15-151 course project

Due at 5:00pm on Thursday 10th August

Project overview

The purpose of the course project is to give you the opportunity to delve deeper into an area of mathematics covered (or not covered) in the course, and to demonstrate the proof-writing skills you have developed.

Your completed project will take the form of a self-contained mathematical document, in the style of a modern mathematical research paper, which is typeset using LaTeX. This paper should provide the background necessary for understanding a main result, state and prove the result, and either apply the main result to solve an interesting problem, or generalise or extend the main result in a new direction.

Learning objectives

Your completed course project should demonstrate your acquisition of the following skills:

- **Mathematical literacy and communication**
  - Typesetting a substantial mathematical document using LaTeX;
  - Providing a self-contained exposition of an important result, including all necessary definitions and preliminary results;
  - Explaining abstract concepts in a comprehensible way, including providing relevant and carefully selected examples;
  - Writing clear and correct mathematical definitions, result statements and proofs, which make appropriate use of variable quantification, notation and terminology.
- **Problem-solving skills**
  - Applying abstract mathematical concepts to solve a substantial real-world or conceptual problem;
  - Proving substantial results about a novel mathematical concept or result.

It is against these learning objectives that your project will be assessed—see the section below entitled *Rubric* for more information.

Instructions

Use LaTeX to typeset a mathematical document which:

- States and proves an interesting or important mathematical result—this may be one of the results from the *Suggested topics* section below, or another topic, subject to Clive's approval;
- Develops all the definitions and preliminary results necessary to state and prove the main result;
- Applies the main result to an interesting or important problem, or generalises or extends the main result in a new direction; and
- Contains answers to a small set of questions that Clive will provide to you when you have chosen a topic for your project.

Your document should be logically structured—to this end, a project template `.tex` file has been uploaded to the course web page to help you structure your document, but you are not required to use this template or the document structure it suggests. For example, you should feel free to rename sections, split the background section into smaller sections, and so on.

Submit the `.tex` file of your project to the appropriate section of Canvas in advance of the project deadline (9:30pm on Thursday 10th August).

Deadlines

The project must be completed and uploaded to Canvas by **9:30pm** on **Thursday 10th August**. Projects submitted late will attract a reduction in credit, unless an extension has been agreed to prior to the deadline.

To help you through the process of writing your project, there will be four 'milestones' before the final submission deadline:

- **Tuesday 1st August.** Select a project or choose your own topic.
- **Thursday 3rd August.** Prove the main result and the prescribed problem questions.
- **Sunday 6th August.** Choose what background material to include in your project, and write an outline for the background section.
- **Tuesday 8th August.** Complete the background and main result sections of your project.
- **Thursday 10th August.** Finish the project and submit it to Canvas by 9:30pm.

Topic suggestions

Suggested in this document are three topics arising from number theory. If you wish to suggest a topic in another area of mathematics, then please speak to Clive.

Linear Diophantine equations

A *linear Diophantine equation* is an equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

where $a_1, a_2, \ldots, a_n, c \in \mathbb{Z}$.

In the course, we considered the case when $n = 2$ and asked when the equation $ax+by = c$ has an integral solution. We proved that a solution exists if and only if $\gcd(a, b) \mid c$, or else no solution exists—this was Bézout's lemma. However, we didn't develop a way of *finding* the solutions.

One method to find a solution is to reverse the Euclidean algorithm (see page 131 in the text). The aim of this project is to classify *all* solutions to such an equation. This leads us to the following main result:

Theorem. Let $a, b, c \in \mathbb{Z}$, let $d = \gcd(a, b)$ and suppose that $d \mid c$. Let (x_0, y_0) be a fixed integral solution to the equation $ax + by = c$. A pair of integers (x, y) is a solution to the equation if and only if

$$x = x_0 + k \cdot \frac{b}{d} \quad \text{and} \quad y = y_0 - k \cdot \frac{a}{d}$$

for some $k \in \mathbb{Z}$.

