Number Theory

Chapter 4
ICSI 210 Discrete Structures

Number Theory

- *Number theory* is the part of mathematics devoted to the study of the integers and their properties. It has important applications to computer science.
  - Key ideas： *divisibility* and the *primality* of integers.
    - Primality: the property of being a prime number.
    - Representations of integers including binary and hexadecimal representations
- Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.

Topics

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

Divisibility and Modular Arithmetic

Section 4.1

Division

- **Definition**: If *a* and *b* are integers with $a \neq 0$, then *a divides b* if there exists an integer *c* such that $b = ac$.
  - When *a* divides *b, denoted by* $a \mid b$, *a* is a *factor* or *divisor* of *b, b* is a *multiple* of *a*, and *b*/*a* is an integer.
  - $a \nmid b$: *a* does not divide *b*.
  - For example, $3 \mid 12$ and $3 \nmid 7$.

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 $a \mid c$.

Properties of Divisibility

- Proof (optional):

i. Suppose $a \mid b$ and $a \mid c$, then there are integers s and t with $b = as$ and $c = at$. Hence, $b + c = as + at = a(s + t)$. Hence, $a \mid (b + c)$

ii. Suppose that $a \mid b$, then there exists an integer k such that $ka = b$. Because $a(ck) = bc$ it follows that $a \mid bc$.

iii. Suppose $a \mid b$, so that $b = at$ for some t , and $b \mid c$, so that $c = bs$ for some s. Then substituting the first equation into the second, obtain $c = (at)s = a(ts)$. Hence, $a \mid c$.

Properties of Divisibility

- **Corollary**: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Properties of Divisibility

- **Proof (optional):**

  By Theorem 1 ii,

  $a \mid b$, then $a \mid mb$ for all integers m.

  $a \mid c$, then $a \mid nc$ for all integers n.

  By Theorem 1 i,

  $a \mid mb + nc$ whenever m and n are integers.

Division Algorithm

- **Division Algorithm**: If a is an integer and d is a **positive** integer, then there are unique integers q and r , with $\mathbf{0 \leq r < d}$, such that $a = dq + r$.
  - a is called the *dividend*.
  - d is called the *divisor*.
  - q is called the *quotient*.
    - Function *div*: $q = a$ **div** d
  - r is called the *remainder*.
    - Function *mod*: $r = a$ **mod** d

Division Algorithm

- **Example**: What are the quotient and remainder when 101 is divided by 11?

  Solution:

  $a = dq + r$

  $q = a \text{ div } d = 101 \text{ div } 11 = 9.$

  $r = a \bmod d = 101 \bmod 11 = 2.$

  $101 = 11(9) + 2$, d (11) is a **positive** integer, and $0 \leq r < d = 0 \leq 2 < 11$ satisfies.

Division Algorithm

- **Example**: What are the quotient and remainder when −11 is divided by 3?

  Solution:

  $a = dq + r$

  try $-11 = 3(-3) + (-2)$ and d (3) is a **positive** integer.
  but $0 \leq r < d = 0 \leq -2 < 3$ doesn't satisfy.

  Change q to -4. $-11 = 3(-4) + 1$, d (3) is a **positive** integer, and $0 \leq r < d = 0 \leq 1 < 3$ satisfies.

Modular Arithmetic

- Sometimes, only the remainder of an integer, when divided by some specified **positive** integer, matters.
  - For instance, when we ask what time it will be (on a 24-hour clock) 50 hours from now, we care only about the remainder when 50 plus the current hour is divided by 24.
- **Congruence Relation**: two integers have **the same remainder** when they are divided by the **positive** integer *m*.

Congruence Relation

- **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 $a \bmod m = b \bmod m$.
  - $a \equiv b \pmod{m}$: a is congruent to b modulo m.
  - $a \not\equiv b \pmod{m}$: a is **not** congruent to b modulo m.
  - $a \equiv b \pmod{m}$ is a *congruence* and m is its *modulus.*
- a and b are congruent modulo m if and only if
  1) **they have the same remainder when divided by m.**

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* and *b* are congruent modulo *m* if and only if
  1) they have the same remainder when divided by *m*.
     or
  2) ***m* divides *a – b*.**

(mod *m*) and **mod** *m*

- In $a \equiv b \pmod{m}$, **mod** is a relation on the set of integers.
- In $a \bmod m = b$, **mod** is a function.

Congruence Relation

- **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.

Congruence Relation

- **Example**: modulo 6 table.

…

$-5 \equiv 1 \ (mod\ 6)$

$-4 \equiv 2 \ (mod\ 6)$

$-3 \equiv 3 \ (mod\ 6)$

$-2 \equiv 4 \ (mod\ 6)$

$-1 \equiv 5 \ (mod\ 6)$

$0 \equiv 6 \ (mod\ 6)$

$1 \equiv 7 \ (mod\ 6)$

$2 \equiv 8 \ (mod\ 6)$

$3 \equiv 9 \ (mod\ 6)$

$4 \equiv 10 \ (mod\ 6)$

$5 \equiv 11 \ (mod\ 6)$

$6 \equiv 12 \ (mod\ 6)$

$7 \equiv 13 \ (mod\ 6)$

…

Congruence Relation

- **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 $a = b + km$.

Congruence Relation

- **Theorem 4 proof (optional)**:
  - If $a \equiv b \pmod{m}$, then $m \mid a - b$ *by* definition. 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 $a \equiv b \pmod{m}$.

Congruence Relation

- **Summary:** If a and b are integers and m is a positive integer, the integers a and b are congruent modulo m

1) *if only if* a **mod** $m = b$ **mod** m. (Theorem 3)

   or

2) *if* m divides $a - b$. (Definition)

   or

3) *if only if* there is an integer k such that $a = b + km$. (Theorem 4)

Congruence 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

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

  - Notice that the modulus of the two congruences must be the same.
  - The sum of two congruences is a congruence.
  - The product of two congruences is a congruence.

Congruence of Sums and Products

- **Theorem 5 proof (optional):**

  Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers s and t with $b = a + sm$ and $d = c + tm$.

  Therefore,

  $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and

  $b\,d = (a + sm)(c + tm) = ac + m(at + cs + stm)$.

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

Congruence of Sums and Products

- **Example**: Find the sum and the product of the following congruence.

  $7 \equiv 2 \pmod 5$

  $11 \equiv 1 \pmod 5$

  Solution:

  Because $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$, the sum of them is

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

  The product of them is

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

Manipulation of Congruence

- Multiplying both sides of a valid congruence by an integer preserves validity.
  If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.
- Adding an integer to both sides of a valid congruence preserves validity.
  If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

Manipulation of Congruences

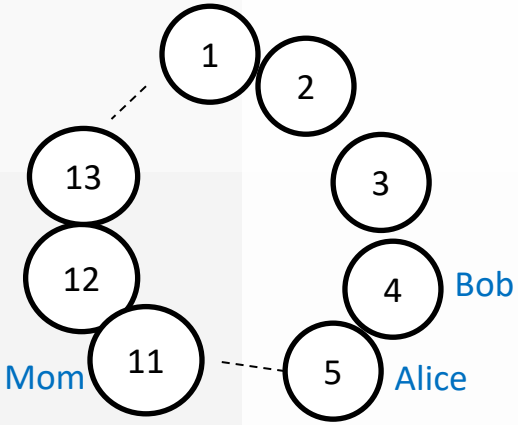
- Dividing both sides of a congruence by an integer **does not always** produce a valid congruence.
- **Example**:
  $14 \equiv 8 \pmod 6$.

  Dividing both sides by 2, but $7 \not\equiv 4 \pmod 6$.

- We will discuss in section 4.3 for conditions when Dividing both sides of a congruence by an integer preserves validity.

Exercises

- When Bob and Alice were kids, they loved the Merry-Go_Round ride. There were 13 seats in the ride. There were also 13 waiting points. Mom was always at the 11th point.
  - Bob always started at the 4th point. He had a button inside his seat that, when he pushed, advanced his ride 5 seats.
  - Alice always started at the 5th point. She had a button inside her seat that, when she pushed, advanced her ride 6 seats.



