σ(4) = 2,
  a. Encrypt the plaintext PIRATE ATTACK
  b. Decrypt the ciphertext message SWUE TRAEOEHS, which was encrypted using the same cipher.
- **Solution**:
  a. Split into four blocks PIRA TEAT TACK.
     Apply the permutation σ giving IAPR ETTA AKTC
  b. σ^{-1}: $\sigma^{-1}(1) = 2$, $\sigma^{-1}(2) = 4$, $\sigma^{-1}(3) = 1$, $\sigma^{-1}(4) = 3$.

     Apply the permutation σ^{-1} giving USEW ATER HOSE.

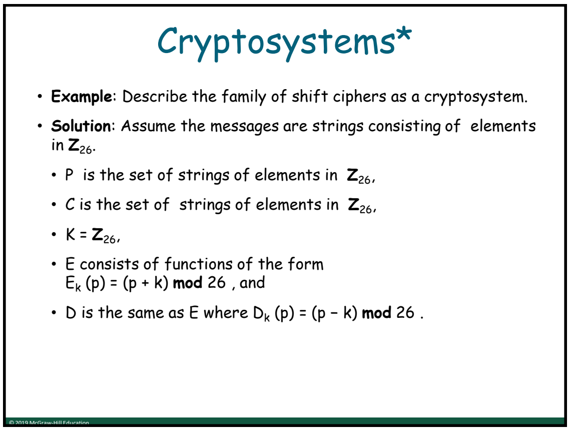
     Split into words to obtain USE WATER HOSE

65

Cryptosystems

- **Definition**: A cryptosystem is a five-tuple (P,C,K,E,D), where
  - P is the set of plaintext strings
  - C is the set of ciphertext strings,
  - K is the keyspace (set of all possible keys)
  - E is the set of encryption functions
  - D is the set of decryption functions
- The encryption function in E corresponding to the key k is denoted by E_k and the description function in D that decrypts cipher text encrypted using E_k is denoted by D_k. Therefore:
- $D_k(E_k(p)) = p$, for all plaintext strings p.

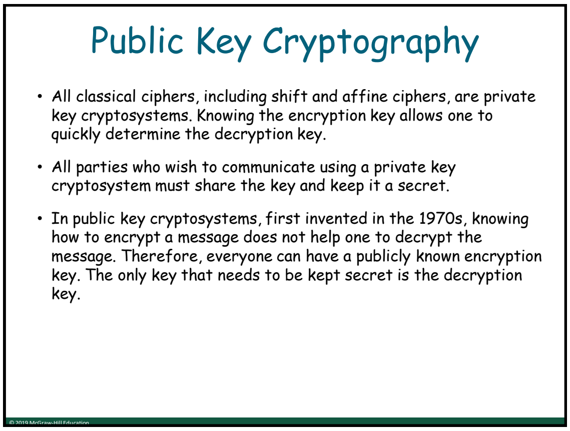
66



Cryptosystems*

- **Example**: Describe the family of shift ciphers as a cryptosystem.
- **Solution**: Assume the messages are strings consisting of elements in $\mathbf{Z}_{26}$.
  - P is the set of strings of elements in $\mathbf{Z}_{26}$,
  - C is the set of strings of elements in $\mathbf{Z}_{26}$,
  - K = $\mathbf{Z}_{26}$,
  - E consists of functions of the form $E_k(p) = (p + k)$ **mod** 26 , and
  - D is the same as E where $D_k(p) = (p - k)$ **mod** 26 .

