## **Sketch of Lecture 13**

**Example 78. (ISBN)** The International Standard Book Number ISBN-10 consists of nine digits  $a_1a_2...a_9$  followed by a tenth check digit  $a_{10}$  (the symbol X is used if the digit equals 10), which satisfies

$$a_{10} \equiv \sum_{k=1}^{9} ka_k \pmod{11}.$$

The ISBN 006085396-? is missing the check digit (printed as "?"). Compute it!

**Solution.**  $1 \cdot 0 + 2 \cdot 0 + 3 \cdot 6 + 4 \cdot 0 + 5 \cdot 8 + 6 \cdot 5 + 7 \cdot 3 + 8 \cdot 9 + 9 \cdot 6 = 88 + 21 + 72 + 54 \equiv 4 \pmod{11}$ Hence, the full ISBN is 0060853964.

5.1 Representations of integers in different bases

**Example 79.**  $25 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ . We write  $25 = (11001)_2$ .

**Example 80.** We are commonly using the **decimal system** of writing numbers:

 $1234 = 4 \cdot 10^0 + 3 \cdot 10^1 + 2 \cdot 10^2 + 1 \cdot 10^3.$ 

10 is called the base, and 1, 2, 3, 4 are the digits in base 10. To emphasize that we are using base 10, we will write  $1234 = (1234)_{10}$ . Likewise, we write

$$(1234)_b = 4 \cdot b^0 + 3 \cdot b^1 + 2 \cdot b^2 + 1 \cdot b^3.$$

In this example, b > 4, because, if b is the base, then the digits have to be in  $\{0, 1, ..., b - 1\}$ .

**Example 81.** Express 25 in base 2.

Solution. We already noticed that  $25 = 16 + 8 + 1 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ . Hence,  $25 = (11001)_2$ . Alternatively, here's how we could have determined the digits without prior knowledge:

- $25 = 12 \cdot 2 + 1$ . Hence,  $25 = (...1)_2$  where ... are the digits for 12.
- $12 = 6 \cdot 2 + 0$ . Hence,  $25 = (...01)_2$  where ... are the digits for 6.
- $6=3\cdot 2+0$ . Hence,  $25=(...001)_2$  where ... are the digits for 3.
- $3 = 1 \cdot 2 + 1$ , with 1 left over. Hence,  $25 = (11001)_2$ .

**Example 82.** Express 49 in base 2.

Solution.

- $49 = 24 \cdot 2 + 1$ . Hence,  $49 = (...1)_2$  where ... are the digits for 24.
- $24 = 12 \cdot 2 + 0$ . Hence,  $49 = (...01)_2$  where ... are the digits for 12.
- $12 = 6 \cdot 2 + 0$ . Hence,  $49 = (...001)_2$  where ... are the digits for 6.
- $6 = 3 \cdot 2 + 0$ . Hence,  $49 = (...0001)_2$  where ... are the digits for 3.
- $3 = 1 \cdot 2 + 1$ , with 1 left over. Hence,  $49 = (110001)_2$ .

Other bases. What is 49 in base 3?  $49 = 16 \cdot 3 + 1$ ,  $16 = 5 \cdot 3 + 1$ ,  $5 = 1 \cdot 3 + 2$ , 1. Hence,  $49 = (1211)_3$ . What is 49 in base 7?  $49 = (10)_7$ .

**Example 83.** Bases 2, 8 and 16 (binary, octal and hexadecimal) are commonly used in computer applications.

For instance, in JavaScript or Python, 0b... means  $(...)_2$ , 0o... means  $(...)_8$ , and 0x... means  $(...)_{16}$ .

The digits 0, 1, ..., 15 in hexadecimal are typically written as 0, 1, ..., 9, A, B, C, D, E, F.

**Problem.** Which number is 0xD1?

**Solution.**  $0xD1 = 13 \cdot 16 + 1 = 209.$ 

The South Alabama Jaguar NCAA team color code is 0xD11241. That means RGB(209, 18, 65), where each value (ranging from 0 to 255) quantifies the amount of red (R), green (G) and blue (B).

For instance, 0x000000 is black, and 0xFF0000 is red, and 0xFFFFFF is white.

We can thus see that the color 0xD11241 is close to a red (though not a pure one).

**Example 84.** (divisibility by 9) A number  $n = (a_m a_{m-1} \cdots a_0)_{10}$  is divisible by 9 if and only if the sum of its decimal digits  $a_m + a_{m-1} + \ldots + a_0$  is divisible by 9.

Why? Note that  $10^r \equiv 1^r \equiv 1 \pmod{9}$  for any integer  $r \ge 0$ .

In particular,  $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10^1 + a_0 \equiv a_m + a_{m-1} + \ldots + a_1 + a_0 \pmod{9}$ .

For instance. 1234567 is not divisible by 9 because  $1 + 2 + 3 + ... + 7 = \frac{7(7+1)}{2} = 28$  is not divisible by 9. In fact,  $1234567 \equiv 28 \equiv 1 \pmod{9}$ .

**Example 85.** (divisibility by 11) A number  $n = (a_m a_{m-1} \cdots a_0)_{10}$  is divisible by 11 if and only if the alternating sum of its decimal digits  $(-1)^m a_m + (-1)^{m-1} a_{m-1} + \ldots + a_0$  is divisible by 11.

Why? Note that  $10^r \equiv (-1)^r \pmod{11}$  for any integer  $r \ge 0$ . In particular,

 $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10^1 + a_0 \equiv (-1)^m a_m + (-1)^{m-1} a_{m-1} + \ldots - a_1 + a_0 \pmod{11}.$ For instance. 123456 is not divisible by 11 because 6 - 5 + 4 - 3 + 2 - 1 = 3 is not divisible by 11. In fact, 123456  $\equiv 3 \pmod{11}$ .

**Example 86.** Using binary exponentiation, compute  $5^{49} \pmod{105}$ .

**Solution.** Recall that  $49 = (110001)_2 = 2^0 + 2^4 + 2^5$ .  $5^1 = 5, 5^2 = 25, 5^4 = 25^2 = 625 \equiv -5, 5^8 \equiv (-5)^2 = 25, 5^{16} \equiv 25^2 \equiv -5, 5^{32} \equiv (-5)^2 = 25$ Hence,  $5^{49} = 5^{32} \cdot 5^{16} \cdot 5^1 \equiv 25 \cdot (-5) \cdot 5 \equiv 5$ .

Alternative solution. If we prefer, we can be a tiny bit more efficient by computing the binary expansion and powers at once:

 $5^{49} = 5 \cdot 5^{2 \cdot 24} = 5 \cdot 25^{24} = 5 \cdot (25^2)^{12} \equiv 5 \cdot (-5)^{12} = 5 \cdot 25^6 = 5 \cdot (25^2)^3 \equiv 5 \cdot (-5)^3 \equiv -5$