Exercises

- How many times does Bob have to push his buttons to meet mom? After meeting mom first time, how many more times does he have to push the button to meet mom again?
- How many times does Alice have to push her buttons to meet mom? After meeting mom first time, how many more times does she have to push the button to meet mom again?
- Write the modular arithmetic formula corresponding to the two cases.

Exercises

n	Bob +5	Alice+6
0	4	5
1	9	**11**
2	1	4
3	6	10
4	**11**	3
5	3	9
6	8	2
7	13	8
8	5	1
9	10	7
10	2	13
11	7	6
12	12	12
13	4	5
14	…	**11**

Exercises

Bob:

$4 + 5 \times n \equiv 11 \pmod{13}$

Add -4 to both sides:

$4 + (-4) + 5 \times n \equiv 11 + (-4) \pmod{13}$

$5 \times n \equiv 7 \pmod{13}$

Alice:

$5 + 6 \times n \equiv 11 \pmod{13}$

Add -5 to both sides:

$5 + (-5) + 6 \times n \equiv 6 + (-5) \pmod{13}$

$6 \times n \equiv 6 \pmod{13}$

Can this congruence be divided by 6?

mod *m* Function

- **Corollary**: Let *m* be a positive integer and let *a* and *b* be integers.

  $(a + b)$ **mod** $m = ((a \textbf{ mod } m) + (b \textbf{ mod } m))$ **mod** m

  ab **mod** $m = ((a \textbf{ mod } m)(b \textbf{ mod } m))$ **mod** m

- Use a **mod** m and b **mod** m to find $(a + b)$ **mod** m and (ab) **mod** m.

mod *m* Function

- **Example:** find the value of the expression.
  (−133 **mod** 23 + 261 **mod** 23) **mod** 23.

Solution:

a = -133, b = 261, and m = 23.

(−133 **mod** 23 + 261 **mod** 23) **mod** 23

= (-133 + 261) **mod** 23

= 128 **mod** 23 = 13.

mod *m* Function

- **Example:** find the value of the expression.
  (457 **mod** 23 · 182 **mod** 23) **mod** 23

  Solution:

  $a = 457$, $b = 182$, and $m = 23$.

  (457 **mod** 23 · 182 **mod** 23) **mod** 23

  = (457 · 182) **mod** 23

  = 83174 **mod** 23

  = 6

Arithmetic Modulo *m*

- **Definitions**: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m: {0,1, …., $m-1$}.
  - The operation $+_m$ is defined as $a +_m b = (a + b)$ **mod** m. This is *addition modulo m*.
  - The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b)$ **mod** m. This is *multiplication modulo m*.

Arithmetic Modulo *m*

- **Example**: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

  Solution:

  $7 +_{11} 9 = (7 + 9)$ **mod** $11 = 16$ **mod** $11 = 5$

  $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$

$+_m$ and $\cdot_m$ Properties

- **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**: If a belongs to $\mathbf{Z}_m$, then

  $a +_m 0 = a$ and $a \cdot_m 1 = a$.
  - The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.

$+_m$ and $\cdot_m$ Properties

- **Additive inverses**: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.

  $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

- **Distributivity**: If a, b, and c belong to $\mathbf{Z}_m$, then

  $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

  $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Integer Representations and Algorithms

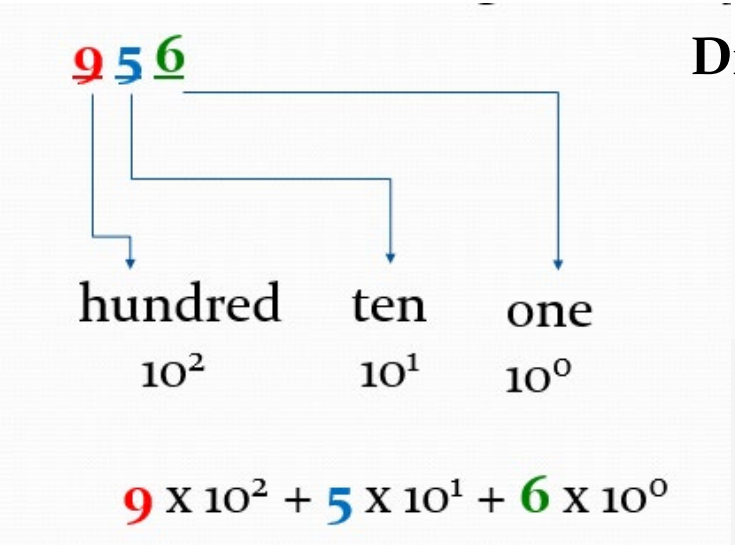
Section 4.2

Topics

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

Representations of Integers

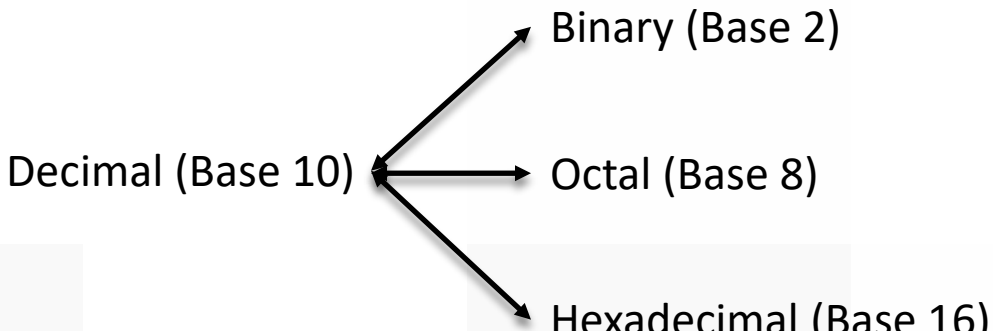
- In the modern world, we use *decimal,* or *base* 10, *notation* to represent integers. For example when we write 956, we mean $9 \cdot 10^2 + 5 \cdot 10^1 + 6 \cdot 10^0$.
- We can represent numbers using any base *b*, where *b* is a positive integer greater than 1.



Digits: {0,1,2,3,4,5,6,7,8,9}

Representations of Integers

- The bases *b* = 2 (*binary*), *b* = 8 (*octal*) , and *b* = 16 (*hexadecimal*) are important for computing and communications.



Base *b* Representations

- **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 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.

  - called the *base b expansion of n* and denoted by $(a_k a_{k-1} \ldots a_1 a_0)_b$.
  - can omit the subscript 10 for base 10 expansions.

Binary Expansions

- Most computers represent integers and do arithmetic with binary (base 2) expansions of integers.
- The binary expansions use the digits {0,1}.

Digits from {0,1}										
value	…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1

Binary Expansions

- **Example**: What is the decimal expansion of the integer that has $(1\ 0101\ 1111)_2$ as its binary expansion?

Solution:

2^9 512	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
	1	0	1	0	1	1	1	1	1

$$(1\ 0101\ 1111)_2 = 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 351.$$

Binary Expansions

- **Example**: What is the decimal expansion of the integer that has $(11011)_2$ as its binary expansion?

  Solution:

2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
1	1	0	1	1

$$(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 27.$$

Octal Expansions

- The octal expansion (base 8) uses the digits {0,1,2,3,4,5,6,7}.

Digits from {0,1}.										
value	…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
Digits from {0,1,2,3,4,5,6,7}.										
value	…	8^8 …	8^7 …	8^6 …	8^5 …	8^4 4096	8^3 512	8^2 64	8^1 8	8^0 1

Octal Expansions

- **Example**: What is the decimal expansion of the number with octal expansion $(7016)_8$?

Solution:

8^3 512	8^2 64	8^1 8	8^0 1
7	0	1	6

$$7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$$

Octal Expansions

- **Example**: What is the decimal expansion of the number with octal expansion $(111)_8$?

Solution:

8^2 64	8^1 8	8^0 1
1	1	1

$$1 \cdot 8^2 + 1 \cdot 8^1 + 1 \cdot 8^0 = 64 + 8 + 1 = 73$$

Hexadecimal Expansions

- The hexadecimal expansion needs 16 digits.
- The hexadecimal system uses the digits {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.