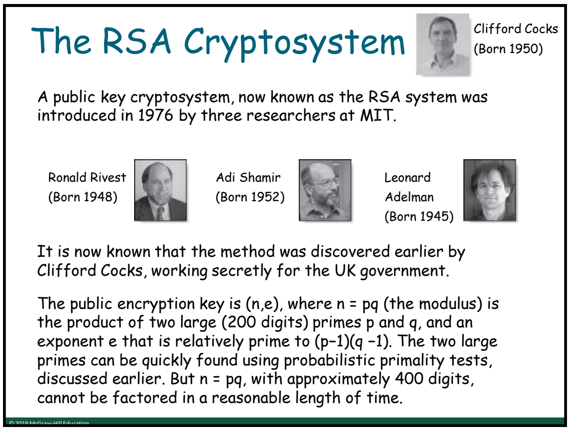
67



Public Key Cryptography

- All classical ciphers, including shift and affine ciphers, are private key cryptosystems. Knowing the encryption key allows one to quickly determine the decryption key.
- All parties who wish to communicate using a private key cryptosystem must share the key and keep it a secret.
- In public key cryptosystems, first invented in the 1970s, knowing how to encrypt a message does not help one to decrypt the message. Therefore, everyone can have a publicly known encryption key. The only key that needs to be kept secret is the decryption key.

68



The RSA Cryptosystem

Clifford Cocks
(Born 1950)

A public key cryptosystem, now known as the RSA system was introduced in 1976 by three researchers at MIT.

Ronald Rivest
(Born 1948)

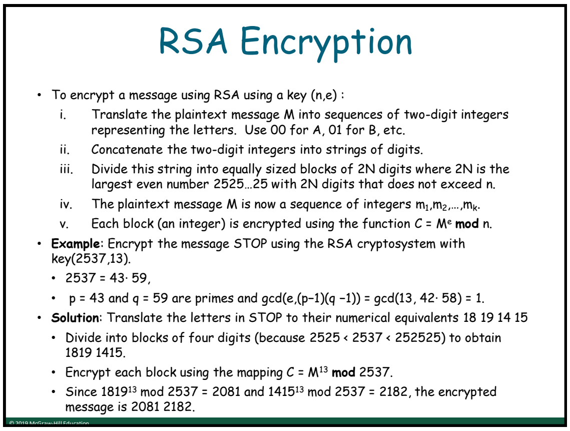
Adi Shamir
(Born 1952)

Leonard Adelman
(Born 1945)

It is now known that the method was discovered earlier by Clifford Cocks, working secretly for the UK government.

The public encryption key is (n,e), where n = pq (the modulus) is the product of two large (200 digits) primes p and q, and an exponent e that is relatively prime to (p−1)(q −1). The two large primes can be quickly found using probabilistic primality tests, discussed earlier. But n = pq, with approximately 400 digits, cannot be factored in a reasonable length of time.

