Option A

Hand in at least one question from at least three sheets

**Sheet 1: Introduction to prime numbers.**

(provisional date for handing in: class 2)

1. Use Sieve of Eratosthenes to find all prime numbers between 100 and 200.
2. Write the integers 57, 2010 and 24000 as products of primes.
3. Find all pairs of primes $p$ and $q$ satisfying $p - q = 3$.
4. The arithmetic mean of the twin primes 3 and 5 is the perfect square 4. Are there any other twin primes with a square mean?
5. Modify Euclid’s proof that there are infinitely many primes by assuming the existence of a largest prime $p$ and using the integer $N = p! + 1$ to arrive at a contradiction.
6. Show that the product of two elements of the form $4n + 1$ also has the same form, and so an integer of the form $4n + 3$ must have a prime divisor of the same form. Deduce that there are infinitely many primes of the form $4n + 3$.
7. Show that there are arbitrarily long sequences of consecutive composite numbers.
1. Calculate \( \text{hcf}(143, 227) \), \( \text{hcf}(306, 657) \) and \( \text{hcf}(272, 1479) \).

2. Use Euclidean Algorithm to calculate \( d = \text{hcf}(119, 272) \) and find \( x \) and \( y \) satisfying \( d = 119x + 272y \).

3. Give an example of four positive integers such that any three of them have a common factor that is bigger than 1, but only 1 divides all four of them.

4. Use the division algorithm to establish that the cube of any integer has the form \( 7k - 1 \), \( 7k \) or \( 7k + 1 \).

5. Is the converse to the Euclidean Algorithm true? In other words, if \( x, y \) and \( d \) are such that
   \[
   ax + by = d,
   \]
   does it necessarily follow that \( d = \text{hcf}(a, b) \)? Provide a proof or a counterexample.

6. Show that if \( \text{hcf}(a, b) = d \) then \( \text{hcf}(\frac{a}{d}, \frac{b}{d}) = 1 \).

7. Suppose that \( a \) and \( b \) are coprime, \( a | c \) and \( b | c \). Prove that \( ab | c \).
1. Calculate $1^3$, $2^3$ and $3^3$ (mod 4) and deduce the value of $1^3 + 2^3 + \cdots + 99^3 + 100^3$ (mod 4).

2. Find the remainders of $2^{50}$ and $41^{65}$ when divided by 7.

3. The International Standard Book Number (ISBN-13) consists of twelve digits $d_1, \ldots, d_{12}$ followed by a thirteenth digit $d_{13}$, which satisfies

$$d_{13} \equiv 10 - (d_1 + 3d_2 + d_3 + 3d_4 + \cdots + d_{11} + 3d_{12}) \pmod{10}.$$

Determine whether each of the ISBN is correct:

(a) 978-019285361-5
(b) 978-019921986-6
(c) 978-054513970-0

4. Using decimal representation of integers, establish the following criteria:

(a) An integer is divisible by 2 if and only if its units digit is 0, 2, 4, 6 or 8.
(b) An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.
(c) An integer is divisible by 4 if and only if the number formed by its tens and units digits is divisible by 4.

5. Calculate $\phi(13)$, $\phi(91)$ and $\phi(361)$. Deduce the value of $3^{688}$ (mod 361).

6. Let $a$, $b$, $c$ and $d$ be integers and let $n$ be a positive integer. Show that

(a) $a \equiv a \pmod{n}$;
(b) if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$;
(c) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$;
(d) if $a \equiv b \pmod{n}$ then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$;
(e) if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a \pm c \equiv b \pm d \pmod{n}$ and $ac \equiv bd \pmod{n}$. In particular, $a^k \equiv b^k \pmod{n}$ for any $k$.

7. Let $p$ be a prime and $e$ be any positive integer. Calculate $\phi(p^e)$. 
1. Solve the following linear congruences:
   (a) \(3x \equiv 1 \pmod{7}\).
   (b) \(7x \equiv 3 \pmod{10}\).

2. For each of the following linear congruences determine whether it is soluble and if so, find its solutions.
   (a) \(2x \equiv 3 \pmod{26}\).
   (b) \(5x \equiv 15 \pmod{20}\).

3. Solve the following set of simultaneous congruences:
   \[x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}.\]

4. Solve the following set of simultaneous congruences:
   \[2x \equiv 1 \pmod{5}, \quad 3x \equiv 9 \pmod{6}, \quad 4x \equiv 1 \pmod{7}, \quad 5x \equiv 9 \pmod{11}.\]

5. (Brahmagupta, 7th century AD) When eggs in a basket are removed 2, 3, 4, 5, 6 at a time, there remain respectively 1, 2, 3, 4, 5 eggs. When they are taken out 7 at a time, none are left. Find the smallest number of eggs that could have been contained in the basket.

6. Obtain three consecutive positive integers, each having a square factor.
1. Encrypt the plaintext message “SECRET MESSAGE” using the RSA algorithm with parameters $n = 2419$, $e = 3$.

2. Suppose that the ciphertext message produced by RSA encryption with parameters $e = 5$ and $n = 2881 = 43 \times 67$ is

$$2148\ 1766\ 1761\ 1320\ 0004\ 2236\ 0057\ 0243.$$ 

What is the plaintext message?
Option B

Produce a 500 words’ essay on one of the following topics:

1. A number $n$ of the form $2^a - 1$ is called a Mersenne number. If such $n$ is prime, it is called a Mersenne prime. So, who was Mersenne, what did he have to do with these numbers and what is so special about them?

(provisional oral presentation date: week 2)

2. The equation $d = ax + by$ obtained from the Euclidean Algorithm is an example of a Diophantine equation. Narrate a brief history of Diophantus of Alexandria, who the equations are named after, and explain what these equations are. Include examples, history of the topic and maybe even typical solution methods.

(provisional oral presentation date: week 3)

3. Use modular arithmetic to describe how one can calculate any day of the week and/or Easter date, in any year. Include examples.

(provisional oral presentation date: week 4)

4. Euler’s function $\phi$ is an example of an arithmetical function, that is, a real- or complex-valued function defined on the set $\mathbb{N}$ of natural numbers. Describe other famous arithmetical functions, e.g. $\tau$, $\sigma$ or $d$, together with some of their properties.

(provisional oral presentation date: week 4)

5. One way of determining whether a given number $n$, is prime, is to check its divisibility by $2, 3, \ldots, \sqrt{n}$. Another one is the Sieve of Eratosthenes. Which other primality tests exist?

(provisional oral presentation date: week 5)

6. The RSA algorithm is based on the fact that whilst it is easy to multiply two (prime) numbers, the reverse process is (currently) very hard in general. Describe some existing methods of prime factorisation.

(provisional oral presentation date: week 5)

7. Pick your favourite number-theoretic problem that is still open and describe its history, main characters and present state of the art.

(provisional oral presentation date: week 5)