Lecture 20: Integer Representations and Algorithms

Jingjin Yu |Computer Science @ Rutgers

November 20, 2020

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

Algorithmic Robotics & Control Lab

Outline

- Lecture 19 review
- Base b representation
  - From decimal to base b
  - From base b to decimal
  - Between binary, octal, and hexadecimal
- Binary computations
  - Addition and subtraction
  - Multiplication and division
- Modular exponentiation

- A repeating note: **make sure you read the textbook**

L19: Number Theory & Divisibility

- A **key goal** of Lecture 19 is to build up to **Theorem 5** and **Corollary 6**, which are really "**algorithms**" for helping with computation of modular arithmetic.

- **Def^n: Number theory** is the part of mathematics devoted to the study of integers.

- **Def^n: Divisibility**. Let a and b be integers. Then, a **divides** b if $b = ac$ for some integer c. Otherwise, a does not divide b.
  - Notation: a divides b: $a \mid b$, a does not divide b: $a \nmid b$
  - If $a \nmid b$, $b = aq + r$ for some integers q (**quotient**) and $0 < r < b$ (**remainder**)

- **Ex**: $a = 4, b = 12$. $a \mid b$?
- **Ex**: $a = 3, b = 10$. $a \mid b$?

L19: Properties on Divisibility

- **Theorem 1.** a, b, and c are integers and $a \neq 0$. Then:
  - (i) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  - (ii) If $a \mid b$, then $a \mid bc$ for all integers c.
  - (iii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

- **Theorem 2.** a and $d > 0$ are integers. Then there are **unique** integers q and r with $0 \leq r < d$ s.t. $a = dq + r$.

- **Ex:** $a = 47, d = 8$.
- **Ex:** $a = -14, d = 5$.

L19: Modular Arithmetic

- Notation: $a \bmod m$ is the remainder of a divided by m.
- **Def^n**: Let a and b be integers and m a positive integer. We say **a is congruent to b modulo m** if $m \mid (a - b)$.
  - Notations:
    - $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$
    - $a \not\equiv b \pmod{m}$ if and only if $m \nmid (a - b)$
- **Theorem 3.** a, b, and $m > 0$ are integers. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$
- **Ex**: $a = 17, b = 5, m = 6$. $a \equiv b \pmod{m}$?
- **Ex**: $a = 24, b = 516, m = 6$. $a \equiv b \pmod{m}$?

L19: More Properties

- **Theorem 4.** $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some integer k.

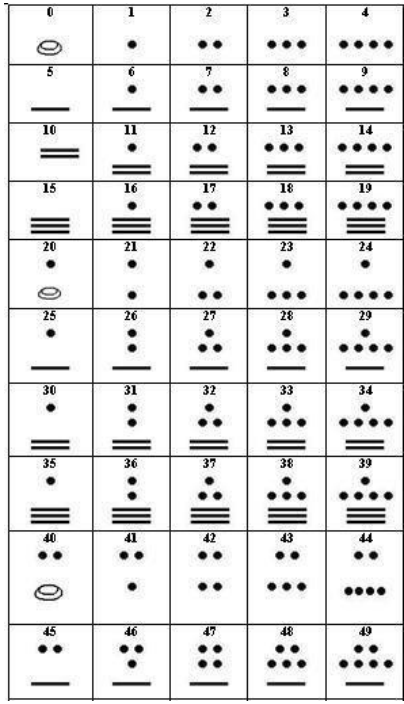
- **Theorem 5.** $m > 0$ is an integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
- **Ex:** $m = 7, a = 11, b = 18, c = 22, d = 8$

- **Corollary 6.** a, b and $m > 0$ are integers. Then
  - $(a + b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m.$
  - $(ab) \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m.$
- **Ex:** $a = 13241, b = 479, m = 3.$
  - $(a + b) \bmod m = ?$
  - $(ab) \bmod m = ?$

Representing Integers

- For everyday: decimals are **base 10** representations.

