LAB 6

MyGCD and PositivePowerMod

RSA is based on using exponents rather than products, and relies on computations of the GCD.

PROBLEM 6.1. Compute

$$\text{REM}\,(123412342^{3224435}, 341234)$$

in Mathematica. How long does the calculation take, in milliseconds?

PROBLEM 6.2. Write down the algorithm for `FastMultiply` that we have used before.

PROBLEM 6.3. Is it true that $\text{REM}\,(123412342^{3224435}, 341234) = \text{REM}\,(123412342^{\text{REM}(3224435,341234)}, 341234)$?

PROBLEM 6.4. Compute

$$\text{REM}\left(123412342^{3224435}, 341234\right)$$

in under a millisecond by writing your won `FastExponentiateModM` function (feel free to shorten the name).

PROBLEM 6.5. Write a recursive function that computes $MyGCD(a, b)$ for any pair of integers a, b.

Next time, we will be implementing the Extended Euclidean Algorithm, which requires us to keep track of the quotients and remainders involved in computing $GCD(a, b)$: the current a, b, q, and r.

PROBLEM 6.6. Write a while loop that creates a table of all the numbers for the GCD. It should look something like this:

```
EuclideanTable[a_,b_]:=Module[{ETable={},i=1},
      AppendTo[ETable, (*add the starting row*)];
      While[(*remainder of a and b is not zero*),
          (*add a new row to ETable*);
          i++;
      ];
      EETable
]
```