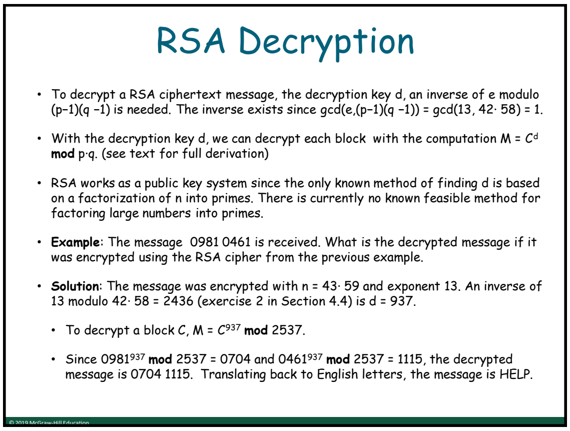
69



RSA Encryption

- To encrypt a message using RSA using a key (n,e) :
  1. i. Translate the plaintext message M into sequences of two-digit integers representing the letters. Use 00 for A, 01 for B, etc.
  2. ii. Concatenate the two-digit integers into strings of digits.
  3. iii. Divide this string into equally sized blocks of 2N digits where 2N is the largest even number 2525…25 with 2N digits that does not exceed n.
  4. iv. The plaintext message M is now a sequence of integers $m_1, m_2, \ldots, m_k$.
  5. v. Each block (an integer) is encrypted using the function $C = M^e$ **mod** n.
- **Example**: Encrypt the message STOP using the RSA cryptosystem with key(2537,13).
  - 2537 = 43· 59,
  - p = 43 and q = 59 are primes and gcd(e,(p−1)(q −1)) = gcd(13, 42· 58) = 1.
- **Solution**: Translate the letters in STOP to their numerical equivalents 18 19 14 15
  - Divide into blocks of four digits (because 2525 ‹ 2537 ‹ 252525) to obtain 1819 1415.
  - Encrypt each block using the mapping $C = M^{13}$ **mod** 2537.
  - Since 1819^{13} mod 2537 = 2081 and 1415^{13} mod 2537 = 2182, the encrypted message is 2081 2182.

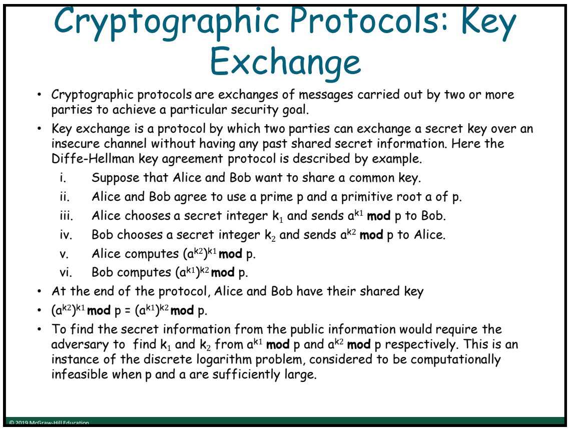
70



RSA Decryption

- To decrypt a RSA ciphertext message, the decryption key d, an inverse of e modulo (p−1)(q −1) is needed. The inverse exists since gcd(e,(p−1)(q −1)) = gcd(13, 42· 58) = 1.
- With the decryption key d, we can decrypt each block with the computation $M = C^d$ **mod** p·q. (see text for full derivation)
- RSA works as a public key system since the only known method of finding d is based on a factorization of n into primes. There is currently no known feasible method for factoring large numbers into primes.
- **Example**: The message 0981 0461 is received. What is the decrypted message if it was encrypted using the RSA cipher from the previous example.
- **Solution**: The message was encrypted with n = 43· 59 and exponent 13. An inverse of 13 modulo 42· 58 = 2436 (exercise 2 in Section 4.4) is d = 937.
  - To decrypt a block C, $M = C^{937}$ **mod** 2537.
  - Since 0981^{937} **mod** 2537 = 0704 and 0461^{937} **mod** 2537 = 1115, the decrypted message is 0704 1115. Translating back to English letters, the message is HELP.