Decimal	Hexadecimal
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F

Hexadecimal Expansions

Digits from {0,1}										
value	…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
Digits from {0,1,2,3,4,5,6,7}										
value	…	8^8 …	8^7 …	8^6 …	8^5 …	8^4 4096	8^3 512	8^2 64	8^1 8	8^0 1
Digits from {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}										
value	…	16^8	16^7	16^6	16^5	16^4	16^3	16^2	16^1	16^0

Hexadecimal Expansions

- **Example**: What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

  Solution:

16^4	16^3	16^2	16^1	16^0
2	A	E	0	B

$$2\cdot16^4 + 10\cdot16^3 + 14\cdot16^2 + 0\cdot16^1 + 11\cdot16^0 = 175627$$

Hexadecimal Expansions

- **Example**: What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?

  Solution:

16^1	16^0
E	5

$$14 \cdot 16^1 + 5 \cdot 16^0 = 224 + 5 = 229$$

Hexadecimal Expansions

- **Example**: What is the decimal number of $(1AC9)_{16}$?

  Solution:

16^4	16^3	16^2	16^1	16^0
	4096	256	16	1
	1	A	C	9

$$(1AC9)_{16} = 1 \times 4096 + 10 \times 256 + 12 \times 16 + 9 \times 1$$
$$= 6857$$

Decimal to Hexadecimal

- To convert from decimal to hexadecimal:
  - **Step 1:** Decimal -> Binary
  - **Step 2**: Binary -> Hexadecimal
    - Each hexadecimal digit corresponds to a block of 4 binary digits.
    - Form blocks of 4 binary digits from right to left.
    - Conversion between binary and hexadecimal is easy.

Step 1: Decimal -> Binary

- **Method 1:** Descending Powers of Two* and Subtraction. For example, 175_{10}.
  1) Make a chart.
  2) Start with the greatest power of 2 that is ≤ 175. if it fits, subtract it from 175 or the current remainder and mark it with 1. If it doesn't fit, mark it with 0.
  3) Move to the next lower power of two. Repeat until you reach the end of the chart.
  4) Write out the binary answer.

* This method work for any base such as 2,8, and 16.

Step 1: Decimal -> Binary

- **Method 1 example:** For example, 175_{10}.
  1) Make a chart.

…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1

Step 1: Decimal -> Binary

- **Method 1 example cont.:**
  - Start with the greatest power of 2 that is ≤ 175. if it fits, subtract it from 175 or the current remainder and mark it with 1. If it doesn't fit, mark it with 0.

…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
		1							

  - Start with 128, subtract 128 from 175, and mark it with 1. The remainder is 175 – 128 = 47.

Step 1: Decimal -> Binary

- **Method 1 example cont.:**
  - Move to the next lower power of two. Repeat until you reach the end of the chart.

…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
		1	0	1	0				

  - The next lower power of two is 64 that doesn't fit. Mark 64 with 0.
  - The next lower power of two is 32 that fits. Subtract 32 from 47 and mark it with 1. The remainder is 47 – 32 = 15.
  - The next lower power of two is 16 that doesn't fit. Mark 16 with 0.

Step 1: Decimal -> Binary

- **Method 1 example cont.:**
  - Move to the next lower power of two. Repeat until you reach the end of the chart.

…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
		1	0	1	0	1	1	1	1

  - The next lower power of two is 8 that fits. Subtract 8 from 15 and mark it with 1. The remainder is 15 – 8 = 7.
  - The next lower power of two is 4 that fits. Subtract 4 from 7 and mark it with 1. The remainder is 7 – 4 = 3.

Step 1: Decimal -> Binary

- **Method 1 example cont.:**
  - Move to the next lower power of two. Repeat until you reach the end of the chart.

…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
		1	0	1	0	1	1	1	1

  - The next lower power of two is 2 that fits. Subtract 2 from 3 and mark it with 1. The remainder is 3 – 2 = 1.
  - The next lower power of two is 1 that fits. Subtract 1 from 1 and mark it with 1. The remainder is 1 – 1 = 0. The end of the chart is reached.

Step 1: Decimal -> Binary

- **Method 1 example cont.:**
  - Write out the binary answer.

…	2^8 256	2^7 128	2^6 64	2^5 32	2^4 16	2^3 8	2^2 4	2^1 2	2^0 1
		1	0	1	0	1	1	1	1

$$(175)_{10} = 128 + 32 + 8 + 4 + 2 + 1$$
$$= 1010\ 1111_2$$

Step 2: Binary -> Hexadecimal

- **Binary -> Hexadecimal**
  - Form blocks of 4 binary digits from right to left.
  - Convert each group to hexadecimal.

$(175)_{10} = \underline{1010}\ \underline{1111}_2$

$(1010)_2 = A_{16}$

$(1111)_2 = F_{16}$

$(175)_{10} = 1010\ 1111_2 = AF_{16}$

Hexadecimal Expansions

- **Example**: What is the hexadecimal expansion of the number $(1275)_{10}$?

  Solution:

  $(1275)_{10} = 1024 + 128 + 64 + 32 + 16 + 8 + 2 + 1$

		2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
		1024	512	256	128	64	32	16	8	4	2	1
	0	1	0	0	1	1	1	1	1	0	1	1
	4				F				B			

$(1275)_{10} = 4FB_{16}$

Base Conversion

- **Method 1:** Descending Powers of *b* and Subtraction
  - Convert a decimal expansion to a non-decimal expansion such as binary, octal or hexadecimal.
  - It gets complicated when the decimal value is larger.
- **Method 2**: Divide method
  - Another conversion method
  - More efficient
  - See next slide

Base Conversion

- **To construct the base *b* expansion of an integer *n*:**
  - Divide *n* by *b* to obtain a quotient and a remainder.

    $n = bq_0 + a_0 \quad 0 \leq a_0 < b$
  - The remainder, a_0, is the rightmost digit in the base *b* expansion of *n*. Next, divide q_0 by *b*.

    $q_0 = bq_1 + a_1 \quad 0 \leq a_1 < b$
  - 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.**

Base Conversion

- **Example**: Find the hexadecimal expansion of $(175)_{10}$.

  Solution: Successively dividing by 16 gives:

  $175 = 16 \cdot 10 + \mathbf{15}$

  $10 = 16 \cdot 0 + \mathbf{10}$ STOP when quotient is 0.

  15 is the rightmost digit. 15 is F.

  10 is the second digit from the right. 10 is A.

  Hence, $(175)_{10} = (AF)_{16}$.

Base Conversion

- **Example**: Find the binary expansion of $(175)_{10}$.

  Solution: Successively dividing by 2.

$175 = 2 \cdot 87 + \mathbf{1}$

$87 = 2 \cdot 43 + \mathbf{1}$

$43 = 2 \cdot 21 + \mathbf{1}$

$21 = 2 \cdot 10 + \mathbf{1}$

$10 = 2 \cdot 5 + \mathbf{0}$

$5 = 2 \cdot 2 + \mathbf{1}$

$2 = 2 \cdot 1 + \mathbf{0}$

$1 = 2 \cdot 0 + \mathbf{1}$ STOP when quotient is 0.

$(175)_{10} = (10101111)_2$

Base Conversion

- **Example**: Find the hexadecimal expansion of $(177130)_{10}$.

  Solution: Successively dividing by 16.

  $177130 = 16 \cdot 11070 + \mathbf{10}$ **A**

  $11070 = 16 \cdot 691 + \mathbf{14}$ **E**

  $691 = 16 \cdot 43 + \mathbf{3}$ **3**

  $43 = 16 \cdot 2 + \mathbf{11}$ **B**

  $2 = 16 \cdot 0 + \mathbf{2}$. STOP when quotient is 0. **2**

  $$(177130)_{10} = (2B3EA)_{16}$$

Base Conversion

- **Example**: Find the octal expansion of $(12345)_{10}$

  Solution: Successively dividing by 8.

  $12345 = 8 \cdot 1543 + \mathbf{1}$

  $1543 = 8 \cdot 192 + \mathbf{7}$

  $192 = 8 \cdot 24 + \mathbf{0}$

  $24 = 8 \cdot 3 + \mathbf{0}$

  $3 = 8 \cdot 0 + \mathbf{3}$ STOP when quotient is 0.