A couple of possible areas for extension or generalisation are as follows:

- Consider the case where the coefficients and solutions to the equation $ax + by = c$ are required to be *natural numbers*—that is, we fix $a, b, c \in \mathbb{N}$ and ask when natural number solutions x, y to the equation $ax+by = c$ exist. When a and b are coprime, it is known that the least value of c for which no natural number solution exists is $ab - a - b$. Prove this, and consider what happens when a and b are *not* coprime.
- Consider the case when there are $n \geq 1$ variables, not necessarily exactly two variables—that is, consider an equation of the form $\sum_{k=1}^{n} a_k x_k = c$ for some $n \geq 1$ and some $a_1, a_2, \ldots, a_n, c \in \mathbb{Z}$. Generalise Bézout's lemma to this case; this will require that you define a notion of greatest common divisor for collections of n integers, and then find and prove a necessary and sufficient condition for the equation $\sum_{k=1}^{n} a_k x_k = c$ to have a solution.

Chinese remainder theorem

Given $a, b, n \in \mathbb{Z}$, the existence of an integral solution x to the congruence $ax \equiv b \bmod n$ is equivalent to the existence of an integral solution (x, y) to the equation $ax + ny = b$—as such, Bézout's lemma tells us precisely when a solution exists, namely when $\gcd(a, n) \mid b$.

The *Chinese remainder theorem*, named after early Chinese mathematician Sunzi Suanjing, concerns the existence of solutions to systems of *simultaneous* congruences. That is, we fix $b_1, b_2, \ldots, b_r \in \mathbb{Z}$ and moduli $n_1, n_2, \ldots, n_r$, and ask about integral solutions x to the system of congruences

$$\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ \quad \vdots \\ x \equiv b_r \bmod n_r \end{cases}$$

The Chinese remainder theorem goes some way towards classifying when a solution exists, and proving that it is unique up to congruence modulo N, for a suitable value of N. This leads us to the following main result:

Theorem (Chinese remainder theorem)**.** Let m and n be coprime moduli and let $a, b \in \mathbb{Z}$. Then there exists an integer x such that

$$x \equiv a \bmod m \quad \text{and} \quad x \equiv b \bmod n$$

Moreover, if y is another integer satisfying both congruences, then $x \equiv y \bmod mn$.

The Chinese remainder theorem can be used for *secret-sharing*. Suppose my 4-digit PIN is P. I tell Alice that $P \equiv 2 \bmod 16$, and I tell Bob that $P \equiv -16 \bmod 625$. Neither Alice nor Bob can say very much about my PIN, but since $16 \perp 625$ and $16 \times 625 = 10000$, by the Chinese remainder theorem, if Alice and Bob share their information with each other, then they can recover my PIN.

A suggestion for an generalisation of the Chinese remainder theorem is to consider the case when there are $r \geq 1$ congruences, not necessarily exactly two congruences. We can say that r integers $n_1, n_2, \ldots, n_r$ are *coprime* if their only common divisors are units—that is, if $d \in \mathbb{Z}$ is such that $d \mid n_i$ for all $1 \leq i \leq r$, then $d = 1$ or $d = -1$. In this case, prove that a solution x exists to the system of r congruences, and show if y is another solution, then $x \equiv y \bmod N$ for a suitable choice of modulus N.

Another suggestion for generalisation is to consider what happens in the case when m and n are not required to be coprime. However, this is covered in the text, so if you wish to take this route, then you should think of some further applications or generalisations.

Public key cryptography

Alice wants to securely send Bob a message. Bob has a *public key*, used for *encryption*, and a *private key*, used for *decryption*. Bob sends Alice his public key, which she uses to encrypt the message, and he keeps his private key to himself; Alice then sends her encrypted message, and Bob uses his private key to decrypt the message.

The idea of public key cryptography is to make the private key very difficult to find with knowledge of the public key. Since the public key can only be used to *encrypt* messages, it is then of no use to someone intercepting the encrypted message.

RSA is a public-key cryptosystem which derives from the theory of modular arithmetic. Although the title of the project, the main result of the project is actually a result called *Euler's theorem*:

Theorem (Euler's theorem)**.** Let n be a modulus and let $a \in \mathbb{Z}$ coprime to n. Then

$$a^{\varphi(n)} \equiv 1 \bmod n$$

where $\varphi(n)$ is the **totient** of n, i.e. the number of elements of the set $[n]$ which are coprime to n.