89546 2222



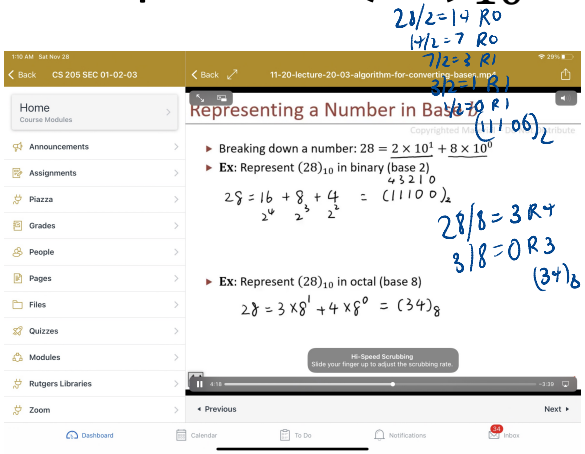
  - Why do we use decimal numbers?
  - Mayans use base 20 and base 5
- We can use any positive integer as the base
  - Base 1: unary numbers, e.g., $(1111111)_1$
  - Base 2: binary numbers, e.g., $(0010\ 1110)_2$
  - Base 3: ternary
  - Base 8: octal
  - Base 16: hexadecimal

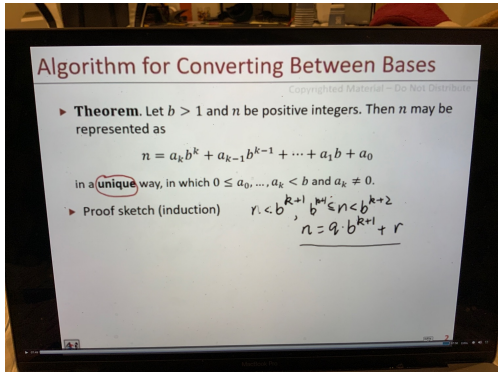
Representing a Number in Base b

- Breaking down a number: $28 = 2 \times 10^1 + 8 \times 10^0$
- **Ex**: Represent $(28)_{10}$ in binary (base 2)

$28 = 16 + 8 + 4 = (11100)_2$

- **Ex**: Represent $(28)_{10}$ in octal (base 8)





Algorithm for Converting Between Bases

- **Theorem.** Let $b > 1$ and n be positive integers. Then n may be represented as

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

in a **unique** way, in which $0 \leq a_0, \ldots, a_k < b$ and $a_k \neq 0$.

- Proof sketch (induction)

Convert from Base b to Base 10

- **Algorithm** for converting from base b to base 10: simply compute the polynomial!
- **Ex:** $(101011111)_2$ to base 10