  The remainders are the digits from right to left yielding $(30071)_8$.

Decimal to Octal

- Similar to converting from decimal to hexadecimal, to convert from decimal to octal:
  - **Step 1:** Decimal -> Binary
  - **Step 2**: Binary -> Octal
    - **Form blocks of 3 binary digits from right to left.**
    - Each octal digit corresponds to a block of 3 binary digits.
    - Conversion between binary and octal is easy.

Binary to Octal

- **Example**: Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$.

Solution:

Form blocks of three from right to left. Add initial 0s as needed.

$(0\underline{11}\ \underline{111}\ \underline{010}\ \underline{111}\ \underline{100})_2$

3 7 2 7 4

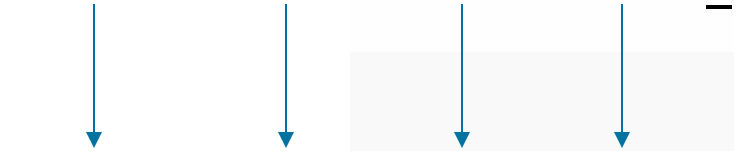
The octal expansion is $(37274)_8$.

Binary to Hexadecimal

Solution cont.:

Form blocks of four from right to left. Add initial 0s as needed.

$$(0011\ 1110\ 1011\ 1100)_2$$



Hence, the solution is $(3EBC)_{16}$.

Algorithms for Integers Operations

- Algorithms for performing operations with integers using their binary expansions are important as computer chips work with binary numbers.
- Each digit is called a *bit*.
- The binary expansions of a and b are

$$a = (a_{n-1}\, a_{n-2}\, \ldots\, a_1\, a_0)_2$$
$$b = (b_{n-1}\, b_{n-2}\, \ldots\, b_1\, b_0)_2$$

- a and b each have n bits. Add initial 0s as need.

Binary Addition Algorithm

- Add pairs of binary digits together with carries, when they occur, to compute the sum of two integers.
- To add a and b, first add their rightmost bits.

$$a_0 + b_0 = c_0 \cdot 2 + s_0$$

$$\begin{array}{r} c_0 \\ a_{n-1}\ a_{n-2}\ \ldots\ a_1\ a_0 \\ b_{n-1}\ b_{n-2}\ \ldots\ b_1\ b_0 \\ \hline s_0 \end{array}$$

s_0 (sum bit): **the rightmost bit** in the binary expansion of $a + b$.

c_0 (carry bit): the **carry**, which is either 0 or 1.

Binary Addition Algorithm

- Then add the next pair of bits and the carry.

$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$$

$$\begin{array}{r} \phantom{a_{n-1}\, a_{n-2}\, \ldots\, a_1\, a_0} \quad c_1\ c_0 \\ a_{n-1}\, a_{n-2}\, \ldots\, a_1\, a_0 \\ b_{n-1}\, b_{n-2}\, \ldots\, b_1\, b_0 \\ \hline \phantom{a_{n-1}\, a_{n-2}\, \ldots\, a_1\, a_0} \quad s_1\ s_0 \end{array}$$

s_1 (sum bit): the next bit in the binary expansion of $a + b$.

c_1 (carry bit): the **carry**, which is either 0 or 1.

Binary Addition Algorithm

- Continue this process to determine the next bit. At the last stage,

$$a_{n-1} + b_{n-1} + c_{n-2} = c_{n-1} \cdot 2 + s_{n-1}$$

$$\begin{array}{r} c_{n-1}\, c_{n-2} \cdots \quad c_1\ c_0 \\ a_{n-1}\, a_{n-2} \ \ldots\ a_1\ a_0 \\ b_{n-1}\, b_{n-2} \ \ldots\ b_1\ b_0 \\ \hline s_{n-1}\ s_{n-2} \cdots \quad s_1\ s_0 \end{array}$$

- The leading bit of the sum is $s_n = c_{n-1}$. The binary expansion of $a + b$ is $(s_n s_{n-1} s_{n-2} \ldots s_1 s_0)_2$.

Binary Addition of Integers

- Binary Addition:

$$\begin{array}{r} 0 \\ +\ 0 \\ \hline 0 \end{array} \qquad \begin{array}{r} 0 \\ +\ 1 \\ \hline 1 \end{array} \qquad \begin{array}{r} 1 \\ +\ 0 \\ \hline 1 \end{array} \qquad \begin{array}{r} 1 \\ +\ 1 \\ \hline 1\ 0 \end{array}$$

carry

Binary Addition of Integers

- **Example**: Add $a = (1110)_2$ and $b = (1011)_2$.

	1	1	1		
		1	1	1	0
+		1	0	1	1
		1	**0**	**0**	**1**

$s = a + b = (\mathbf{1}11001)_2$.

Binary Multiplication of Integers

- Multiply two n-bit integers a and b *u*sing the distributive law.

$$b = (b_0 2^0 + b_1 2^1 + \ldots + b_{n-1} 2^{n-1})$$

$$ab = a(b_0 2^0 + b_1 2^1 + \ldots + b_{n-1} 2^{n-1})$$

$$= a(b_0 2^0) + a(b_1 2^1) + \ldots + a(b_{n-1} 2^{n-1})$$

- **Note that** $ab_j = a$ if $b_j = 1$ and $ab_j = 0$ if $b_j = 0$.

Binary Multiplication of Integers

- Each time we multiply a term by 2, we shift its binary expansion one place to the left and add a zero at the tail end of the expansion.
- Consequently, we can obtain $(ab_j)2^j$ by **shifting** the binary expansion of ab_j j places to the left, adding j zero bits at the tail end of this binary expansion.
- Finally, we obtain ab by adding the n integers $ab_j\ 2^j$, $j = 0, 1, 2, \ldots, n - 1$.

Binary Multiplication of Integers

- **Example:** Find the product of $a = (110)_2$ and $b = (101)_2$.

  Solution:

  $ab = a(b_0 2^0 + b_1 2^1 + b_2 2^2) = a(1 \bullet 2^0 + 0 \bullet 2^1 + 1 \bullet 2^2)$

  $ab_0 2^0 = (110)_2 \bullet 1 \bullet 2^0 = (110)_2$ No shifting

  $ab_1 2^1 = (110)_2 \bullet 0 \bullet 2^1 = (0000)_2$ Shift 1 place to the left

  $ab_2 2^2 = (110)_2 \bullet 1 \bullet 2^2 = (11000)_2$ Shift 2 places to the left

  Add $ab_0 2^0$, $ab_1 2^1$ and $ab_2 2^2$.

```
    00110
    00000
+   11000
-------
    11110
```

Binary Multiplication of Integers

- Binary Addition:

$$\begin{array}{r} 0 \\ +\ 0 \\ \hline 0 \end{array} \qquad \begin{array}{r} 0 \\ +\ 1 \\ \hline 1 \end{array} \qquad \begin{array}{r} 1 \\ +\ 0 \\ \hline 1 \end{array} \qquad \begin{array}{r} 1 \\ +\ 1 \\ \hline 1\ 0 \end{array}$$

carry

- Binary Multiplication:

$$\begin{array}{r} 0 \\ \times\ 0 \\ \hline 0 \end{array} \qquad \begin{array}{r} 0 \\ \times\ 1 \\ \hline 0 \end{array} \qquad \begin{array}{r} 1 \\ \times\ 0 \\ \hline 0 \end{array} \qquad \begin{array}{r} 1 \\ \times\ 1 \\ \hline 1 \end{array}$$

No carry

Binary Multiplication of Integers

- **Example:** Find the product of $a = (110)_2$ and $b = (101)_2$.

			1	1	0
x			1	0	1
			1	**1**	**0**
		0	**0**	**0**	
	1	**1**	**0**		
	1	**1**	**1**	**1**	**0**

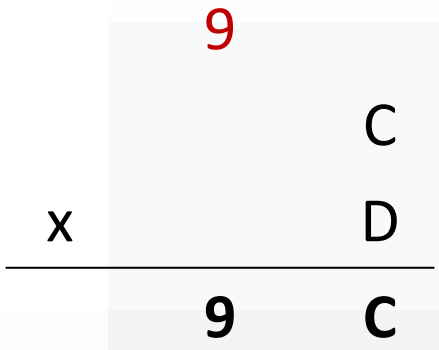
a

b

$ab = (1\ 1110)_2$

Hexadecimal Multiplication of Integers

- Multiply the decimal values of the corresponding bits, and then, convert the product to hexadecimal.
- When a digit-by-digit answer is too large to fit (i.e., greater than 15), we “carry” into the next column.
- For example, C x D = $(12 \times 13)_{10} = 156_{10} = 9C_{16}$.



Hexadecimal Multiplication of Integers

- **Example:** Find the product of $a = (1C)_{16}$ and $b = (2D)_{16}$.

  Solution:

$C \times D = 156_{10} = 9C_{16}$ $(156 \div 16 = 9R12)$
$1 \times D + 9 = 22_{10} = 16_{16}$
$2 \times C = 24_{10} = 18_{16}$
$2 \times 1 + 1 = 3_{10} = 3_{16}$

		9	
		1	C
x	1	2	D
	1	**6**	**C**
	3	**8**	
	4	**E**	**C**

$ab = (4EC)_{16}$

Check: 28(1C) x 45(2D) = 1260(4EC)

Decimal	Hexadecimal
10	A
11	B
12	C
13	D
14	E
15	F

Binary Modular Exponentiation

- In cryptography, 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: $b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \ldots b^{a_1\cdot 2} \cdot b^{a_0}$.
  - To compute b^n, we need only compute the values of b, b^2, $(b^2)^2 = b^4$, $(b^4)^2 = b^8$, . . . , b^{2^k} .
  - Once we have these values, we multiply the terms b^{2^j} in this list, where $a_j = 1$.
  - For efficiency, after multiplying by each term, we **reduce the result modulo *m***. This gives us b^n**.**
  - This method is also called *square* method.

Binary Modular Exponentiation

- Some exponent properties you need to know:

Exponent Properties
$a^b \cdot a^c = a^{b+c}$
$a^b / a^c = a^{b-c}$
$(a^b)^c = a^{b \cdot c}$
$(a \cdot b)^c = a^c \cdot b^c$
$(a / b)^c = a^c / b^c$

Binary Modular Exponentiation

- **Example**: Compute 3^{11}.

  $2^3 \quad 2^2 \quad 2^1 \quad 2^0$
  $(1 \quad 0 \quad 1 \quad 1)_2$

  Solution: Note that $11 = (1011)_2$

  $11 = 1 \cdot 2^3 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 2 + 1$

  $3^{11} = 3^{8+2+1} = 3^8\, 3^2\, 3^1$

  Compute 3^8, 3^2 and 3^1 using the *square* method.

  $3^1 = 3$

  $(3^1)^2 = 3^2 = 9$

  $(3^2)^2 = 3^4 = 81$

  $(3^4)^2 = 3^8 = (81)^2 = 6561$

  Multiply these terms: $3^{11} = 3^8\, 3^2\, 3^1$

  $= 6561 \cdot 9 \cdot 3 = 177{,}147.$

Binary Modular Exponentiation

- **Example**: Compute 3^{11} *mod* 50.

  $2^3 \quad 2^2 \quad 2^1 \quad 2^0$
  $(1 \quad 0 \quad 1 \quad 1)_2$

  Solution: Note that $11 = (1011)_2$

  $11 = 1 \cdot 2^3 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 2 + 1$

  $3^{11} = 3^{8+2+1} = 3^8\, 3^2\, 3^1$

  Compute 3^8, 3^2 and 3^1 using the *square* method and **reduce the result modulo *m***.

  $(3^1) = 3$, 3 *mod* $50 = 3$

  $(3^1)^2 = 9$, 9 *mod* $50 = 9$

  $(3^2)^2 = 3^4 = 9^2 = 81$, 81 *mod* $50 = 31$

  (81 is reduced to 31 modulo 50.)

Binary Modular Exponentiation

Solution cont.:

$(3^4)^2 = 3^8 = 31^2 = 961$, $961 \ mod \ 50 = 11$

(961 is reduced to 11 modulo 50.)

STOP since we have obtained 3^8 , 3^2 and 3^1 .

Multiply these terms:

$3^{11} \ mod \ 50 = 3^8 \ 3^2 \ 3^1 \bmod 50$

$= (11)(9)(3) \bmod 50$

$= 297 \bmod 50$

$= 47 \bmod 50$

$= 47$

Binary Modular Exponentiation

- **Example**: Compute 3^{644} mod 645.

  Solution: Note that 644 = $(1010000100)_2$

  $3^{644} = 3^{512 + 128 + 4} = 3^{512}\ 3^{128}\ 3^{4}$

  $(3^1) = 3$, 3 *mod* 645 = 3

  $(3^1)^2 = 9$, 9 *mod* 645 = 9

  $(3^2)^2 = 3^4 = 9^2 = 81$, 81 *mod* 645 = 81

  $(3^4)^2 = 3^8 = 81^2 = 6561$, 6561 *mod* 645 = *111*

  (6561 is reduced to 111 modulo 645.)

  $(3^8)^2 = 3^{16} = 111^2 = 12321$, 12321 *mod* 645 = *66*

  (12321 is reduced to 66 modulo 645.)

  $(3^{16})^2 = 3^{32} = 66^2 = 4356$, 4356 *mod* 645 = *486*

  (4356 is reduced to 486 modulo 645.)

Binary Modular Exponentiation

Solution cont.:

$(3^{32})^2 = 3^{64} = 486^2 = 236196$, $236196 \; mod \; 645 = 126$

(236196 is reduced to 126 modulo 645.)

$(3^{64})^2 = 3^{128} = 126^2 = 15876$, $15876 \; mod \; 645 = 396$

(15876 is reduced to 396 modulo 645.)

$(3^{128})^2 = 3^{256} = 396^2 = 156816$, $156816 \; mod \; 645 = 81$

(156816 is reduced to 81 modulo 645.)

$(3^{256})^2 = 3^{512} = 81^2 = 6561$, $6561 \; mod \; 645 = 111$

(6561 is reduced to 111 modulo 645.)

Binary Modular Exponentiation

Solution cont.:

$$3^{644} \textit{ mod } 645 = 3^{512 + 128 + 4} \textit{ mod } 645$$

$$= 3^{512}\, 3^{128}\, 3^{4} \textit{ mod } 645$$

$$= (111)(396)(81) \textit{ mod } 645$$

$$= 3{,}560{,}436 \textit{ mod } 645$$

$$= 36 \bmod 645$$

$$= 36$$

3^{644} has the same remainder as 36 when divided by 645.

Binary Modular Exponentiation

- **Example**: Let m be a positive integer. If $a \equiv b$ **(mod** m**)**, is $a^n \equiv b^n$**(mod** m**)**?

Solution: By Theorem 5, sums and products of congruences are valid congruences.

$a \equiv b \pmod 5$
$a \equiv b \pmod 5$
$a \equiv b \pmod 5$
...
$a \equiv b \pmod 5$

} Multiply the n congruences.

$a^n \equiv b^n \pmod 5$.

Binary Modular Exponentiation

- **Example**: Compute 273^{25} **mod** 5.

