Lab #4

Out : October 2, 1997; 2:30 pm
Due : October 9, 1997, 12:30 pm

Experiment 1:

You and your classmates are close to failing out of quadruple credit "Intensive Welsh." The professor decides to have mandatory lectures every day of the week, and to continue giving pop quizzes on the new material you learn. Fortunately, you stumble upon an encrypted message from the professor to his secretary which contains the day of the next test. Your professor has bragged in class about the fact that his cryptosystem of choice, the one-time pad, is perfectly secure. Being the determined sort, you decide to have a crack at it. When you open this experiment, you will will find a transcript containing the cyphertext. The block size is one symbol (2 digits), and the modulus is 100. NOTE: This experiment will be handed in on paper.

(a) Can you eliminate any possible plaintexts?

(b) Given what you know, what are the possible keys?

In Brief...	
We give you:	A cyphertext encrypted with a one-time-pad. You are not given a key.
Your task:	Think on and answer the above questions.
Hand in:	Hand in your answers on paper.

Experiment 2:

Paying for college is getting really out of hand, and you find that your UFS job does not provide enough funds to pay for your education. To your delight, you find an Internet roulette game hosted at an offshore gambling web site and decide to try your luck. The game works like this: The player sends a guess (a number between 0 and 39) and a monetary bet to a computer in Anguilla. The computer "spins the wheel" and either credits or debits your account with the amount of the bet based on whether or not the number that was chosen is the one that you picked. However, this presents a problem if the casino is dishonest (i.e., the casino might purposely choose a number other than the player chose). The casino therefore requires the player to encrypt her guess guess before sending it. After the "virtual roulette wheel" is spun, the casino sends the player the outcome. The player then sends the key to the casino so that they can decrypt the player's guess and compare the plaintext to the outcome.

(a) When you open this experiment, you will find a calculator that represents the casino, a cell used to keep track of your winnings, and a calculator for you. The casino has decided to have the player use the addition cypher with a modulus of 40. Program your calculator to send an encryption of your guess, receive the winning number, and then respond by sending a key. This protocol allows players to cheat

