CM30173/CM50210 Self assessment

Purpose

To help you to evaluate whether you are prepared for the mathematical content of the course.

A user's guide

1. Spend as long as you want and consult as many resources as you wish!
2. Fill in the self evaluation at the end.
3. Hand in: your solutions **including working**, and self evaluation on Tuesday 3rd in the first lecture.
4. Once returned: consider feedback, your self evaluation, list of resources used and time taken *together* in order to assess:
   - Whether you are prepared for the maths in the course
   - Whether you need to spend extra time on the mathematical parts of the course
   - What resources worked best for you
5. Make an appointment during office hours to discuss the outcome if you wish.

Set notation

1. Write out the members of the set $\{0,1\}^3$
2. Describe in one sentence the members of the set

$$\bigcup_{i=m+1}^{\infty} \{0,1\}^i$$

   for some fixed $m \in \mathbb{N}$.

3. What is the cardinality of the following sets?
   (a) The set of all strings of length n of symbols 0 and 1
   (b) The power set 2^A of A
   (c) $\prod_{1 \le i \le n} A_i$ in terms of $|A_1|, |A_2|, \ldots, |A_n|$

Numbers

1. Let $a = 1001$ and $b = 1100$ be binary numbers, give the following in hexadecimal: $a,\ b,\ a \oplus b$
2. Give each hexadecimal number in binary: $A,\ D,\ F$
3. What are the defining properties of a prime number?
4. Find the prime decomposition of 5184; why is this job harder for the number 4819?
5. State the Fundamental Theorem of Arithmetic.

6. How many numbers $0 \leq n < 15$ are relatively prime to 15? Can you work this out without listing them?
7. Find $\gcd(10, 15)$ and $\operatorname{lcm}(10, 15)$.
8. Calculate the following:

$$\begin{array}{ccc} (10-3) \bmod 5, & (-123) \bmod 5, & 2^4 \bmod 5, \\ 2^{17} \bmod 5, & (-123 \times 2^{17}) \bmod 5, & 2^{-1} \bmod 5 \end{array}$$

9. Find some x mod 15 such that

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

10. Why you can't find an x mod 18 such that

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 6 \end{aligned}$$

Structures

First, a reminder of some definitions which you should have seen before:

Definition (Group)**.**
A group $(G, \circ)$ is a set G and a binary operation $\circ$ on G such that:

- (Associative) $\forall\, a, b, c \in G,\ a \circ (b \circ c) = (a \circ b) \circ c$
- (Identity) $\exists\, e \in G\ \forall\, a \in G,\ a \circ e = e \circ a = a$ and we call e the identity.
- (Inverses) $\forall\, a \in G\ \exists\, b \in G,\ a \circ b = b \circ a = e$ and we call b the inverse to a.

A group is Abelian if $\forall\, a, b \in G,\ a \circ b = b \circ a$.

Definition (Ring)**.**
A ring $(R, +, \times)$ is set R with two binary operations (arbitarily denoted) $+, \times$ on R such that:

- $(R, +)$ is an Abelian group with identity 0.
- The operation $\times$ is associative: $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$.
- There is a multiplicative identity 1 ($1 \neq 0$) such that $a \times 1 = 1 \times a = a$ for all $a \in R$.
- The operation $\times$ distributes over $+$: $a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = (b \times a) + (c \times a)$ for all $a, b, c \in R$

R is a commutative ring if $a \times b = b \times a$ for all $a, b \in R$.

Definition (Field)**.**
A field is a commutative ring in which all non-zero elements have multiplicative inverses.

1. Which of the following are groups? Explain your answer.

$$(\mathbb{N}, +), \quad (\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{Z}, \times), \quad (\mathbb{Q}, \times), \quad (\mathbb{R}, \times),$$

2. Which of the following are rings? fields? Explain your answer.

$$(\mathbb{N}, +, \times), \quad (\mathbb{Z}, +, \times), \quad (\mathbb{Q}, +, \times), \quad (\mathbb{R}, +, \times),$$

3. Give an example of a non-Abelian group.

4. Let $(G, \circ)$ be a group. Show that
   - If $a \circ b = a \circ c$ then $b = c$
   - If $b \circ a = c \circ a$ then $b = c$

5. Show that in any commutative ring, $0 \times a = 0 = a \times 0$

6. Show that in any field, if $a \times b = 0$ then at least one of a and b is zero.

7. Let $\mathbb{Z}_n$ be the integers modulo $n \in \mathbb{N}$. When are the following statements true:
   (a) $(\mathbb{Z}_n, +)$ is a group
   (b) $(\mathbb{Z}_n, \times)$ is a group
   (c) $(\mathbb{Z}_n, +, \times)$ is a ring
   (d) $(\mathbb{Z}_n, +, \times)$ is a field

Functions

1. Give concise definitions of *injective function*, *surjective function* and *bijective function.*

2. Give a binary operation such that the set of bijective functions on some set A is a group. Explain.

Computability

1. Let ϵ, c be arbitrary constants such that $0 < \epsilon < 1 < c$. Place the following in increasing order of their asymptotic growth rates:

$$c^n, \quad \ln \ln n, \quad n^c, \quad c^{c^n}, \quad n^{\ln n}, \quad 1, \quad \exp(\sqrt{\ln n \ln \ln n}), \quad n^n, \quad \ln n, \quad n^\epsilon$$

2. How many multiplication operations are required to calculate 2^{19} using the *square-and-multiply* algorithm?

3. What is meant by the term “computationally infeasible”?

Self evaluation and feedback

Self evaluation:

- Estimated *total* time to complete:
- Proportion of time consulting resources:
- Resources used (including books, people, notes, websites etc.):
- How familiar to you was the content and notation?
- How difficult or easy did you find the questions?
- Were any ideas gleaned from resources particularly helpful? How did they help?
- If you decided not to answer some or all questions consider why that was:
- Do you need to look at any of the methods or ideas again?

Feedback from lecturer: