MATH2068/2988 Sample Quiz

Name _____

Student ID _____

Tutor's name _____

Tutorial room _____

Tutorial time and day _____

Signature _____

Time allowed: 45 minutes

The quiz for MATH2068/2988 will be held in the tutorials in Week 9 (4–5 October). This quiz, which is the same for both units, contributes 10% towards the final mark, except that the better mark principle applies: if your mark in the exam is better than your mark in the quiz, then your exam mark will count for 80% rather than 70%, and your quiz mark will not count. For this reason, there is no point applying for Special Consideration or Special Arrangements in relation to the quiz: the mark reweighting it would produce is automatic anyway.

The quiz will cover material relating to weeks 1–6 of the MATH2068/2988 lectures, up to and including multiplicative functions, the Möbius Inversion Formula, and the RSA cryptosystem, and the associated Tutorials 1–6 (including Tutorial 6 in Week 7) and Computer Labs 1–6 (including Computer Lab 6 in Week 7). For the purposes of this quiz, which consists of short-answer questions, only the unstarred computational questions in those tutorials are relevant, not the proof questions or starred questions; and only the underlying ideas in those computer labs will be tested, not the details of MAGMA syntax or programming skills. This sample quiz will give you an idea of the sorts of questions that will be asked. (The order of the questions here does not necessarily indicate anything about the order of questions in the actual quiz.) It is strongly recommended that you try to complete this sample quiz under exam conditions in the assigned time, before looking at the solutions. This should help you identify which topics you need to focus on in your revision.

1. Each question has a box for your working and a smaller box for your final answer. You *must* write your answer in the answer box even if it is included in the working.
2. If your answer is correct, you will receive full marks for the question; if your answer is incorrect, partial marks *may* be awarded for your working.
3. Please write carefully and legibly using ink and *not* pencil.
4. The complete quiz paper, together with any other pages used for working, must be handed in at the end of the quiz.
5. Only University-approved non-programmable calculators, with the sticker from the Student Centre, may be used.

This quiz paper has six pages and 15 questions.

1. Find $\gcd(10^{20}, 84)$.

Answer

2. Find the smallest prime which divides 123456789123456789.

Answer

3. Find which element of $\{1, 2, \cdots, 58\}$ is inverse to 17 modulo 59.

Answer

4. Find the order of 5 modulo 31.

Answer

5. Find the residue of 3^{1010} modulo 7.

Answer

6. Find the unique $x \in \{0, 1, 2, \cdots, 194\}$ such that $x \equiv 3 \pmod{13}$ and $x \equiv 2 \pmod{15}$.

Answer

7. Find the residue of 2^{1010} modulo 111.

Answer

8. Find $\sigma(640)$, the sum of the positive integer divisors of 640.

Answer

9. What is the smallest positive integer with exactly 10 positive divisors?

Answer

10. If a simple substitution cipher encrypts the word `SUGAR` as `JWZXD`, what is the decryption of `XDZWJ`?

Answer

11. What would be the output of the following MAGMA commands?

```
> V:=VigenereCryptosystem(3);
> encipheringkey:=V!"BAY";
> Enciphering(encipheringkey,Encoding(V,"HOTEL"));
```

Answer

12. Suppose you are given two long ciphertexts `sct1` and `sct2` and told that one of them is some ordinary English text enciphered with a block transposition cipher and the other is the same English text enciphered with a Vigenere cipher. If you see the following MAGMA code, which one was (probably) enciphered using the block transposition cipher?

```
> CoincidenceIndex(sct1);
0.065201231214704805740688281507 1
> CoincidenceIndex(sct2);
0.041587978794878087462142783659 4
```

Answer

13. If an RSA cryptosystem has public key $(22, 3)$, what is the decryption exponent?

Answer

14. Suppose that an RSA cryptosystem has a public key of $(33, 3)$. Encrypt the message $[4, 6]$.

Answer

15. What would be the output of the following MAGMA commands?

```
> p:=NextPrime(100);
> 6^p mod p;
```

Answer

This is the last page of the quiz paper.