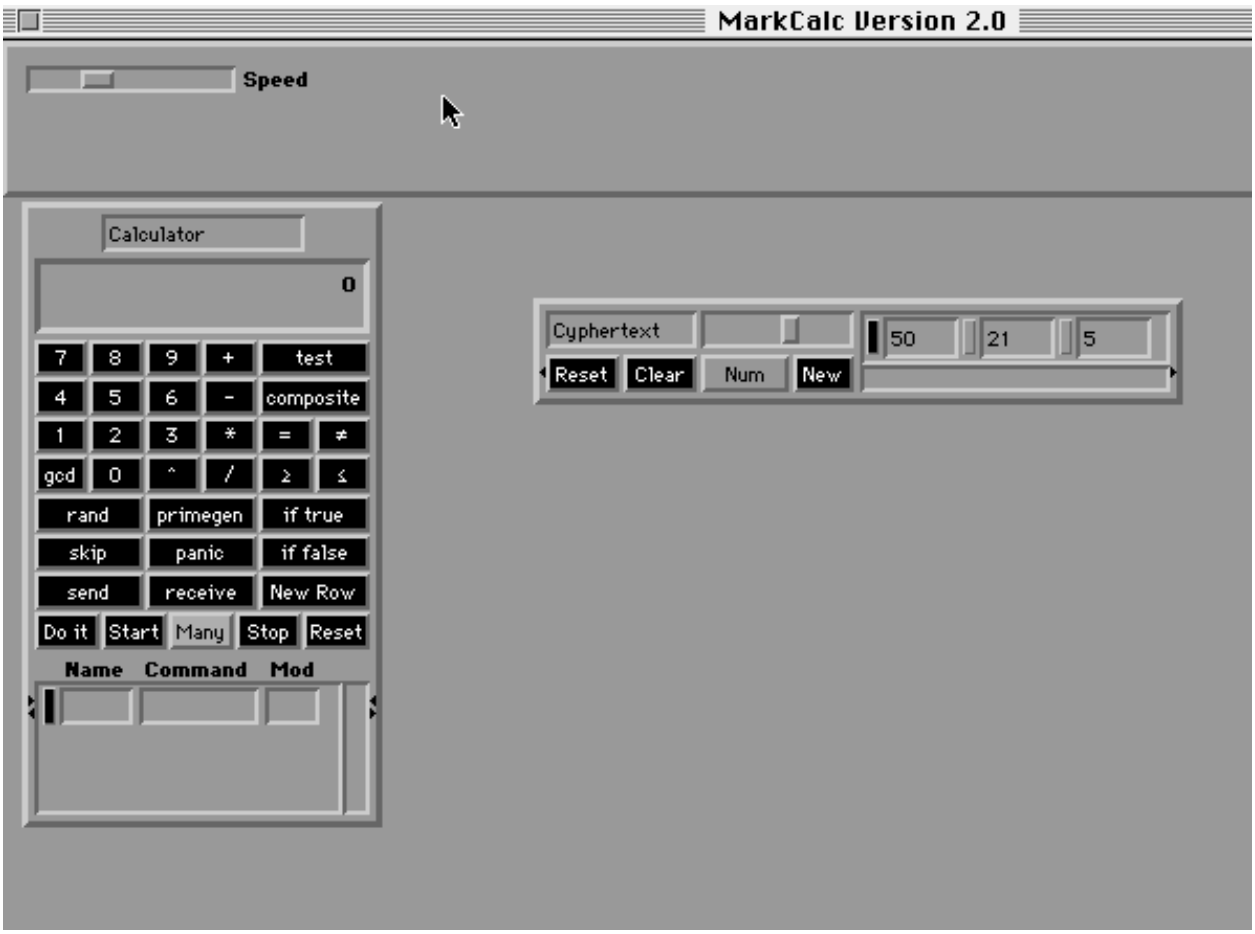

Figure 1: Experiment 1

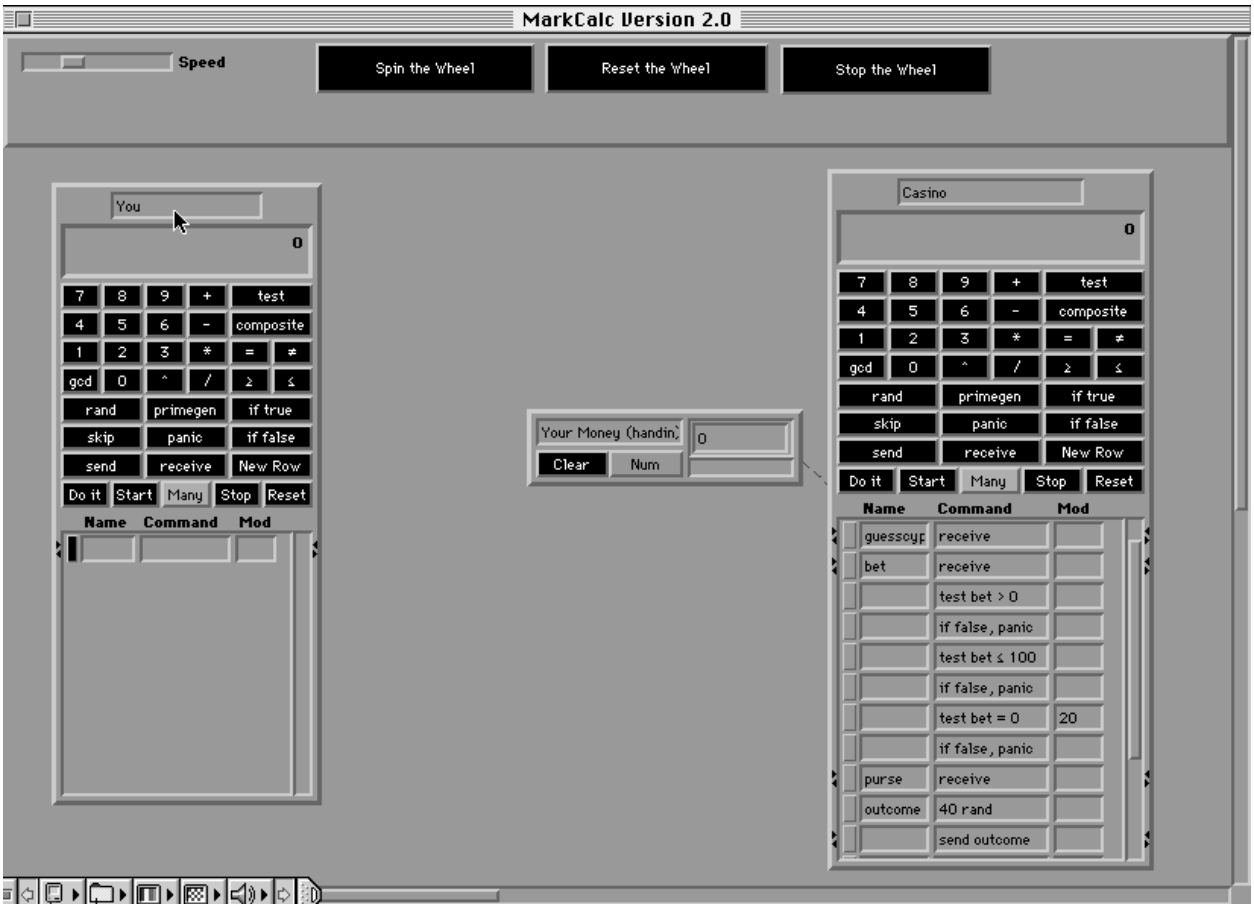

Figure 2: Experiment 2a

with impunity. You must figure out how. You can bet up to $ 100 in increments of $ 20. Your goal is to win $ 500, enough to cover your books for the semester. When your winnings total 500, *submit results* from the file menu. Then, hand in on paper a brief explanation of how you managed to beat the system.

In Brief...	
We give you:	A calculator set up to act as a casino, a cell containing your current winnings, and a calculator for you.
Your task:	Play the game, but cheat by sending a key that will result in you winning.
Hand in:	Submit electronically once your net winnings total $ 500, and hand in a brief description of the flaw on paper..

(b) With tuition rising, you are convinced that the real money is to be made by running your own Internet roulette table. In order to prevent rampant cheating of the sort demonstrated in part a, the

