# Number Theory and Cryptography (6G5Z3006)

# Syllabus topics

**Number Theory:** We study the integers and examine in detail the concepts of

- divisibility
- prime numbers
- congruences and modular arithmetic
- solutions of polynomial congruences
- quadratic residues and quadratic reciprocity

# Syllabus topics

**Cryptography:** We start with the study of basic encryption techniques such as

- substitution ciphers
- Hill ciphers
- affine ciphers
- stream ciphers

Then in the second term looks at more modern developments in public key encryption such as the

- RSA algorithm
- El-Gamal encryption
- Diffie-Helman key exchange
- primality testing.

# Teaching team, teaching pattern & assessment

- 3 hours lecture + 1 hour tutorial per week.
- This year the number theory is taught by Dr Killian O'Brien and the two cryptography terms are taught by Dr Andrew Wiseman and Dr Jon Borresen respectively.
- The tutorials concentrate on the two parts of the unit in alternate weeks and are taken by the relevant lecturer.
- Assessment is by Coursework Report (30%) and Summer Exam (70%).
- Both NT & C contribute 50% to all teaching and assessment.

# Nature of the unit

- A nice combination of proof oriented theoretical work and practical calculation based methods.
- Definately suited to students who like problem solving and the unit will develop your skills in this area.
- Matlab is used to take the pain out of the lengthy calculations in the cryptography half. Its use is necessary for the coursework but plenty of support and sample code is provided.
- I am also increasingly making use of Sagemath (www.sagemath.org, cloud.sagemath.org, sagecell.sagemath.org) to help investigate number theory and use it to demonstrate some aspects of number theory.

# *Some highlights from the unit*

In the unit we prove a lot of interesting results in Number Theory ....

- There are an infinite amount of primes $2, 3, 5, 7, 11, \ldots$ (see at least three proofs of this)
- The prime harmonic series diverges, i.e.

$$\sum_{p} \frac{1}{p} = \infty$$

- We describe some famous unsolved conjectures in number theory, such as the twin prime conjecture: *There are an infinite number of pairs of integers* $n, n+2$*, both of which are prime.*
- As a counterpoint to this we will prove(tutorial exercise) that there exist arbitrarily large gaps between the primes.

# *Some highlights from the unit*

And in Cryptography we meet . . .

- Public Key Cryptography: This enables parties to communicate securely in public without ever having shared secrets beforehand. Relies on the properties of number theoretic functions.

# . . . and some interesting functions you will meet . . .

- Can you explain the accumulation lines in the plots of the following functions?

The divisor sum function

$$d(n) = \sum_{d \text{ divides } n} d$$

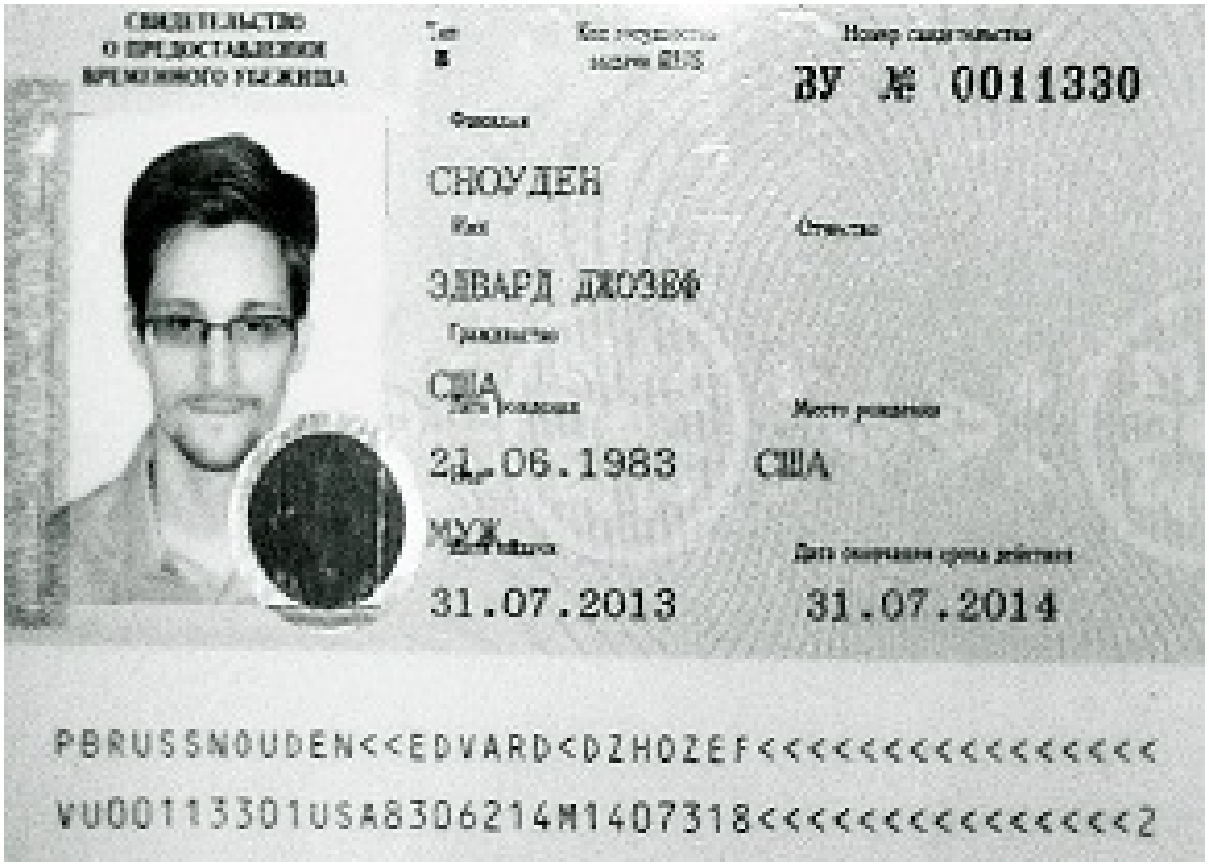
(If you cannot see the Sagemath code cell above then click here for a link to the cell showing a plot of the divisor sum function. You may need to use a modern browser such as Chrome or Mozilla Firefox.)

Euler's totient function

$\phi(n) =$ number of $m$ such that $1 \leq m \leq n$ and $n, m$ are coprime $= |\mathbb{Z}_n^\times|$.

(If you cannot see the Sagemath code cell above then click here for a link to the cell showing a plot of Euler's totient function. You may need to use a modern browser such as Chrome or Mozilla Firefox.)

# Up to the minute relevance to world politics, justice & human rights . . .




- Guardian, ACLU, Wikipedia