Department of Mathematics

Maths 190 and Maths 190G
Lecture 6 Summary

In this lecture we illustrate two important observations:

- Factorisation is much more difficult than multiplication
- Because of this it is possible to make a code that cannot be decoded, even when you know how it was encoded.

Lecture 6 was based around the following question:

Question: Is it always possible to decode a message when you know how it was encoded?

First we discussed the importance of codes, where they are used, and how much we rely on them.

Then we discussed some simple codes and how they might easily be broken. We discussed how it seems that, if you know how the message was encoded, you should always be able to decode it.

We practised factoring some numbers into primes, and learned how, as the number gets big, the factorisation problem becomes very difficult, too difficult even for the fastest computers around today, working for millions of years.

Then we explained how this fact can be used to construct public secret codes. These are codes that you can't decode, even when you know how they were encoded!

Before you come to the next lecture: You should spend an hour or two thinking and reading about the ideas presented in the lecture. You should also:

- Read Section 2.4, pages 82-89 of the textbook, *Crazy Clocks and Checking out Bars*.

Other activities you could do if you have time are:

- Try following the instructions in the textbook (starting at the bottom of page 99, and continuing on pages 100 and 101) to construct your own public secret code. Try to get a friend to decode a simple message. Show them exactly how you encoded the message. Can they decode it? Before they tried to decode, did they think they would be able to?