$8\,7\,6\,5\,4\,3\,2\,1\,0$

$2^8 + 2^6 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 351$

- **Ex:** $(7016)_8$ to base 10

$3\,2\,1\,0$

$7 \times 8^3 + 1 \times 8^1 + 6 = 3598$

$(7016)_8$

$8^0 \times 6 + 8^1 \times 1 + 8^3 \times 7$

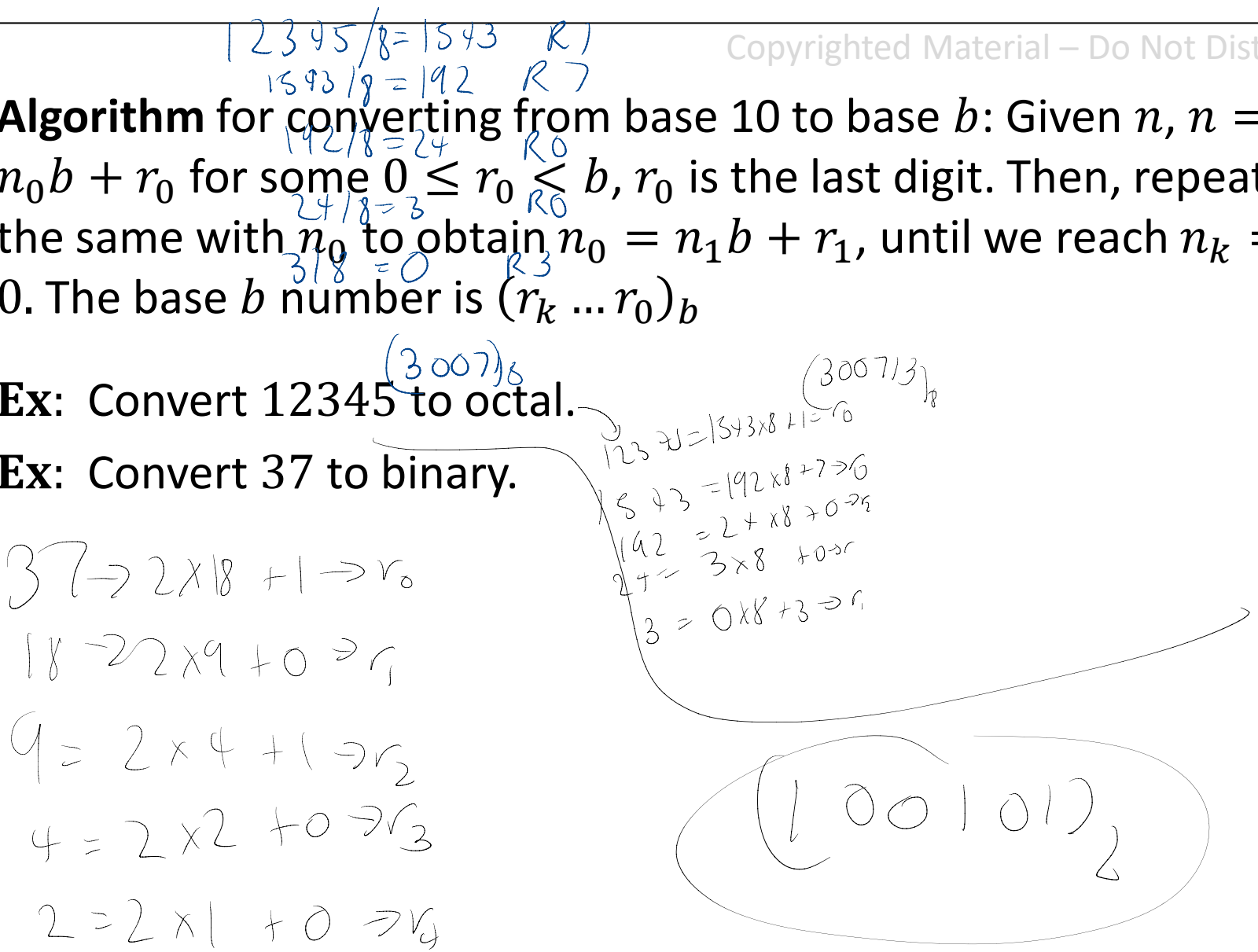
- **Ex:** $(A7E)_{16}$ to base 10

$A \times 16^2 + 7 \times 16 + E \times 1 = 2686$

$16^0 \times 14 + 16 \times 7 + 16^2 \times 10$

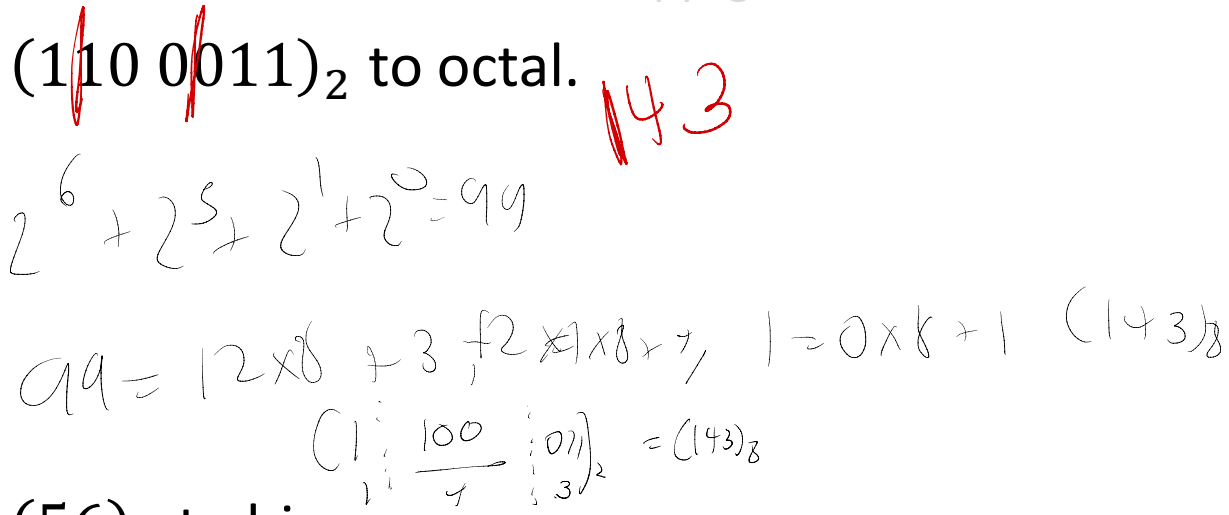
Convert from Base 10 to Base b

- **Algorithm** for converting from base 10 to base b: Given n, $n = n_0 b + r_0$ for some $0 \leq