# Math 3CY3, Test 2

Bradd Hart, Nov. 1, 2018

There are 5 questions and each question is worth 5 marks. Please write complete answers to all of the questions in the test booklet provided. Partial credit may be given for your work. Unless otherwise noted, you need to justify your solutions in order to receive full credit. Please be sure to include your name and student number on all sheets of paper that you hand in.

1. (a) How many fields are there up to isomorphism with $8^2, 9^2$ and $10^2$ elements?
   (b) Is the polynomial $x^2+1$ irreducible over $Z_2$? $Z_3$?

2. As a toy example of RSA, we use the number $n = 77$ and the exponent $e = 7$.
   (a) What is the deciphering exponent for this key?
   (b) Encode the message $m = 7$.

3. Given a large number $n$ (say with more than 100 digits), explain how you would approach determining if it was prime. It is not sufficient to state the name of a test; you must explain how that test would be carried out.

4. Given that

$$880525^2 \equiv 2,\ 2057202^2 \equiv 3,\ 648581^2 \equiv 6 \text{ and}$$

$$880525 \times 2057202 \times 648581 \equiv 720341 \bmod 2288233,$$

   use this information to factor 2288233.

5. Prove that the characteristic of any finite field is a prime number.