

# MathTLC Algebra Project Descriptions

## 1. Elliptic Curves & Congruent Numbers

An integer  $A$  is **congruent** provided it is the area of a right-triangle, each of whose sides is a rational number. For example, 6 is congruent because it is the area of a 3-4-5 triangle. Also, 157 is a congruent number. But the simplest (in terms of number of digits) rational triangle having 157 as its area has hypotenuse of length:

$$c = \frac{2244035177043369699245575130906674863160948472041}{8912332268928859588025535178967163570016480830}$$

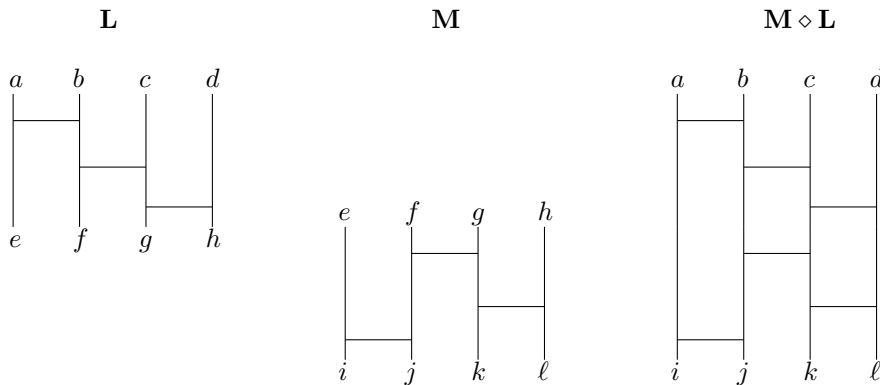
The reading for this project is

- The Congruent Number Problem found at <http://www.math.umd.edu/~eve/congnum.html>

This project should explain how the problem of determining whether or not the integer  $n$  is a congruent number can be formulated as a problem of finding nice rational points on an associated elliptic curve; show elliptic curve operations can be used to produce the solution for 157; Explain how the elliptic curves arise in the problem of determining which pyramidal numbers are also perfect squares.

## 2. Permutation Ladders

This project further explores the permutation ladders that we've discussed in class.



The reading assignment for the project is the paper: *Permutation Ladders*.

The project should discuss how permutation ladders can be used to establish basic results about permutations (e.g. Every permutation is a product of consecutive transpositions; the number of rungs in two ladders that give the same permutation have the same parity).

## 3. Perfect Shuffles

This project explores perfect shuffles of a standard deck of cards.

The reading assignment for the project is:

*Perfect Shuffles* at

<http://www.math.hmc.edu/funfacts/ffiles/20001.1-6.shtml>,

*Seven Shuffles* at

<http://www.math.hmc.edu/funfacts/ffiles/20002.4-6.shtml> and

*Rising sequences* at

<http://www.math.hmc.edu/funfacts/ffiles/20001.4-6.shtml>

The project should discuss the in-shuffle and its disjoint cycle representation; the out-shuffle and its disjoint cycle representation; the number of in-shuffles needed to get a deck back into order; the number of out-shuffles to get a deck back into order; rising sequences; why some permutations of a deck of cards can't be obtained in 5 perfect shuffles; and the fact that 7 shuffles give a random deck.

#### 4. **Pancake Problem**

Here's the problem:

A waiter is navigating a busy restaurant with a stack of  $n$  pancakes. To please the customer, the waiter wants to sort the pancakes in order by size. Having only one free hand, the only available operation is to lift a top portion of the stack, invert it, and replace it. Finding the maximum number of flips needed for a stack of  $n$  pancake is the Pancake Problem.

The reading assignment for the project is:

*Pancake Sorting* at

<http://www.maa.org/mathland/mathtrek090406.html> and

*The Pancake Problem Notes*.

The project should relate that pancake problem to permutations; illustrate that it takes at most  $2n - 3$  flips to get a stack on  $n$  pancakes into order; explain why the odd-even stack requires  $n - 1$  pancakes; mention known results and the gap between lower and upper bound; briefly explain how this problem has real-life applications.

#### 5. **Time to rotate your mattress!**

This project studies the rigid motions of a mattress, and the possible algorithms for flipping a mattress so that each possible orientation of a mattress occurs for the same amount of time.

The reading assignment for the project is: Chapter 12 in *Group Theory in the Bedroom*

The project should relate rotating your mattress with the rigid motions of a box; give the Cayley table for the rigid motions of the box; explain why there is no single rotation that when repeated gets all possible orientations; study the problem of rotating a cubical mattress (e.g. how many different rigid motions are there now?, is there a single motion that gets all of them?)

#### 6. **Bar codes**

Identification numbers are used to identify individual items, specific products, people, accounts etc. This project studies how identification numbers are designed so that when errors in transmitting identification numbers occur how the errors can be detected effectively.

The reading assignment for the project is:

Chapter 1, Chapter 2.4-2.7 of *Identification Numbers and Check Digit Schemes*

The project should describe several check digit schemes, provide examples, describe two of the most common errors, and discuss how “good” each of the check digit schemes is in detecting these errors.

### 7. **Cryptography and the RSA Public-Key System**

Cryptography is the study of methods to send messages in disguised form so that only the intended recipient can decode and read the message. This project studies *Caesar Ciphers* and the celebrated *RSA* public-key system.

The reading assignment for the project is:

Chapter 2.8 of *Identification Numbers and Check Digit Schemes*

Chapter 6,7,8,9 in Part II of *In Code, A mathematical Journey*,

The project should describe Caesar ciphers and RSA public-key system, provides examples, explain what is a public-key system and what is an advantage of such a system, and how “confidentiality” of the transmitting messages is insured in using the systems.

### 8. **Costas Arrays**

A Costas array is an arrangement of  $n$  1s ones in a  $n$ -by- $n$  matrix of 0's and 1's (one 1 per row, one 1 per column) such that the vectors connecting each pair of 1s are distinct. These arrays are useful in sonar and radar systems.

The reading assignment for the project is:

- Costas Arrays at <http://en.wikipedia.org/wiki/Costasarray>. (Just read the first couple of paragraphs).
- Pages 1-2 of *Constructions and Properties of Costas Arrays*

The project should define a Costas array; give examples of Costas Arrays; describe the use of Costas arrays in radar; describe the Welch construction; algebraically verify that the Welch construction gives a Costas Array.