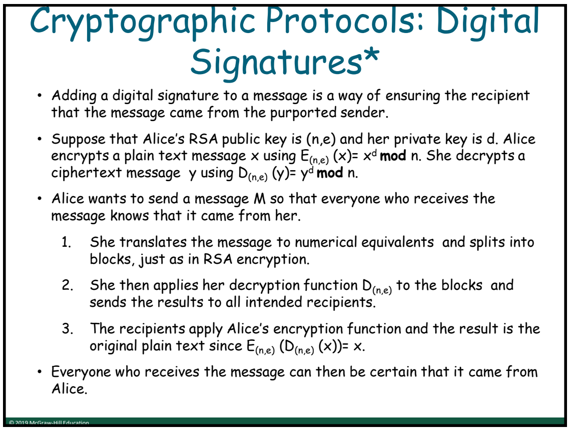
71



Cryptographic Protocols: Key Exchange

- Cryptographic protocols are exchanges of messages carried out by two or more parties to achieve a particular security goal.
- Key exchange is a protocol by which two parties can exchange a secret key over an insecure channel without having any past shared secret information. Here the Diffe-Hellman key agreement protocol is described by example.
  1. i. Suppose that Alice and Bob want to share a common key.
  2. ii. Alice and Bob agree to use a prime p and a primitive root a of p.
  3. iii. Alice chooses a secret integer k_1 and sends a^{k1} **mod** p to Bob.
  4. iv. Bob chooses a secret integer k_2 and sends a^{k2} **mod** p to Alice.
  5. v. Alice computes $(a^{k2})^{k1}$ **mod** p.
  6. vi. Bob computes $(a^{k1})^{k2}$ **mod** p.
- At the end of the protocol, Alice and Bob have their shared key
- $(a^{k2})^{k1}$ **mod** p = $(a^{k1})^{k2}$ **mod** p.
- To find the secret information from the public information would require the adversary to find k_1 and k_2 from a^{k1} **mod** p and a^{k2} **mod** p respectively. This is an instance of the discrete logarithm problem, considered to be computationally infeasible when p and a are sufficiently large.

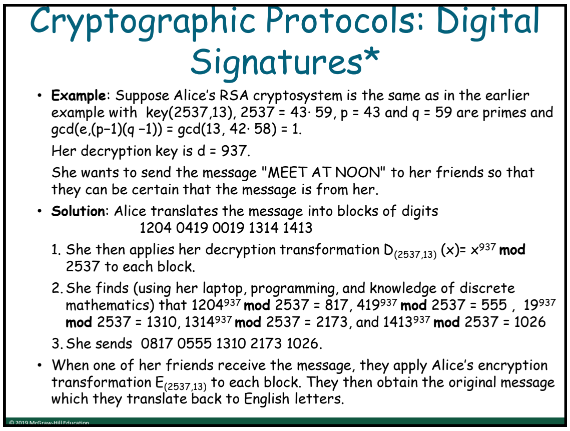
72



Cryptographic Protocols: Digital Signatures*

- Adding a digital signature to a message is a way of ensuring the recipient that the message came from the purported sender.
- Suppose that Alice's RSA public key is (n,e) and her private key is d. Alice encrypts a plain text message x using $E_{(n,e)}$ (x)= x^d **mod** n. She decrypts a ciphertext message y using $D_{(n,e)}$ (y)= y^d **mod** n.
- Alice wants to send a message M so that everyone who receives the message knows that it came from her.
  1. She translates the message to numerical equivalents and splits into blocks, just as in RSA encryption.
  2. She then applies her decryption function $D_{(n,e)}$ to the blocks and sends the results to all intended recipients.
  3. The recipients apply Alice's encryption function and the result is the original plain text since $E_{(n,e)}$ ($D_{(n,e)}$ (x))= x.
- Everyone who receives the message can then be certain that it came from Alice.

73



Cryptographic Protocols: Digital Signatures*

- **Example**: Suppose Alice's RSA cryptosystem is the same as in the earlier example with key(2537,13), 2537 = 43· 59, p = 43 and q = 59 are primes and gcd(e,(p−1)(q −1)) = gcd(13, 42· 58) = 1.

  Her decryption key is d = 937.

  She wants to send the message "MEET AT NOON" to her friends so that they can be certain that the message is from her.
- **Solution**: Alice translates the message into blocks of digits

  1204 0419 0019 1314 1413

  1. She then applies her decryption transformation $D_{(2537,13)}$ (x)= x^{937} **mod** 2537 to each block.
  2. She finds (using her laptop, programming, and knowledge of discrete mathematics) that 1204^{937} **mod** 2537 = 817, 419^{937} **mod** 2537 = 555 , 19^{937} **mod** 2537 = 1310, 1314^{937} **mod** 2537 = 2173, and 1413^{937} **mod** 2537 = 1026
  3. She sends 0817 0555 1310 2173 1026.
- When one of her friends receive the message, they apply Alice's encryption transformation $E_{(2537,13)}$ to each block. They then obtain the original message which they translate back to English letters.

74