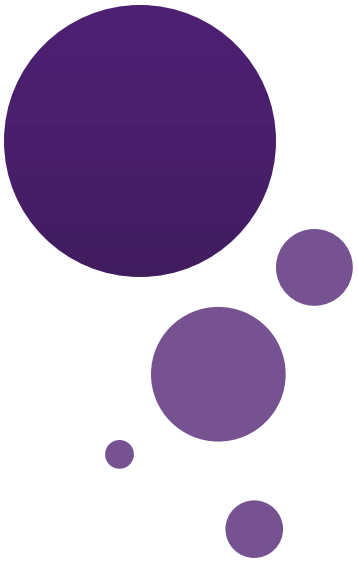


Lecture 18: Integer Representations

Dr. Chengjiang Long
Computer Vision Researcher at Kitware Inc.
Adjunct Professor at SUNY at Albany.
Email: **clong2@albany.edu**

Recap Previous Lecture

- Congruency, and Properties of Mod Function
- Arithmetic of Modulus m
- Applications of Modular Arithmetic

$h(k) = k \bmod m$

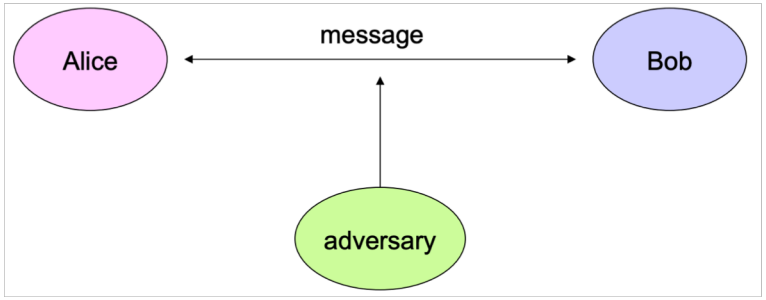
Key: social security #

# of available memory location

Example: h (064212848) = 064212848 mod 111 = 14
when m = 111

$f(p) = (p + 3) \bmod 26 \quad 0 \le p \le 25$

$f(p) = (p + k) \bmod 26$ (shift cepher)
$\Rightarrow f^{-1}(p) = (p - k) \bmod 26$



Outline

- Integer Representations
  - Binary Expansions
  - Octal Expansions
  - Hexadecimal Expansions
- Base Conversion
- Conversion Between Binary, Octal and Hexadecimal Expansion
- Application: Modular Exponentiation

Outline

- **Integer Representations**
  - Binary Expansions
  - Octal Expansions
  - Hexadecimal Expansions
- Base Conversion
- Conversion Between Binary, Octal and Hexadecimal Expansion
- Application: Modular Exponentiation

Representations of Integers

- In the modern world, we use *decimal,* or *base* 10, *notation* to represent integers. For example when we write 965, we mean $9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$.
- 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

Outline

- Integer Representations
  - **Binary Expansions**
  - Octal Expansions
  - Hexadecimal Expansions
- Base Conversion
- Conversion Between Binary, Octal and Hexadecimal Expansion
- Application: Modular Exponentiation

Binary Expansions

- Most computers represent integers and do arithmetic with binary (base 2) expansions of integers. In these expansions, the only digits used are 0 and 1.

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 2 \times 2 = 4$$
$$2^3 = 2 \times 2 \times 2 = 8$$
$$2^4 = 2 \times 2 \times 2 \times 2 = 16$$

Binary Expansions

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

Binary Expansions

- **Example**: What is the decimal expansion of the integer that has $(11011)_2$ as its binary expansion?
- **Solution**:
- $(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 27.$

Outline

- Integer Representations
  - Binary Expansions
  - **Octal Expansions**
  - Hexadecimal Expansions
- Base Conversion
- Conversion Between Binary, Octal and Hexadecimal Expansion
- Application: Modular Exponentiation

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

Outline

- Integer Representations
  - Binary Expansions
  - Octal Expansions
  - **Hexadecimal Expansions**
- Base Conversion
- Conversion Between Binary, Octal and Hexadecimal Expansion
- Application: Modular Exponentiation

Hexadecimal Expansions

- The hexadecimal expansion needs 16 digits, but our decimal system provides only 10. So letters are used for the additional symbols. 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.

Hexadecimal Expansions

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

Outline

- Integer Representations
  - Binary Expansions
  - Octal Expansions
  - Hexadecimal Expansions
- **Base Conversion**
- Conversion Between Binary, Octal and Hexadecimal Expansion
- Application: Modular Exponentiation

Base Conversion

To construct the base b expansion of an integer n:

- Divide n by b to obtain a **quotient** and **remainder**.
  $n = bq_0 + a_0 \quad 0 \leq a_0 \leq b$
- The remainder, a_0 , is the rightmost digit in the base b expansion of n. Next, divide q_0 by b.
  $q_0 = bq_1 + a_1 \quad 0 \leq a_1 \leq b$
- 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.

- Could we construct expansion of any integer base?

