

LAB 6

Base-26

EXPERIMENT 6.1. Let $n = 287,472,347,234$.

(a) Find s_0, \dots, s_{12} such that we can write n as

$$s_0 \times 10^0 + s_1 \times 10^1 + s_2 \times 10^2 + s_3 \times 10^3 + \dots + s_{12} \times 10^{12}.$$

This is the *base ten* expansion of n .

(b) Compute $\text{REM}(n, 10)$. What do you get?

(c) Compute $n_1 = (n - \text{REM}(n, 10))/10$. Was it an accident that you got an integer?

(d) Suppose we keep going. Find $n_j = (n_{j-1} - \text{REM}(n_{j-1}, 10))/10$ for $j = 2, \dots, 12$ without doing any computations.

EXPERIMENT 6.2. Keep $n = 287, 472, 347, 234$ from Experiment 6.1.

(a) Let $s_0 = \text{REM}(n, 26)$ and set $n_1 = (n - s_0)/26$. Compute $s_1 = \text{REM}(n_1, 26)$.

(b) For $j = 2, \dots, 12$, set $n_j = (n_{j-1} - s_{j-1})/26$ and $s_j = \text{REM}(n_j, 26)$. Make a table of all the s 's and n 's.

(c) Compute

$$s_0 \times 26^0 + s_1 \times 26^1 + s_2 \times 26^2 + \cdots + s_{10} \times 26^{10} + s_{11} \times 26^{11}.$$

What did you get? This is called the *base 26 expansion* of n .

(d) Compute the base 26 expansion of $m = 235, 823, 443$.

You can now use the `IntegerDigits` command to find base-10 or base-26 digits of a number.

EXPERIMENT 6.3. Now we want to turn words into numbers using base 26 expansions. Consider the word **CRYPTOLOGY**. Using our usual numbering for the alphabet, we can think of this as

$$\begin{array}{cccccccccc} \text{C} & \text{R} & \text{Y} & \text{P} & \text{T} & \text{O} & \text{L} & \text{O} & \text{G} & \text{Y} & = \\ 2 & 17 & 24 & 15 & 19 & 14 & 11 & 14 & 6 & 24 & = \end{array}$$

$$2 \times 26^0 + 17 \times 26^1 + 24 \times 26^2 + \cdots + 14 \times 26^7 + 6 \times 26^8 + 24 \times 26^9$$

An important note is that some people will will write this the other way around, i.e., as $2 \times 26^9 + 17 \times 26^8 + \cdots + 6 \times 26^1 + 24 \times 26^0$. This is a matter of convention.

(a) Find the number associated with **CRYPTOLOGY**.

(b) Pick a 20-digit public key for Kid Krypto, and write it on a whiteboard. Remember your private key, and make sure to keep it private.

