

**Assignment 1**

Due: 7/9/2009

1. For each prime  $p$  less than 30 find an integer  $a$  such that  $\text{ord}_p(a) = p - 1$ .
2. Find the general solution of the simultaneous congruences

$$7x \equiv 1 \pmod{13},$$

$$6x \equiv 3 \pmod{15},$$

$$4x \equiv 5 \pmod{11}.$$

3. (MATH2068 only)

- (i) Let  $n$  be a positive integer and  $p$  a prime divisor of  $n^2 - 1$ . Show that either  $n \equiv 1 \pmod{p}$  or  $n \equiv -1 \pmod{p}$ .
- (ii) By Fermat's Little Theorem  $2^{46} \equiv 1 \pmod{47}$ . Use Part (i) to deduce that  $2^{23} \equiv \pm 1 \pmod{47}$ .
- (iii) Since  $2 \equiv 7^2 \pmod{47}$  it follows that  $2^{23} \equiv 7^{46} \pmod{47}$ . Use this and Fermat's Little Theorem to eliminate one of the possibilities in Part (ii), and hence show that  $2^{23} - 1$  is not prime.

3. (MATH2988 only)

Let  $p$  be a prime and let  $m$  be the Mersenne number  $2^p - 1$ . Let the sequences  $s_i$  and  $t_i$  be defined as in Question 6 of Tutorial 5, and suppose that  $s_{\frac{1}{4}(m+1)} \equiv 0 \pmod{m}$ . [Note: See the MATH2988 web page for some relevant extra reading.]

- (i) By imitating the method used in Exercise 4 of Tutorial 3, or otherwise, prove that if  $q$  is a prime then  $q$  must be a divisor of at least one element of the set  $\{t_i \mid 1 \leq i \leq q + 1\}$
- (ii) Let  $q$  be a prime and let  $k$  be the least positive integer such that  $q|t_k$ . Using Exercise 6 (i) of Tutorial 5, show that if  $n \in \mathbb{N}$  then  $q|t_n$  if and only if  $k|n$ . (We call  $k$  the *entry point* for  $q$  in the sequence  $(t_n)$ .)
- (iii) Show that if  $q$  is any prime divisor of  $m$  then its entry point in  $(t_n)$  is  $\frac{1}{2}(m + 1) = 2^{p-1}$ . (Hint: The entry point divides  $2^{p-1}$  but not  $2^{p-2}$ .)
- (iv) Deduce from Parts (ii) and (iii) that the only possible prime divisor of  $m$  is  $m$  itself.

Parts (ii) and (iii) of the next question (overleaf) are to be done using magma. Start a magma session, and type

```
load "asst1data.txt";
SetLogFile("a1.txt");
```

(This will ensure that magma saves a record of your session in a file called "a1.txt".) Do the questions, and after ending your magma session, submit the file asst1 for marking by clicking the "handin" icon on your desktop and then entering the keyword m2068asst. If doing the questions on your home computer, use the Computer Tutorial Log File Upload page.

You may (if you wish) edit the file `asst1` before handing it in; e.g. you could use a text editor to remove superfluous incorrect lines. **But make sure that it contains the decrypted message and the magma commands used to find it.**

4. (Both MATH2068 and MATH2988)

As an operative with the government department of Internal Security you are investigating the activities of a covert literary society. Under interrogation a member reveals that they use a system consisting of a block transposition cipher followed by a Vigenère cipher. You discover an enciphered message in the file “ass1ciphertext.txt” on the MATH2068 web page.

- (i) Find the Vigenère period and decryption key, using the javascript Vigenère key finder.
- (ii) Set up a Vigenère cryptosystem with the appropriate period, and use the decryption key you have found to undo the Vigenère part of the enciphering.
- (iii) Use the tools from Computer Tutorial 5 to find the transposition key, and decrypt the message. (Note: The bound for the CI in the CheckPeriod command used in Exercise 3 of Computer Tutorial 5 was too high. It can be safely reduced to 0.007. Similarly, for the FindAdjacencies command you will need to use a bound for the CD that is below 0.004 to find all the correct adjacencies.)