  Solution 1:$273 \equiv 3 \pmod 5$, then, $273^{25} \equiv 3^{25} \pmod 5$.

$$273^{25} \equiv 3^{25} \pmod 5$$
$$\equiv 3^{24} \cdot 3^{1} \pmod 5$$
$$\equiv (3^{2})^{12} \cdot 3^{1} \pmod 5$$
$$\equiv (9)^{12} \cdot 3^{1} \pmod 5$$
$$\equiv (-1)^{12} \cdot 3^{1} \pmod 5$$

Minus trick! $9 \equiv (-1)$ **(mod** 5)

$$\equiv 1 \cdot 3^{1} \pmod 5$$
$$\equiv 3 \pmod 5$$

273^{25} **mod** 5 = 3 **mod** 5 = 3

Binary Modular Exponentiation

Solution 2:

$$273^{25} \equiv 3^{25} \pmod 5$$

$$\equiv (-2)^{25} \pmod 5$$

$$\equiv (-2)^{24} \cdot (-2)^{1} \pmod 5$$

$$\equiv (4)^{12} \cdot (-2) \pmod 5$$ Minus trick! $4 \equiv (-1)$ **(mod** 5)

$$\equiv (-1)^{12} \cdot (-2) \pmod 5$$

$$\equiv 1 \cdot (-2) \pmod 5$$

$$\equiv -2 \pmod 5$$

$$\equiv 3 \pmod 5$$

273^{25} **mod** 5 = 3 **mod** 5 = 3

Binary Modular Exponentiation

- **4^n mod** 6 table

  $4 \equiv 4 \pmod 6$

  $4^2 = (4)(4) \equiv (4)(4) \pmod 6 = 16 \pmod 6 \equiv 4 \pmod 6$

  $4^3 = (4)(4^2) \equiv (4)(4) \pmod 6 = 16 \pmod 6 \equiv 4 \pmod 6$

  $4^4 = (4)(4^3) \equiv (4)(4) \pmod 6 = 16 \pmod 6 \equiv 4 \pmod 6$

  $4^5 = (4)(4^4) \equiv (4)(4) \pmod 6 = 16 \pmod 6 \equiv 4 \pmod 6$

  …

  $4^n = (4)(4^{n-1}) \equiv (4)(4) \pmod 6 = 16 \pmod 6 \equiv 4 \pmod 6$

- Reduce 4^2 , 4^3, 4^4 or 4^5 to 4 modulo 6.

Binary Modular Exponentiation

- **Example**: Compute 28^{25} **mod** 6.

Solution:

$$28^{25} \equiv (4)^{25} \pmod 6$$
$$\equiv ((4)^5)^5) \pmod 6$$
$$\equiv 4^5 \pmod 6$$
$$\equiv 4 \pmod 6$$

28^{25} **mod** 6 = 4

Binary Modular Exponentiation

- **Example**: Compute 28^{221} **mod** 6.

  Solution:

  $28^{221} \equiv 4^{221} \pmod 6$

  $28^{221} \equiv 4 \,.\, 4^{5 \,.\, 44} \pmod 6$

  $\equiv 4 \,.\, (4)^{44} \pmod 6$

  $\equiv 4^{\,45} \pmod 6$

  $\equiv (4^5)^9 \pmod 6 \equiv 4^9 \pmod 6 \equiv 4^4\, 4^5 \pmod 6$

  $\equiv 4 \cdot 4 \pmod 6 \equiv 4^2 \pmod 6 \equiv 4 \pmod 6$

$4^5 \equiv 4 \pmod 6$
reduce 4^5 to 4 modulo 6

28^{221} **mod** 6 = 4 **mod** 6 = 4

Binary Modular Exponentiation

- **Example**: Compute 226^{229} **mod** 13.

  Solution:

$$226^{229} \equiv 5^{229} \pmod{13} \qquad 226 \equiv 5 \pmod{13}$$

$$\equiv 5^{228+1} \textbf{ (mod } 13)$$

$$\equiv 5^{228} \cdot 5^{1} \textbf{ (mod } 13)$$

$$\equiv (5^{2})^{114} \cdot 5^{1} \textbf{ (mod } 13) \qquad 25 \equiv (-1) \textbf{ (mod } 13)$$

$$\equiv ((-1)^{2})^{57} \cdot 5^{1} \textbf{ (mod } 13)$$

$$\equiv (1)^{57} \cdot 5^{1} \textbf{ (mod } 13)$$

$$\equiv 5 \textbf{ (mod } 13)$$

226^{229} **mod** 13 = 5 **mod** 13 = 5

Binary Modular Exponentiation

- **Example**: Compute 12^{10} **mod** 13.

  Solution:

  $12^{10} \equiv (-1)^{10} \pmod{13}$ Minus trick! $12 \equiv (-1) \pmod{13}$

  $\equiv 1 \pmod{13}$

  $12^{10} \bmod 13 = 1 \bmod 13 = 1$

Primes and Greatest Common Divisors

Section 4.3

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.

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. This is called the prime factorization of n.
- **Examples**:

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$641 = 641$

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Find Prime Factorization of n

- Begin by dividing *n* by successive primes, starting with the smallest prime, 2.
- Partial list of prime numbers:
  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, …

Find Prime Factorization of n

- **Example:** Find the prime factorization of 7007.

  Divide 7007 by successive primes, beginning with 2.

  None of the primes 2, 3, and 5 divides 7007.

  7 divides 7007, with 7007/7 = 1001.

  Divide 1001 by successive primes, beginning with 7.

  7 divides 1001, with 1001/7 = 143.

  Divide 143 by successive primes, beginning with 11.

  11 divide 143, with 143/11 = 13.

  Because 13 is prime, the procedure is completed.

  $7007 = 7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$

Find Prime Factorization of n

- **Example:** Find the prime factorization of 120.

Divide 120 by successive primes, beginning with 2.

2 divides 120, with 120/2 = 60.

2 divides 60, with 60/2 = 30.

2 divides 30, with 30/2 = 15.

Divide 15 by successive primes, beginning with 3.

3 divides 15, with 15/3 = 5.

Divide 5 by successive primes, beginning with 5.

5 divides 5, with 5/5 = 1.

Because 1 is prime, the procedure is completed.

$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$

Find Prime Factorization of n

- **Example:** Find the prime factorization of 500.

  Divide 500 by successive primes, beginning with 2.

  2 divides 500, with 500/2 = 250.

  2 divides 250, with 250/2 = 125.

  3 doesn't divide 125.

  Divide 125 by successive primes, beginning with 5.

  5 divides 125, with 125/5 = 25.

  5 divides 25, with 25/5 = 5.

  Because 5 is prime, the procedure is completed.

  $500 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^2 \cdot 5^3$

Greatest Common Divisor

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

- **gcd(a,b)** can be found
  - By inspection (usually for small numbers)
  - Using Prime Factorizations
  - Using the Euclidean Algorithm
  - By finding gcd(a,b) as a linear combination of a and b.

Find GCD 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 are relatively prime because gcd(17, 22) = 1.

Greatest Common Divisor

- **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.

Greatest Common Divisor

- **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.

Find GCD Using Prime Factorizations

- Suppose the prime factorizations of *a* and *b* are:

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

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*.
- It is time-consuming to find prime factorizations.

Find GCD Using Prime Factorizations

- **Example**: Find the greatest common divisor of 120 and 500.

  Solution:

  $120 = 2^3 \cdot 3 \cdot 5$

  $500 = 2^2 \cdot 5^3$

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

  $= 2^2 \cdot 3^0 \cdot 5^1$

  $= 20$

Least Common Multiple (LCM)

- **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.

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

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

Least Common Multiple (LCM)

- **Example:** What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Solution:

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

$$= 2^4\, 3^5\, 7^2$$

GCD and LCM

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

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

- **Example**:

  $\gcd(\mathbf{2^3}3^5\mathbf{7^2}, 2^4\mathbf{3^3}) = 2^3 3^3$

  $\mathrm{lcm}(2^3\mathbf{3^5 7^2}, \mathbf{2^4}3^3) = 2^4 3^5 7^2$

  $\gcd(2^3 3^5 7^2, 2^4 3^3) \cdot \mathrm{lcm}(2^3 3^5 7^2, 2^4 3^3)$

  $= 2^3 3^5 7^2\, 2^4 3^3$

Euclidean Algorithm

- The Euclidian algorithm is an efficient method for computing the GCD of two integers.
- Based on the idea in **Lemma 1**: Let $a = bq + r$, where a, b, q, and r are integers. Then **gcd(a, b) = gcd(b, r).**
- Use successive divisions to reduce the problem of finding the greatest common divisor of two positive integers to the same problem with smaller integers, until one of the integers is zero.
- The greatest common divisor is the last nonzero remainder.

Euclidean Algorithm

- **Example**: Find gcd(91, 287).

  Solution:

  gcd(91, 287) = gcd(287, 91).

  $a = b \cdot q + r$

  $287 = \underline{91} \cdot 3 + \underline{14}$ Divide 287 by 91.

