LAB 5

Kid Krypto

PROBLEM 5.1. Write a recursive function `MyDiv[a_, b_]` that returns the pair $\{\mathrm{Quo}(a,b), \mathrm{Rem}(a,b)\}$. Watch out for weird cases. Then use `MyDiv` to make functions `MyQuo` and `MyRem`.

PROBLEM 5.2. Write a `ModularAddition[a_, b_, m_]` function that computes the sum of a and b, and is only correct mod m. For example, the output of `ModularAddition[6, 7, 10]` should be `3`. You may use Mathematica's + operation and `MyRem`.

Problem 5.3. Look back at the multiplication worksheet where we figured out how to quickly multiply two numbers. Then use `ModularAddition` to write a recursive `ModularMultiply[a_, b_, m_]` function that computes the product of a and b, and is only correct mod m.

Kid Krypto is a *public key* cryptosystem. If Ada would like to receive secret messages, she first chooses any four positive integers that only she will know: a, b, c, and d. Then she computes:

$$\begin{aligned} M &= ab - 1, \\ e &= cM + a, \\ f &= dM + b, \\ n &= \frac{ef - 1}{M}. \end{aligned}$$

Ada tells everyone who wants to send her a message the numbers e and n, these numbers form Ada's *public key*. However, Ada keeps her *private key*, the number f, completely secret. (Ada can securely delete the other numbers used to generate the keys.)

To send Ada a message x, encoded as an integer in the range $0 \leq x \leq n - 1$, the sender computes

$$y = \text{REM}\,(ex, n)$$

and sends y. To decipher the message y, Ada computes

$$\text{REM}\,(fy, n)$$

to recover x.

Experiment 5.4. Suppose Ada chooses $a = 47$, $b = 22$, $c = 11$, and $d = 5$.

(a) What numbers M, e, f, and n would Ada calculate?

(b) Write a Mathematica function called `MyEncrypt` to encode message for the public key pair e, n you just computed. Use your function to encode the message $x = 2020$.

(c) Write a Mathematica function called `MyDecrypt` that decodes a message y using the private key f. Use your function to decode the encrypted message $y = 43155$.

Problem 5.5. On a different day, Ada announces a new public key:

$$n = 17\,239\,722\,505 \quad e = 25\,540\,219.$$

Charles sends her an encrypted message that you intercept: $y = 7\,218\,695\,996$. Crack the encryption to read Charles's message. What does it say?

Problem 5.6. You intercept another message from Charles to Ada: $y = 8\,617\,388\,745$. What does it say? (Hint: try the command `IntegerDigits[263,26]` and improvise based on that.)