Base Conversion

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

Solution: Successively dividing by 8 gives:

- $12345 = 8 \cdot 1543 + 1$
- $1543 = 8 \cdot 192 + 7$
- $192 = 8 \cdot 24 + 0$
- $24 = 8 \cdot 3 + 0$
- $3 = 8 \cdot 0 + 3$

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

Outline

- Integer Representations
  - Binary Expansions
  - Octal Expansions
  - Hexadecimal Expansions
- Base Conversion
- **Conversion Between Binary, Octal and Hexadecimal Expansion**
- Application: Modular Exponentiation

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, we group the digits into blocks of three $(011\ 111\ 010\ 111\ 100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,7,2,7, and 4. Hence, the solution is $(37274)_8$.
- To convert to hexadecimal, we group the digits into blocks of four $(0011\ 1110\ 1011\ 1100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,E,B, and C. Hence, the solution is $(3EBC)_{16}$.

Outline

- Integer Representations
  - Binary Expansions
  - Octal Expansions
  - Hexadecimal Expansions
- Base Conversion
- Conversion Between Binary, Octal and Hexadecimal Expansion
- **Application: Modular Exponentiation**

Modular Exponentiation

- Modular exponentiation $c \equiv b^n \pmod{m}$, where b, n and m are positive integers is very important for the cryptography because:
  - if $b < m$ there is unique solution of the congruency,
  - it is relatively easy to to find the solution even for big numbers, but the inverse logarithmic problem is much more complicated.

Modular Exponentiation

- In cryptography it is common that b is 256-bit binary number (77 decimal digits) and n is 3 decimal digits long. Than b^n is a number of several thousands decimal digit.
- Special algorithms are required for such computations.

Example

- Consider small numbers first. Let $b = 13$, $n = 5$, $m = 21$. Calculate $b^n \bmod m$. We may think about exponentiation as a sequence of multiplications:
- $(13^4 \times 13) \bmod 21 = ((13^4 \bmod 21) \times (13 \bmod 21)) \bmod 21$
- In turn, $13^4 \bmod 21 = ((13^2 \bmod 21) \times (13^2 \bmod 21)) \bmod 21$
- The same about $13^2 \bmod 21$. Thus we may reduce power to two and numbers involved to 20 (21-1 because of mod operations).
- To do this, consider n as sum of powers 2: $n = 5_{10} = 101_2$
- a1 mod m = 13 a2 mod m = (13 x 13) mod 21 = 169 mod 21 = 1 a4 mod m = (1 x 1) mod 21 = 1
- **Solution:** ((b1 mod m) x (b4 mod m)) mod m = (13 x 1) mod m = 13.

Binary Modular Exponentiation

- In general, to to compute b^n we may use the binary expansion of n, $n = (a_{k-1},\ldots,a_1,a_0)_2$. Than

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \ldots b^{a_1\cdot 2} \cdot b^{a_0}.$$

- Therefore, 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 the multiply the terms b^{2^j} in this list, where $a_j = 1$.

$O((\log m)^2 \log n)$ bit operations are used to find $b^n \bmod m$.

Binary Modular Exponentiation

- In general, to to compute b^n we may use the binary expansion of n, $n = (a_{k-1},\ldots,a_1,a_0)_2$. Than

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \ldots b^{a_1\cdot 2} \cdot b^{a_0}.$$

- Therefore, 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 the multiply the terms b^{2^j} in this list, where $a_j = 1$.

$O((\log m)^2 \log n)$ bit operations are used to find $b^n \bmod m$.

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j*** ***8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175$
- d: records the temporal result, starting from the rightmost factor.
- t: represents the next term b^{2^j} where b = 175 in this example.

- j = 1, **$175 \bmod 257$** = 175

  $175^2 \bmod 257 = 42$

  d ← 175, t ← 42.

Practice: $175^{235} \bmod 257$

- $235 = 128 + 64 + 32 + 8 + 2 + 1 = (11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times \mathbf{175^2 \times 175}$

- j = 2, $175^2 \times 175 \bmod 257 = (175^2 \bmod 257) \times (175 \bmod 257) \bmod 257 = t \times d \bmod 257 = 42 \times 175 \bmod 257 = 154$
- $175^4 \bmod 257 = (175^2 \bmod 257)^2 \bmod 257$
- $= t \times t \bmod 257$
- $= 42 \times 42 \bmod 257 = 222$
-
- **d ← $175^2 \times 175 \bmod 257 = 154$**
- **t ← $175^4 \bmod 257 = 222$**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = (11101011)2.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times \mathbf{175^{2} \times 175}$

- j = 3, **no factor 175^{4}.**
- $175^{8} \bmod 257 = (175^{4} \bmod 257)^{2} \bmod 257$
- $= t \times t \bmod 257$
- $= 222 \times 222 \bmod 257 = 197$
-
- **d ← $175^{2} \times 175 \bmod 257 = 154$**
- **t ← $175^{8} \bmod 257 = 197$**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times \mathbf{175^8 \times 175^2 \times 175}$