  $91 = \underline{14} \cdot 6 + \underline{\mathbf{7}}$ **(GCD)** Divide 91 by 14.

  $14 = 7 \cdot 2 + \mathbf{0}$ Divide 14 by 7.

  STOP! $r = 0$.

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

Euclidean Algorithm

- **Example**: Find gcd(414, 662) using the Euclidean algorithm.

Solution: gcd(414, 662) = gcd(662, 414).

$a = b \cdot q + r$

$662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$ **(GCD)**

$82 = 2 \cdot 41 + 0$ **STOP!**

gcd(662, 414) = gcd(414,248) = gcd(248, 166)

gcd(166,82) = gcd(82,2) = 2

Euclidean Algorithm

- **Example**: Find the greatest common divisor of 120 and 500.

  Solution:

  $500 = \underline{120} \cdot 4 + \underline{20}$ **(GCD)**

  $120 = \underline{20} \cdot 6 + 0$ **STOP!**

  $\gcd(500, 120) = \gcd(120, 20) = 20$

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*.
  - Integers *s* and *t:* called *Bézout coefficients* of *a* and *b.*
  - The equation gcd(*a*,*b*) = *sa* + *tb* : called *Bézout's identity.*
  - For example, gcd(6,14) = (−2)·6 + 1·14. *s* = (-2). *t* = 1.

gcds as Linear Combinations

- A general two pass method that can be used to find a linear combination of two integers equal to their greatest common divisor.
  - 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.
- We assume that a linear combination has integer coefficients.

gcds as Linear Combinations

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

Solution:

Pass 1: Use the Euclidean algorithm to show gcd(252,198) = 18.

a) $252 = 198 \cdot 1 + 54$

b) $198 = 54 \cdot 3 + 36$

c) $54 = 36 \cdot 1 + \mathbf{18}$ **(GCD)**

d) $36 = 2 \cdot 18 + 0$

gcds as Linear Combinations

Solution cont.:

Pass 2: Working backwards, from c) to a)above.

Notice that we switch *b* and *q* for convenience.

$a = q \cdot b + r$ instead of $a = b \cdot q + r$. For example,

18 = 54 – 1 · 36 instead of **18** = 54 – 36 · 1.

18 = 54 – 1 · 36 1)

36 = 198 – 3 · 54 2)

54 = **252** – 1 · **198** 3)

To represent 18 as a linear combination of 252 and 198, substitutions are needed.

gcds as Linear Combinations

Solution cont.:

Substitute 2) into 1) yields

$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$ 4)

Substitute 3) into 4) yields

$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 + (-5) \cdot 198$

Hence, gcd(252,198) is a linear combination 252 and 198 such that $18 = s \cdot 252 + t \cdot 198$ where $s = 4$ and $t = -5$.

gcds as Linear Combinations

- **Example**: Express gcd(287,91) = 7 as a linear combination of 287 and 91.

  Solution:

  Pass 1: Use the Euclidean algorithm to show gcd(287,91) = 7

  a) $287 = 91 \cdot 3 + 14$

  b) $91 = 14 \cdot 6 + 7$ (GCD)

  c) $14 = 7 \cdot 2 + 0$

gcds as Linear Combinations

Solution cont.:

Pass 2: Now working backwards, from b) to a) above.

$7 = 91 - 6 \cdot 14$ 1)

$14 = 287 - 3 \cdot 91$ 2)

Substituting 2) into 1) yields

$7 = 91 - 6 \cdot (287 - 3 \cdot 91) = (-6) \cdot 287 + 19 \cdot 91$

Hence, gcd(287,91) is a linear combination 287 and 91 such that $7 = s \cdot 287 + t \cdot 91$ where $s = -6$ and $t = 19$.

Consequences of Bézout's Theorem

- **Lemma 2**: If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

  Proof (optional):

  Assume $\gcd(a, b) = 1$ and $a \mid bc$.

  Since $\gcd(a, b) = 1$, by Bézout's Theorem there are integers s and t such that $sa + tb = 1$.

  Multiplying both sides of the equation by c, yields $sac + tbc = c$.

  Since $a \mid bc$, therefore, $a \mid tbc$. Since $a \mid sac$ and $a \mid tbc$, a divides $sac + tbc$.

  Hence, conclude $a \mid c$, since $sac + tbc = c$.

Dividing Congruence by an Integer

- Lemma 2 can also be used to prove a result about dividing both sides of a congruence by the same integer.
- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence.
  - For example, the congruence $14 \equiv 8 \pmod 6$ holds, but both sides of this congruence cannot be divided by 2 to produce a valid congruence because

    $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod 6$.

Dividing Congruence by an Integer

- **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 $a \equiv b \pmod{m}$.

Proof (optional):
Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$.

$14 \equiv 8 \pmod{6}$

2 is NOT relatively prime to the modulus 6.

Solving Congruences

Section 4.4

Linear Congruences

- **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.

Linear Congruence

- **Definition**: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *in**v**erse* of a modulo m.
- **Example**: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1 \pmod{7}$. $\bar{a} = 5$ is an inverse of 3 modulo 7.
- An inverse of a modulo m is **a *modular multiplicative inverse*** of an integer a.
- One method of solving linear congruences makes use of an inverse $\bar{a}$, if it exists. We can multiply both sides of the congruence by $\bar{a}$ to solve for x.

Inverse of *a* modulo *m*

- **Theorem 1**: **If *a* and *m* are relatively prime integers and *m* > 1**, then an inverse of *a* modulo *m* exists.
- 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*.)
- Theorem 1 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.

Inverse of *a* modulo *m*

- **Proof (optional)**:
  Since gcd(*a*,*m*) = 1, by Bézout's Theorem, there are integers *s* and *t* such that *sa* + *tm* = 1.
  Hence, *sa + tm* ≡ 1 (mod *m*).
  Since *tm* ≡ 0 (mod *m*), it follows that *sa* ≡ 1 (mod *m*).
  Consequently, ***s*** **is an inverse of *a* modulo *m***.

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

Finding Inverses

- **Three steps of finding an inverse of *a modulo m*:**
  - **Step 1:** Check if $\bar{a}$ *modulo m* exists. Use the Euclidean algorithm to find gcd(*a*,*m*) and show gcd(*a*,*m*) = 1. If gcd(*a*,*m*) = 1, $\bar{a}$ exists.
  - **Step 2:** Work backwards from the gcd equation to find the Bézout coefficients of *a* and *m* (gcd(*a*,m) = **s***a* + tm).
  - **Step 3:** Bézout coefficient ***s*** is an inverse of *a modulo m.* Also every integer congruent to **s** *modulo m* is an inverse of *a modulo m.*

Finding Inverses

- **Example**: Find an inverse of 3 modulo 7.

  Solution:

  Step 1: Use the Euclidian algorithm to show gcd(3,7) = 1:

  $7 = 3 \cdot 2 + 1$.

  $3 = 1 \cdot 3 + 0$.

  By Theorem 1, an inverse of 3 modulo 7 exists.

  Step 2: Find Bézout coefficients of 3 and 7. $a = 3$, $m = 7$ and $sa + tm = 1$.

  From the gcd equation $(-2) \cdot 3 + 1 \cdot 7 = 1$, $s = -2$ and $t = 1$.

  Step 3: Hence, -2 is an inverse of 3 modulo 7. Also, every integer congruent to −2 modulo 7 is an inverse of 3 modulo 7, i.e., 5, −9, 12, etc.

Finding Inverses

- **Example**: Find an inverse of 101 modulo 4620.

  Solution:

  Pass 1: Use the Euclidean algorithm to show gcd(101,4620) = 1.

  $4620 = 101 \cdot 45 + 75$

  $101 = 75 \cdot 1 + 26$

  $75 = 26 \cdot 2 + 23$

  $26 = 23 \cdot 1 + 3$

  $23 = 3 \cdot 7 + 2$

  $3 = 2 \cdot 1 + \mathbf{1}$ **(GCD)**

  $2 = 1 \cdot 2 + 0$

  gcd(101, 4260) = 1

Finding Inverses

Solution cont. :

Pass 2: Working Backwards to find the Bézout coefficients. $a = 101$. $m = 4620$. and $sa + tm = 1$.