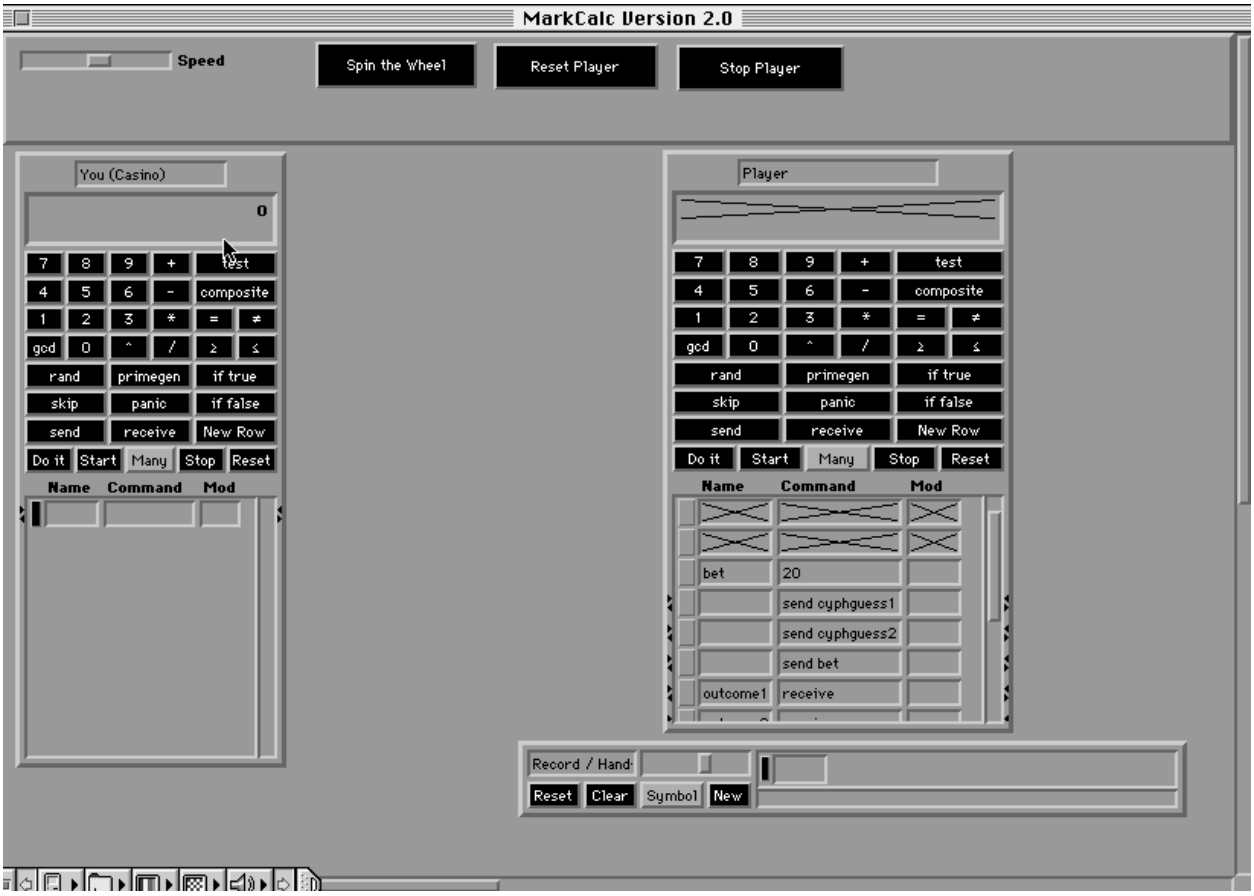

Figure 3: Experiment 2b

encryption you chose to implement is the addition cypher with a block size of 1 digit. For convenience, you alter the roulette rules slightly so that the possible numbers are between 0 and 8. Being ever the profit-minded soul that you are, however, you decide to cheat the players. In this experiment, you must interact with a calculator labeled "Player", who will send you guesses. The player calculator will write "Win" or "Lose" to the Hand-in transcript based on the outcome of each turn. You must make certain that the player consistently loses by submitting when the Hand-in transcript contains a record of 10 sequential losses.

In Brief...	
We give you:	A calculator set up to act as a player, a hand-in transcript, and a calculator for you.
Your task:	Program your calculator to perform the casino's portion of the protocol, making sure to cheat and guess a number that will make the player lose each time.
Hand in:	Submit electronically once the player has lost 10 sequential turns.

Experiment 3:

The NSA has realized that the Phi function may have cryptographic applications, and wants to study it. In particular, they are interested in finding Phi of vaious moduli m. One method that has been proposed is to simply count how many numbers are relatively prime to m. Your job is to try this for several values of m of varying size, and determine if this is an efficient method of calculating $\phi(m)$. When you open experiment 3, you will see a calculator, a counter, a cell, and a transcript. The transcript holds each of the moduli you have been hired to calculate Phi for. For each modulus, you will need to set up the calculator we provide you by typing that value into the appropriate row, and also type the value for $m-1$ into the counter as the maximum value (the rightmost slot). Then, using a stopwatch, time how long it takes for the program to run to completion (ie, when it runs out of values to pull from the counter). The final value of $\phi(m)$ will be in the cell marked "Current Count". There is no electronic hand-in for this experiment. Instead, your boss has requested a paper hand-in summarizing how long it took for each value in the form of a graph, with the given values for m plotted on the x-axis, and the time required to compute $\phi(m)$ on the y-axis. Make sure to indicate the values at each data point. NOTE: When doing this experiment, be sure to reset the cell back to 0 between runs. Also, in order to get comparable results, you must make sure that the speed slider in the upper left is set on the fastest possible setting (far right).

In Brief...	
We give you:	A setup allowing you to find Phi values, and a list of moduli to compute Phi for.
Your task:	Fill in the appropriate fields of the provided setup and run the experiment. Time how long it takes to find Phi for each value of m.
Hand in:	Hand in a graph of the time it takes to compute the values on paper.

Experiment 4:

Impressed with your performance in your last assignment, the NSA has transferred you to the Modular Multiplicative Inverse Department. Here, your job requires you to spend your days calculating multiplicative inverses, mod m. The method you have been told to investigate works as follows: To compute

