

LAB 5

**Base-26**

EXPERIMENT 5.1. Let  $n = 94,729,287,472,347,234$ .

(a) Find  $s_0, \dots, s_{16}$  such that we can write  $n$  as

$$s_0 \times 10^0 + s_1 \times 10^1 + s_2 \times 10^2 + s_3 \times 10^3 + \dots + s_{15} \times 10^{15} + s_{16} \times 10^{16}.$$

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 dumb luck that you got an integer? What is  $\text{REM}(n_1, 10)$ ?

(d) Suppose we keep going and set  $n_j = (n_{j-1} - \text{REM}(n_{j-1}, 10))/10$  for  $j = 2, \dots, 16$ . Can you find  $\text{REM}(n_j, 10)$  without doing any computations?

EXPERIMENT 5.2. Keep  $n = 94,729,287,472,347,234$  from Experiment 5.1.

(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  $s_j = \text{REM}(n_j, 26)$ . What is  $n_{12}$ ? Make a table of  $s_0, \dots, s_{11}$ .

(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  $m = 235,823,443$ .

(e) Is it possible that two different numbers have the same base 26 expansion? Can a number have two different base 26 expansions? Why or why not?

EXPERIMENT 5.3. 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

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

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

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) For what type of word is our convention of whether the first or last letter corresponds to the  $26^0$  term irrelevant?
- (c) Compute the numbers associated with **THIS**, **THAT**, **THEN**, and **THERE** using both conventions. What are your observations?

EXPERIMENT 5.4. Recall that Kid Krypto works as follows. The public key consists of numbers  $e$  and  $n$ , and the private key  $f$  is an inverse of  $e$  modulo  $n$ .

To encode a message, we turn each word into a number  $x$  and then compute  $y = \text{REM}(ex, n)$ . We then compute the base 26 expansion of  $y$  and turn it back into a collection of letters. Note that each word needs to be smaller than  $n$ .

Work along with the following example. I tell you that my public key is:

$$e = 2309$$

$$n = 23768741896345550770650537601358309.$$

(Remarkably, these are both prime numbers.) To encode and send me the message HEY YOU, you compute

$$x_1 = 7 \times 26^0 + 4 \times 26^1 + 24 \times 26^2 = 16335,$$

$$x_2 = 24 \times 26^0 + 14 \times 26^1 + 20 \times 26^2 = 13908$$

Then

$$y_1 = \text{REM}(16335e, n) = 37717515,$$

so HEY encodes as RDZNE, and

$$y_2 = \text{REM}(13908e, n) = 32113572,$$

so YOU becomes KHDHSC. Therefore, you email me RDZNE KHDHSC. Notice that Kid Krypto doesn't preserve the length of words!

I receive your message, and use base 26 expansion to turn the encrypted words into the numbers 37717515 and 32113572. I then compute

$$\text{REM}(37717515f, n) = 16335$$

$$\text{REM}(32113572f, n) = 13908,$$

using my private key  $f$ , then convert these back into HEY YOU.

You want to email me the message CRYPTOLOGY IS FUN using my public key. What do you send?