Department of Mathematics

Maths 190 and Maths 190G Tutorial 3

For this tutorial, please organize yourselves into groups of **three** (preferable) or **four**. Hand in your solution to the boxed question with **Assignment 2.**

1. Express each of the following numbers as a product of primes: 6, 24, 27, 35, 120.

2. Does a nonprime divided by a nonprime ever result in a prime? Always? Sometimes? Never? Explain your answers.

3. Express the first 15 even numbers greater than 2 as as the sum of two prime numbers. Is every even number the sum of two primes?

4. (**Hand in with Assignment 2**) Can every odd number greater than 3 be written as a sum of two primes? Why/Why not?

For the final exercise each group will need a calculator (or computer) that is able raise one number to the power of another, e.g., to compute 5^{10}=9,765,625.

5. Establishing shared secret passwords. In this exercise two of your group members (let's call them Alice and Bob) will generate a shared secret password (to access a bank account, for example). They do this by individually making certain calculations, by publicly declaring the results, and by making a second calculation to determine the password. (In practice this password exchange could take place without Alice or Bob actually meeting, e.g., by publishing their results in a newspaper.) The remaining group member(s) must try to discover the password.

To describe the details, we,need the following mathematical notation: "A mod B" refers to the remainder obtained when A is divided by B. For example, 18 mod 7 = 4 because 18 divided by 7 is 2 with a remainder of 4.

Agree who is to be Alice and Bob and who will observe. Then:

(a) Alice randomly picks a number between 1 and 10 (let's call it *A*) *and tells it to no one*. Bob does the same (let's call this number *B).*

(b) Alice calculates 5^A mod 23 (let's call this number *C*) and writes the result down on a piece of paper viewable by all group members: "*C* = … ." Similarly, Bob calculates 5^B mod 23 (let's call this number *D)* and writes the result underneath: "*D* = … ."

(c) Alice now calculates D^A mod 23. *This is Alice's secret password.* Bob calculates C^B mod 23. *This is Bob's secret password* and it is the **same** as that of Alice! Can you see why?

(d) The remaining group members attempt to discover the shared password, given the values of *C* and *D* written down, together with what they know about how the password was generated.

(e) Discuss your observations, and if time permits change roles.