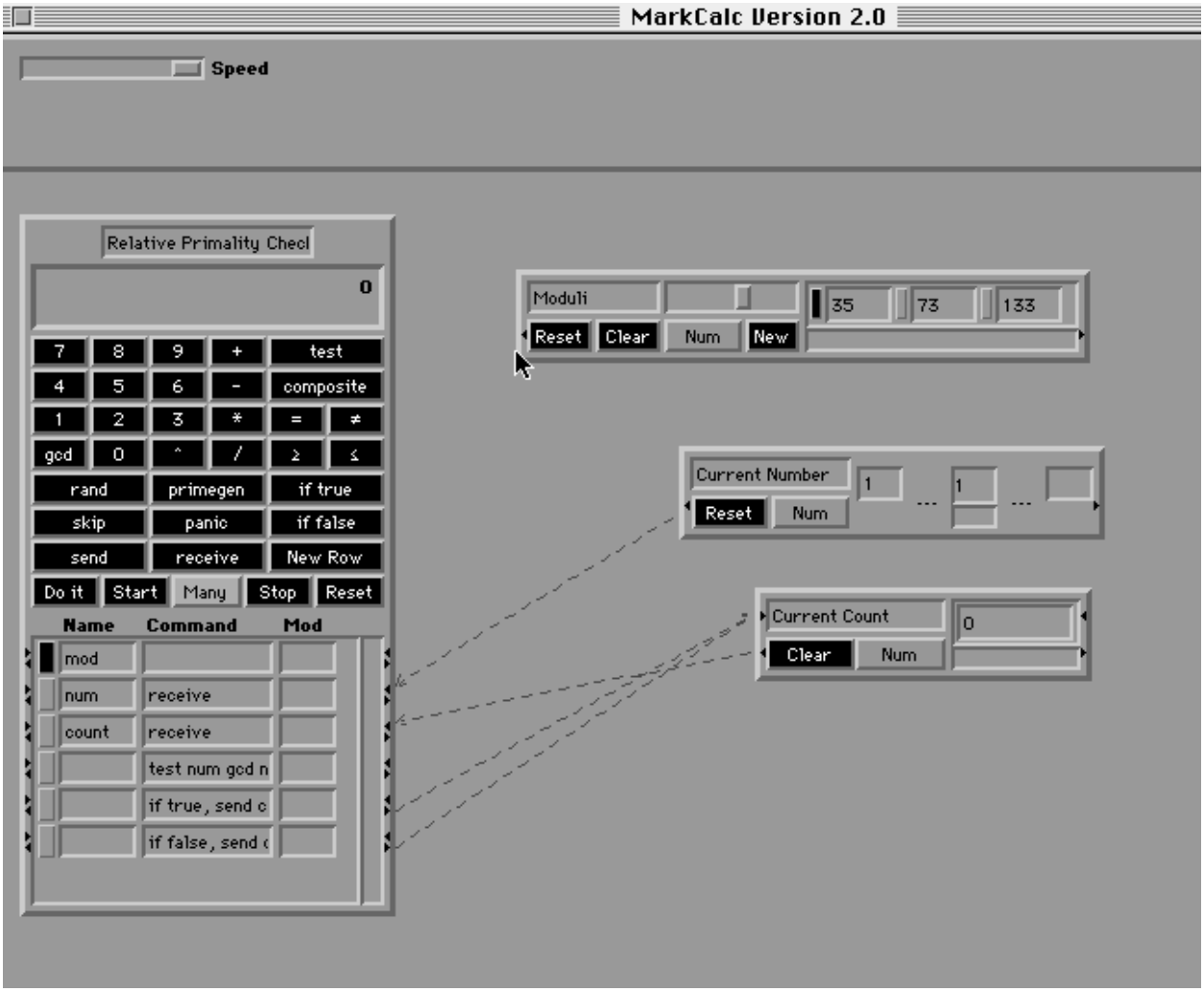

Figure 4: Experiment 3

the multiplicative inverse of some number b, multiply b by each number between 0 and $m-1$. If the result has a standard name of $1 \pmod{m}$, you have found the inverse.

There are three parts to this experiment, contained within separate files. When you open each part, you will see a calculator, a counter, a transcript, and two cells. The transcript labeled "$b - values$" contains values b for which you are to find inverses. The cell labeled "Moduli" contains the modulus to use. You will find the inverse of each b under the given moduli using the above method which the calculator you are provided has been set up to perform. Before proceding, however, you will need to type the value for $modulus - 1$ into the maximum value slot of the counter. You will then enter each value for b in turn into the correct line of the calculator and run the experiment. The calculator will enter into "Panic" mode to let you know when it has found the answer, and it will send the answer to the cell labeled "Inverse". Time how long it takes for each b under the given modulus and record the average of those times. Hand in a graph of the average times it takes to compute the various inverses under each moduli. NOTE: As in the last experiment, be sure that the speed slider in the upper left is set to the far right (the fastest possible setting). Please turn in a graph with clearly-marked axis and values.