$1 = 3 - 1 \cdot 2$

$2 = 23 - 7 \cdot 3$

$3 = 26 - 1 \cdot 23$

$23 = 75 - 2 \cdot 26$

$26 = 101 - 1 \cdot 75$

$75 = 4620 - 45 \cdot 101$

Finding Inverses

Solution cont. :

$1 = 3 - 1 \cdot 2$

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

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

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

$= 26 \cdot (101 - 1 \cdot 75) + (-9) \cdot 75 = 26 \cdot 101 + (-35) \cdot 75$

$= 26 \cdot 101 + (-35) \cdot (4620 - 45 \cdot 101)$

$= 1601 \cdot 101 + (-35) \cdot 4620$

$= (-35) \cdot 4620 + 1601 \cdot 101 = 1601 \cdot 101 + (-35) \cdot 4620.$

1601 is an inverse of 101 modulo 4620.

Using Inverses to Solve Congruence

- Use inverses to solve the congruence

  $ax \equiv b \pmod{m}$

  by multiplying both sides by $\bar{a}$.

Using Inverses to Solve Congruence

- **Example**: What are the solutions of the congruence
  $3x \equiv 4 \pmod 7$?

  Solution:

  Use the Euclidean algorithm to show gcd(3,7) = 1, therefore, $\overline{3}$ exists.

  $7 = 2 \cdot 3 + 1$ **(GCD)**

  $2 = 2 \cdot 1 + 0$

  Work backwards to find the Bézout coefficients of 3 and 7. $a = 3$, $m = 7$ and $sa + tm = 1$.

  $-2 \cdot 3 + 7 = 1$ Therefore, $\overline{a} = -2$.

Using Inverses to Solve Congruence

Solution cont.:

Multiply both sides of the congruence by -2 gives

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7 \qquad -2 \cdot 3 \equiv 1 \pmod 7$$

$$x \equiv -8 \pmod 7 \qquad -8 \equiv 6 \pmod 7$$

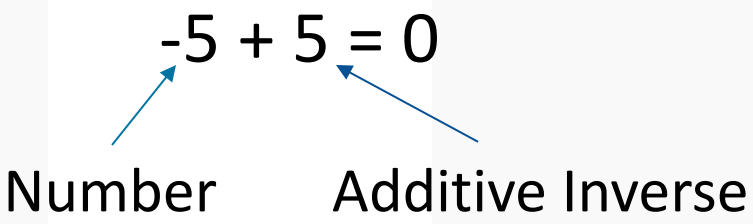
$$x \equiv 6 \pmod 7$$

The solutions are the integers x such that $x \equiv 6 \pmod 7$ namely, $6, 13, 20 \ldots$ and $-1, -8, -15, \ldots$.

Test if every x with $x \equiv 6 \pmod 7$ is a solution. Assume that $x \equiv 6 \pmod 7$ then $3x = 3 \cdot 6 = 18 \equiv 4 \pmod 7$.

Additive inverse of a number

- In mathematics, the additive inverse of a number *a* is the number that, when added to a, yields zero.
- This number is also known as the opposite (number), sign change, and negation.
- For example, 5 is the additive inverse of (-5).



Using Inverses to Solve Congruence

- **Example** : How many times does Bob have to press to meet mom?

  $4 + 5n \equiv 11 \pmod{13}$

Solution:

Add -4, the additive inverse of 4 to both sides.

$4 + 5n \equiv 11 \pmod{13}$

$-4 + 4 + 5n \equiv -4 + 11 \pmod{13}$

$5n \equiv 7 \pmod{13}$

$a = 5$, m = 13, gcd(5,13) = 1, therefore, $\overline{5}$ modulo 13 exists.

Using Inverses to Solve Congruences

Solution cont.:

Find , $\overline{5}$ modulo 13. Use the Euclidean algorithm to show gcd(5,13) = 1.

$13 = 5 \cdot 2 + 3 \quad 3 = 13 - 5 \cdot 2$

$5 = 3 \cdot 1 + 2 \quad 2 = 5 - 3 \cdot 1$

$3 = 2 \cdot 1 + 1 \quad 1 = 3 - \underline{2} \cdot 1$

$2 = 1 \cdot 2 + 0$

Work backwards to find the Bézout coefficients of 5 and 13.

$1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 2 \cdot \underline{3} - 5 = 2 \cdot (13 - 5 \cdot 2) - 5$

$= \mathbf{(-5)} \cdot 5 + 2 \cdot 13$

Using Inverses to Solve Congruences

Solution cont. :

-5 and 2 are Bézout coefficients. s = -5. -5 is $\overline{5}$, an inverse of 5 modulo 13. So are its congruences 8,21, …

Multiply both sides by 8, one of the $\overline{5}$.

$5n \equiv 7 \pmod{13}$

$\overline{5} \cdot 5n \equiv 8 \cdot 7 \pmod{13}$

$n \equiv 56 \pmod{13}$

$n \equiv 4 \pmod{13}$

Therefore, Bob needs to press 4, 17, 30,… times to meet mom.

Using Inverses to Solve Congruence

- **Example** : How many times does Alice have to press to meet mom?

$$5 + 6n \equiv 11 \pmod{13}$$

Solution:

Add -5, the additive inverse of 5 to both sides.

$-5 + 5 + 6n \equiv -5 + 11 \pmod{13}$

$6n \equiv 6 \pmod{13}$

Since gcd(6,13) = 1, $\bar{6}$ exists.

Using Inverses to Solve Congruences

Solution cont. :

Find $\overline{6}$:

Use the Euclidean algorithm to show gcd(6,13) = 1.

$13 = 6 \cdot 2 + 1$

$6 = 1 \cdot 6 + 0$

Work backwards to find the Bézout coefficients of 6 and 13.

$1 = -2 \cdot 6 + 1 \cdot 13$

$\overline{6}$ is -2. $-2 \equiv 11 \pmod{13}$

Using Inverses to Solve Congruences

Solution cont. :

Multiply both sides by $\overline{6}$ (11).

$\overline{6} \cdot 6n \equiv 11 \cdot 6 \pmod{13}$

$\overline{6} \cdot 6n \equiv 66 \pmod{13}$

$n \equiv 66 \pmod{13}$

$n \equiv 1 \pmod{13}$ (66 is congruent to 1 (mod 13).)

Therefore, Alice needs to press 1, 14, 27,… times to meet mom.

Using Inverses to Solve Congruences

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence.
- But dividing by **an integer relatively prime to the modulus** does produce a valid congruence.

Alterative solution (Alice):

$6n \equiv 6 \pmod{13}$

Divide both sides by 6 since 6 and 13 coprime.

$n \equiv 1 \pmod{13}$

Therefore, Alice needs to press 1, 14, 27,… times to meet mom.

Fermat's Little Theorem

- ***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.

Fermat's Little Theorem

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

  Solution:
  $a = 7$ and $p = 11$. 7 is not divisible by 11. By Fermat's little theorem, $7^{10} \equiv 1 \pmod{11}$.

  $(7^{10})^k \equiv 1 \pmod{11}$ 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.

Fermat's Little Theorem

- **Example**: Find $7^{2275} \bmod 13$.

  Solution:

  $a = 7$, $p = 13$. 7 is not divisible by 13. By Fermat's little theorem, $7^{12} \equiv 1 \pmod{13}$.

$$7^{2275} \equiv 7^{12 \cdot 189} \cdot 7^7 \pmod{13}$$

$$\equiv (7^{12})^{189} \cdot 7^7 \pmod{13} \equiv (1)^{189} \cdot 7^7 \pmod{13}$$

$$\equiv 7^7 \pmod{13} \equiv 7^{2 \cdot 3 + 1} \pmod{13}$$

$$\equiv 7 \cdot (7^2)^3 \pmod{13} \equiv 7 \cdot (49)^3 \pmod{13}$$

$$\equiv 7 \cdot (10)^3 \pmod{13} \equiv 7 \cdot (-3)^3 \pmod{13}$$

$$\equiv -7 \cdot 27 \pmod{13} \equiv -7 \cdot 1 \pmod{13} \equiv 6 \pmod{13}$$