r_0 < b$, r_0 is the last digit. Then, repeat the same with n_0 to obtain $n_0 = n_1 b + r_1$, until we reach $n_k = 0$. The base b number is $(r_k \ldots r_0)_b$
- **Ex**: Convert 12345 to octal.
- **Ex**: Convert 37 to binary.

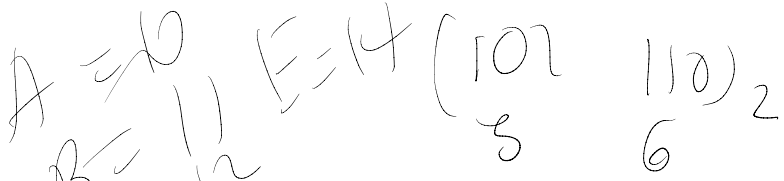


Convert between Binary, Octal, Hexadecimal

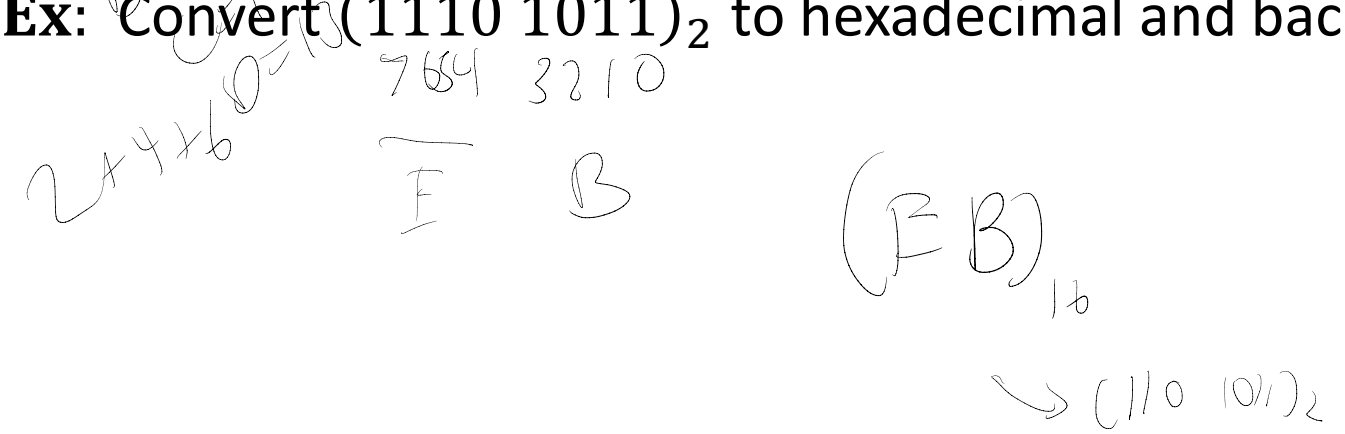
- **Ex:** Convert $(110\ 0011)_2$ to octal.



- **Ex:** Convert $(56)_8$ to binary.

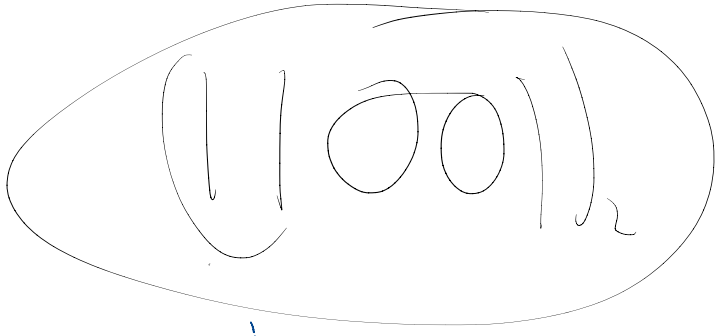


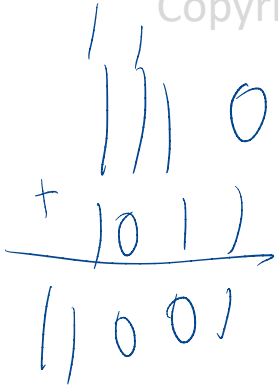
- **Ex:** Convert $(1110\ 1011)_2$ to hexadecimal and back.



