6G5Z3006 Number Theory and Cryptography

Options talk by Dr Killian O'Brien

MMU, January 2016, these slides at tinyurl.com/ntc1617

The unit

- Number Theory (Dr Killian O'Brien)
- Cryptography (Dr Jon Borresen)
- 3 hours lecture + 1 hour tutorial per week
- Coursework problems (30%), Examination (70%)
- Popular unit (49 students in 14/15) with good ISS results

In a nutshell

Number Theory

- The study of the integers

$$\mathbb{Z} = \{\cdots - 3, -2, -1, 0, 1, 2, 3, \dots\}$$

- Of fundamental importance are the primes

$$2, 3, 5, 7, \dots$$

- Nice mixture of proof oriented theoretical work and algorithmic methods

Cryptography

- The science/art of transforming *text* so that it can only be *read* by selected recipients.
- Often in connection to military/industrial/political/... secrets.
- Universally and intensively used in modern computer network communications.

Software

- Interesting use of mathematical software for various aspects of the unit
  - Matlab
  - SageMath

A quick tour of some highlights from the unit

Integers in the news

What's so special about … ?

- $74,207,281$
- $2^{74,207,281}-1$

. . .

The 49th known Mersenne prime found by the GIMPS project.

Open conjecture or tutorial problem?

- There are infinitely many prime numbers.
- 2^n-1 can only be prime when n is prime.
- There are infinitely many 2^n-1 which are prime.

. . .

The following SageMath code finds the first few Mersenne primes. See the results

.

Open conjecture or tutorial problem?

- There are infinitely many primes p for which $p+2$ is also prime, i.e. *narrow* steps on the π staircase.
- For any integer $n \geq 1$ there are infinitely many gaps of at least length n between consecutive primes, i.e. *wide* steps on the π staircase.

Classical vs. modern cryptography

Classical

- Topics include mono- and poly-alphabetic substitution ciphers.
- Classical cryptography required prearranged secrets between sender and recipient.
- Can be broken with the aid of frequency analysis and these vulnerabilities.

Modern

- Crypto systems based on number theoretic concepts.
- Prearranged secrets no longer required, so called *Public Key Cryptography*.
- Enables secure mass communication between anyone across public non-secure networks.

Who is this?

Who was that?

- Edward Snowden, former worker for the CIA and NSA.
- In 2013, he fled the USA, briefly staying in Hong Kong before securing temporary asylum in Russia.
- Has passed many thousands of classified files from the NSA, GCHQ and other intelligence agencies to journalists.
- These revelations concern global surveillance programs carried out by these agencies on the public.

CitizenFour movie

How did Snowden make secure contact with journalists he had never met?