The application of Euler's theorem to the RSA cryptosystem works as follows:

- Let p and q be positive prime numbers, and let $n = pq$.
- Choose $e \in \mathbb{Z}$ with $1 < e < (p-1)(q-1)$ and $e \perp (p-1)(q-1)$. The pair (n, e) is called the **public key**.
- Choose $d \in \mathbb{Z}$ with $de \equiv 1 \bmod (p-1)(q-1)$. The pair (n, d) is called the **private key**.
- To encrypt a message M (which is encoded as an integer), compute $K \in [n]$ such that $K \equiv M^e \bmod n$. Then K is the encrypted message.
- The original message M can be recovered by noticing that $M \equiv K^d \bmod n$.

You should prove that the algorithm defined above is correct—that is, with p, q, d, e as chosen, that $(M^d)^e \equiv M \bmod n$. You should then apply this to actually encrypt a message. (Your message could be something simple, like an integer. If you wish to do something more elaborate, find a way of encoding your message as an integer.)

In addition, you should discuss efficient ways of computing large powers of an integer modulo n to make it feasible on a computer—one such method is *exponentiation by squaring*. More details on this will be distributed to you if you choose this project.

Rubric

Your project will be graded out of a total of 150 points, according to the following criteria, whose weightings are indicated:

- **Appearance and use of LaTeX** (20 points)**.** Your document should be laid out neatly and should look professional. It should be typeset in LaTeX, and should make full use of its functionality in the same way that the LaTeX project did. A more specific breakdown of this criterion is as follows.
  - **Accuracy and appearance:** the extent to which the typeset document is neat, professional and readable.
  - **Document structure:** use of sections and subsections, paragraphs, and both bulleted and enumerated lists.
  - **Text formatting:** use of emphasis (e.g. bold face, italic or underlined text), text alignment and different fonts.
  - **Mathematical notation:** use of math mode to typeset mathematical notation, appropriate use of variables and symbols, in-line and displayed equations, and aligned equations.
  - **Results, definitions and references:** appropriate use of definition, theorem and proof environments, and use of labels and references.
- **Selection of material** (20 points)**.** Your document should be self-contained, but may assume knowledge of the sections on induction, logic, sets and functions. Any other definitions and preliminary results needed to understand the statement and proof of your main result, and material in subsequent sections, should be developed in your project.
- **Comprehensibility and examples** (20 points)**.** Your document should be comprehensible to another student in the course, and should contain examples illustrating the concepts and results covered.
- **Mathematical correctness** (30 points)**.** The definitions, result statements and proofs in your document should all be mathematically correct, and should be written in enough detail that another student in the course can understand them.
- **Accuracy of mathematical writing** (30 points)**.** Your use of mathematical notation and terminology should be accurate, and your variables should be correctly quantified.
- **Prescribed questions** (30 points)**.** When you have selected your project, you will receive a list of questions that your project must address. Your document should answer these questions correctly, although you do not need to specifically identify where in the project they are answered.

Academic honesty and integrity

As with homework and quizzes, the academic honesty and integrity policies of the syllabus apply to the project. To make sure that you avoid plagiarism in your project, make sure that you:

- Acknowledge any help you receive from classmates, or anyone else, and say how they helped you.
- Cite any external sources you used to learn about the material in your project, such as websites, articles or books. If you cite a website, include the URL of the specific web page(s) that you used.
- Write up everything you do completely independently. Do not copy from another person or source, and destroy any permanent records made from discussions with others before writing up your work.
- Do not show other people your project work until after the submission deadline. (Verbal discussion is fine, but pointing to a proof you wrote and saying 'this is how I did it' is not.)

Given the heavy weighting of the course project in your final grade and the 'independent study' nature of the project, these policies will be strictly enforced. You will be uploading your project to Canvas, which has automatic plagiarism detection software. If plagiarism is detected in your project, it will not receive any credit.

If at any point you are unsure if something you are doing goes against the academic honesty and integrity policies, then please ask Clive as soon as possible!