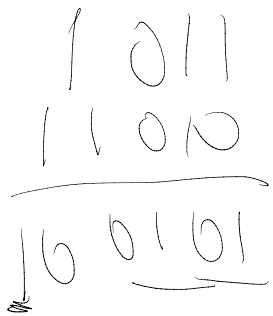
Binary Addition and Subtraction

- **Ex:** $1110_2 + 1011_2$



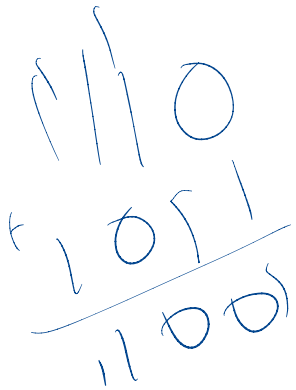


- **Ex:** $1011_2 - 101_2$

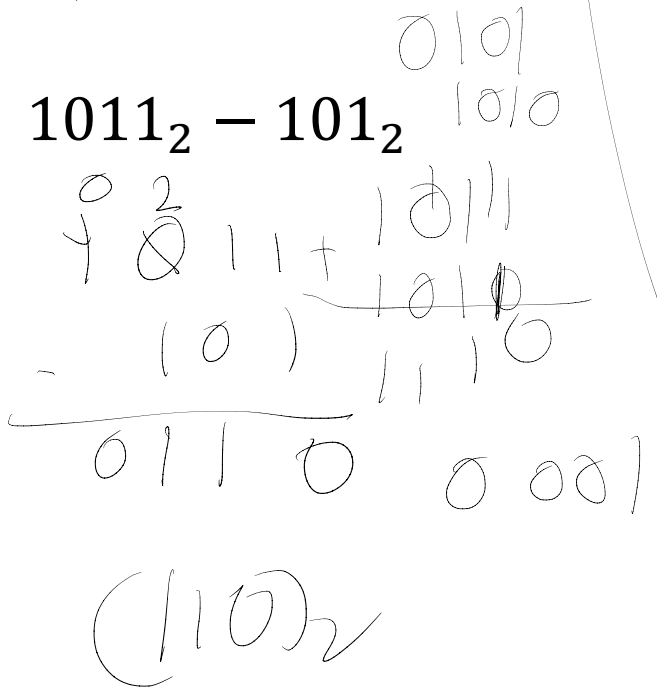


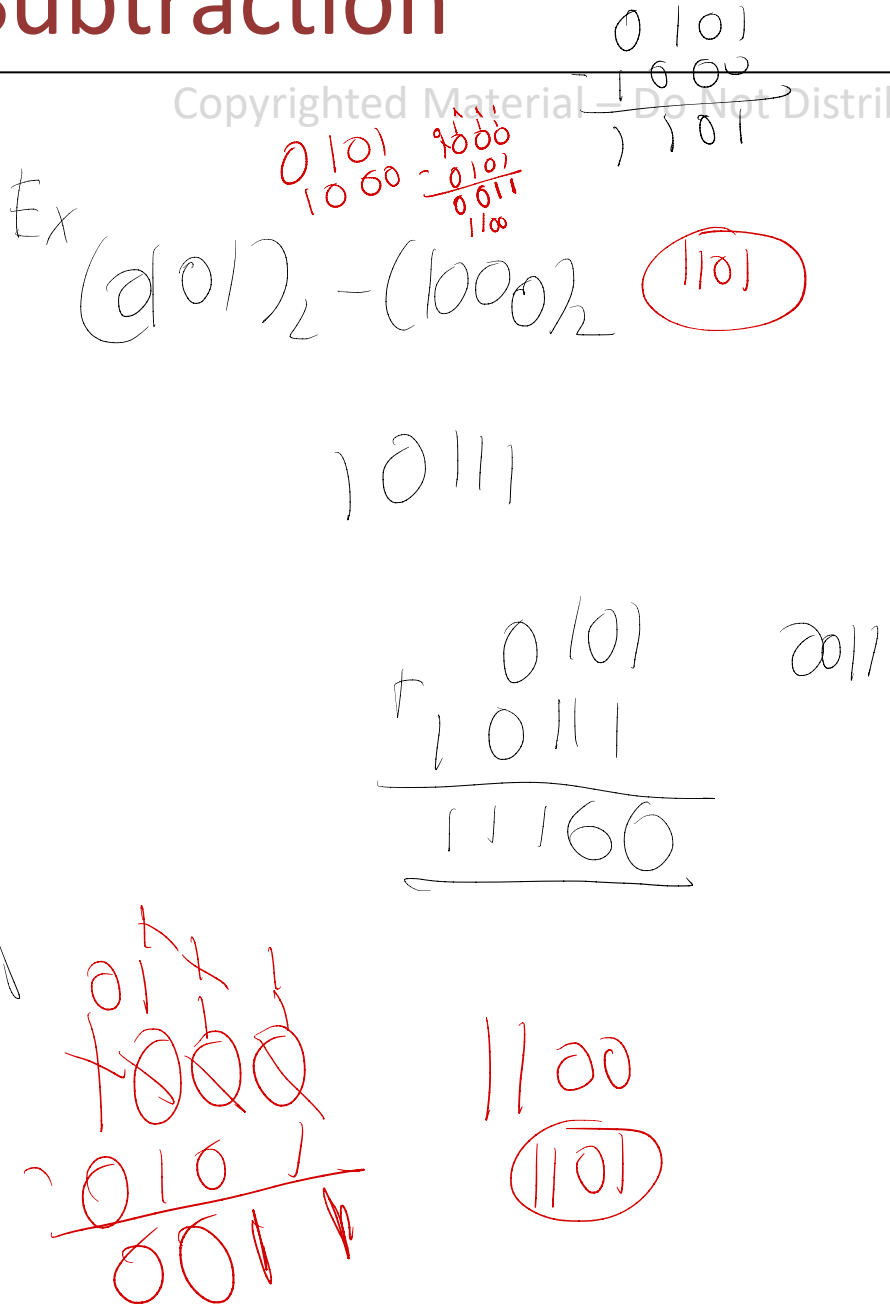
Binary Addition and Subtraction

