

CM10196: Discrete Mathematics for Computation

Problem Sheet 8

Set December 3rd 2007; hand in by Dec 13th 2007

Coursework forms 25% of the assessment for this unit. Coursework will consist of your answers to eight problem sheets, plus the “learning log” exercise. Each problem sheet will be marked out of 10, and there will be 20 marks for the learning log.

On this sheet, each question is worth two marks.

For the first two questions, you need to know that the set $4\mathbb{Z} + 1$ consists of those integers of the form $4n + 1$ for some integer n .

1. Prove that $4\mathbb{Z} + 1$ is a monoid under the usual multiplication. That is, prove that multiplying two elements of this set gives you another element of the set; and that there is a unit element in the set.
2. We say that a positive element is *prime* in $4\mathbb{Z} + 1$ if it has no positive factors in this set, apart from 1 and itself. Find the smallest two positive numbers in the set which are prime in $4\mathbb{Z} + 1$ but not prime in the usual sense.
3. Consider the *exclusive or* operation on truth values, written \oplus , with truth table:

x	y	$x \oplus y$
t	t	f
t	f	t
f	t	t
f	f	f

Show that this operation makes the set $\{\mathbf{t}, \mathbf{f}\}$ into a group. (You have to work out what the unit is, and what the inverses are, and show that the operation is associative.)

4. Prove the cancellation law for groups, i.e. that in any group, for any a, b and c , if $ab = ac$ then $b = c$ and if $ba = ca$ then $b = c$.
5. Write out the multiplication table for the group $(\mathbb{Z}/p\mathbb{Z})^*$ where $p = 7$. When you have done this, calculate the order of each element.