In Brief...	
We give you:	A setup allowing you to find multiplicative inverses, a transcript containing values for which you must find inverses, and a transcript containing the moduli to use.
Your task:	Type the appropriate values into the setup you are provided, and run the experiment, timing how long it takes to find each inverse.
Hand in:	Hand in, on paper, a graph of the average time it takes to compute the inverse for each moduli.

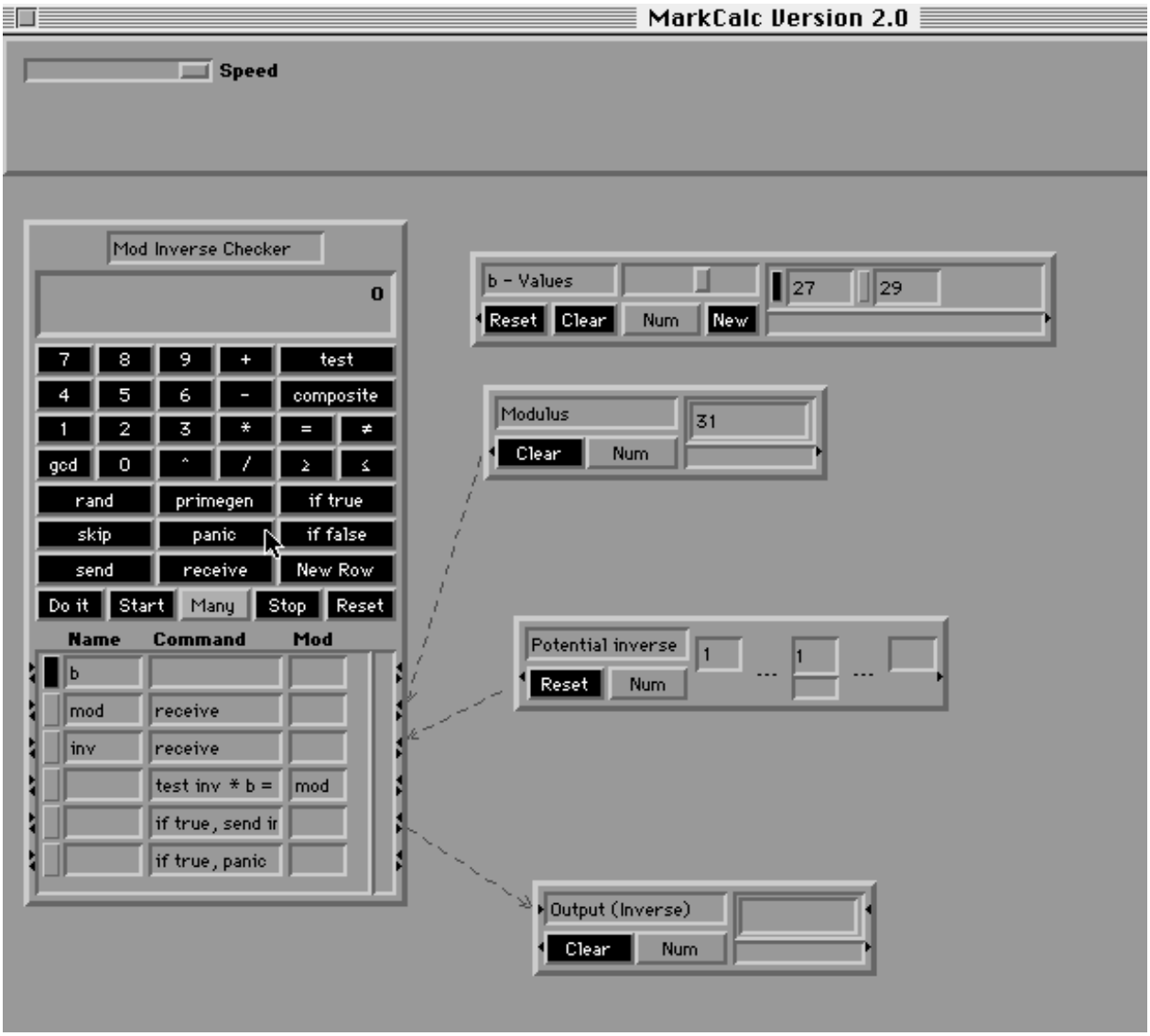

Figure 5: Experiment 4