- **Ex:** $1110_2 + 1011_2$



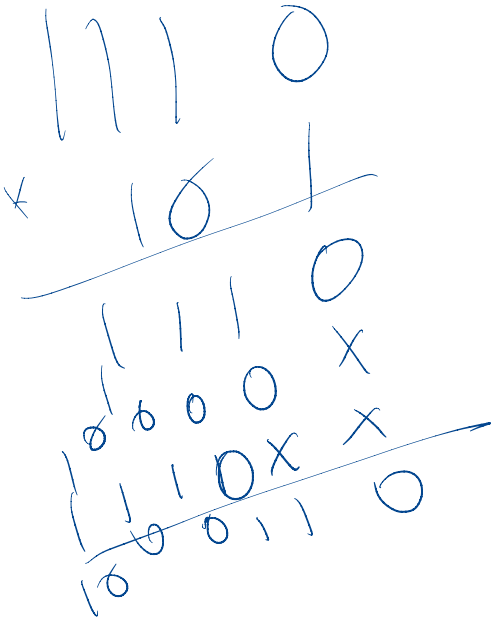
- **Ex:** $1011_2 - 101_2$

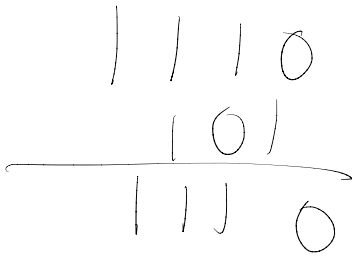


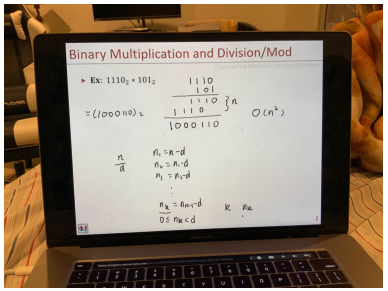


Binary Multiplication and Division/Mod

- **Ex:** $1110_2 * 101_2$







Modular Exponentiation

- **Ex:** $5^{11} \bmod 7$