- j = 4, $\mathbf{175^8 \times 175^2 \times 175} \bmod 257 = (175^8 \bmod 257) \times (\mathbf{175^2 \times 175} \bmod 257) \bmod 257 = t \times d \bmod 257 = 197 \times 154 \bmod 257 = 12$
- $175^{16} \bmod 257 = (175^8 \bmod 257)^2 \bmod 257$
- $= t \times t \bmod 257$
- $= 197 \times 197 \bmod 257 = 2$
- **d ← $175^8 \times 175^2 \times 175$** mod 257 = 12
- **t ← 175^{16} mod 257 = 2**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times \mathbf{175^8 \times 175^2 \times 175}$

- j = 5, no factor $\mathbf{175^{16}}$
- 175^{32} mod 257 = $(175^{16}$ mod 257$)^2$ mod 257
- = t x t mod 257
- = 2 x 2 mod 257 = 4
- **d ← 175^8 x175^2 x175** mod 257 = 12
- **t ← 175^{32} mod 257 = 14**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times \mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175}$

- j = 6, $\mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175}$ mod 257 = (175^{32} mod 257) x ($\mathbf{175^{8} \times 175^{2} \times 175}$ mod 257) mod 257 = t x d mod 257 = 4 x 12 mod 257 = 48

- 175^{64} mod 257 = (175^{32} mod 257)^2 mod 257
- = t x t mod 257
- = 4 x 4 mod 257 = 16
- **d ← $175^{32} \times 175^{8} \times 175^{2} \times 175$ mod 257 = 48**
- **t ← 175^{64} mod 257 = 16**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times \mathbf{175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175}$

- j = 7, $\mathbf{175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175}$ mod 257 = (175^{64} mod 257) x ($\mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175}$ mod 257) mod 257 = t x d mod 257 = 16 x 48 mod 257 = 254

- 175^{128} mod 257 = (175^{64} mod 257)^2 mod 257
- = t x t mod 257
- = 16 x 16 mod 257 = 256
- **d ← $175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175$ mod 257 = 48**
- **t ← 175^{128} mod 257 = 256**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = \mathbf{175^{128}\ x175^{64}\ x175^{32}\ x175^{8}\ x175^{2}\ x175}$

- j = 8, $\mathbf{175^{128}\ x\ 175^{64}\ x175^{32}x175^{8}\ x175^{2}\ x175}$ mod 257 = (175^{128} mod 257) x ($\mathbf{175^{64}\ x\ 175^{32}x\ 175^{8}\ x\ 175^{2}\ x175}$ mod 257) mod 257 = t x d mod 257 = 256 x 254 mod 257 =3

- 175^{128} mod 257 = $(175^{64}$ mod $257)^2$ mod 257
- = t x t mod 257
- = 16 x 16 mod 257 = 256
- **d ← 175^{128} x 175^{64} x 175^{32}x175^{8} x175^{2} x175 mod 257 = 3**
- **return d.**

Analysis on d and t (1)

- d = $175 \bmod 257$
- d = $175^2 \times 175 \bmod 257$
- d = $175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{64} \times 175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{128} \times 175^{64} \times 175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$

$d = t \times d \bmod 257$ when $t = \mathbf{175^k}$ **and** $\mathbf{k = 2^{j-1}}$

Analysis on d and t (2)

- $t = 175^2 \bmod 257 = 42$
- $t = 175^4 \bmod 257 = (175^2 \bmod 257)^2 \bmod 257 = 222$
- $t = 175^8 \bmod 257 = (175^4 \bmod 257)^2 \bmod 257 = 197$
- $t = 175^{16} \bmod 257 = (175^8 \bmod 257)^2 \bmod 257 = 2$
- $t = 175^{32} \bmod 257 = (175^{16} \bmod 257)^2 \bmod 257 = 4$
- $t = 175^{64} \bmod 257 = (175^{32} \bmod 257)^2 \bmod 257 = 16$
- $t = 175^{128} \bmod 257 = (175^{64} \bmod 257)^2 \bmod 257 = 256$

$$t = t^2 \bmod 257$$

Practice: $175^{235} \bmod 257$

- $235_{10} = 11101011_2$.
- *1*. d := 1 × 175 mod 257 = 175, t := 175^2 mod 257 = 42;
- *2*. d := 175 × 42 mod 257 = 154, t := 42^2 mod 257 = 222;
- *3*. t := 222^2 mod 257 = 197;
- *4*. d := 154 × 197 mod 257 = 12, t := 197^2 mod 257 = 2;
- *5*. t := 2^2 mod 257 = 4;
- *6*. d := 12 × 4 mod 257 = 48, t := 4^2 mod 257 = 16;
- *7*. d := 48 × 16 mod 257 = 254, t := 16^2 mod 257 = 256;
- *8*. d := 254 × 256 mod 257 = 3
- ***Return* d = 3**

Next class

- Topic: Primes and Greatest Common Divisors
- Pre-class reading: Chap 4.3