

## Second test, Math4181, Fall 2007

The second test will be held on Friday November 16. This will cover material from Section 2.4, chapter 3, and some of Chapter 4.

### Additional Practice for Second test, Math4181, Fall 2007

(1) Theory: Make sure you would be able to state and prove the Chinese remainder theorem. (See section 4.1)

(2) Computation: Make sure you can solve problems such as:

If  $x \equiv 2 \pmod{5}$ ,  $x \equiv 3 \pmod{7}$  and  $x \equiv 1 \pmod{9}$ , what the smallest possible positive integer value of  $x$ ?

[The answer turns out to be 262, but you should show your working. See class notes for Wednesday November 7 for a method to solve such systems of congruences.]

### Solutions to first Practice for Second test, Math4181, Fall 2007

**For theorems:** See proofs given in text book, on pages indicated in previous handout, or in class notes.

#### Computational problems: solutions

Different numbers would be used in test questions.

- **Question:** Which of the following rings is *not* a field?

$$\mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_9, \mathbf{Z}_{11}$$

For the example or examples which are not fields, give a non zero element which does not have a multiplicative inverse.

#### Solution:

$\mathbf{Z}_n$  is a field if and only if  $n$  is a prime. So  $\mathbf{Z}_6$  and  $\mathbf{Z}_9$  are not feilds.

In  $\mathbf{Z}_6$ ,  $\bar{2}$  does not have an inverse, since it is a zero divisor, since  $\bar{2} \times \bar{3} = \bar{0}$  in  $\mathbf{Z}_6$ .

In  $\mathbf{Z}_9$ ,  $\bar{3}$  does not have an inverse, since it is a zero divisor, since  $\bar{3} \times \bar{3} = \bar{0}$  in  $\mathbf{Z}_9$ .

- **Question** Find the value of  $\phi(20)$ , where  $\phi$  is the Euler phi function.

#### Solution

$\phi(20) = |U_{20}|$ , and

$$U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

So  $\phi(20) = 8$ .

- **Question** Find all the subgroups of  $U_{18}$ .

#### Solution

$$U_{18} = \{1, 5, 7, 11, 13, 17\}.$$

Since  $|U_{18}| = 6$ , and  $U_{18}$  is abelian, we have  $U_{18} \cong Z_6$ , since all abelian subgroups of order 6 are cyclic, and a cyclic subgroup of order  $n$  is isomorphic to  $\mathbf{Z}_n$ .

We know that  $Z_6$  has subgroups  $\langle d \rangle$  for positive integers  $d$  with  $d|6$ , so the subgroups of  $\mathbf{Z}_6$  are  $\langle 1 \rangle = \mathbf{Z}_6$ ,  $\langle 2 \rangle$ ,  $\langle 3 \rangle$ ,  $\langle 6 \rangle = \{0\}$ .

So,  $U_{18}$  must also have 4 subgroups, including  $U_{18}$  and  $\{1\}$ .

What is the order of 5? (In the following, numbers are taken to be in  $U_{18}$ , and overlines are omitted.)

$5^2 = 25 = 7$ ,  $5^3 = 5 \times 7 = 35 = -1$ , so 5 has order 6 (since it doesn't have order 1, 2, 3.

So  $5^2 = 7$  has order 3, and  $5^3 = -1$  has order 2.

we have subgroups  $\langle 7 \rangle = \{1, 7, 49 = 13\}$  and  $\langle -1 \rangle = \{1, -1\}$ .

So the list of all subgroups of  $U_{18}$  is:

$$\begin{aligned} &\{1\} \\ &\{1, 17\} \\ &\{1, 7, 13\} \\ &U_{18} \end{aligned}$$

- **Question** Use Fermat's little theorem to find an integer  $a$  with  $0 \leq a < 37$  such that  $3^{400} \equiv a \pmod{37}$ .

**Solution** By Fermat's little theorem,  $3^{36} \equiv 1 \pmod{37}$ .

$400 = 36 \times 11 + 4$ , so  $400 \equiv 4 \pmod{36}$ , so

$$3^{400} \equiv 3^4 = 81 \equiv 7 \pmod{37}.$$

The solution is  $a = 7$

- **Question** Write out the elements of each of the cosets of  $\langle \bar{5}_{13} \rangle$  in  $U_{13}$ .

**Solution**

We have

$$U_{13} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

and

$$\langle \bar{5}_{13} \rangle = \{1, 5, 12, 8\},$$

So the cosets of  $\langle \bar{5}_{13} \rangle$  are:

$$\begin{aligned} \langle \bar{5}_{13} \rangle &= \{1, 5, 12, 8\}, \\ 2\langle \bar{5}_{13} \rangle &= \{2, 10, 11, 3\}, \\ 4\langle \bar{5}_{13} \rangle &= \{4, 7, 9, 6\}. \end{aligned}$$

- **Question** Which of the following groups are isomorphic?

$$U_{16}, \mathbf{Z}_8, U_{15}, U_{20}$$

**Solution**

All these groups have order 8. We need to work out the structure of these groups, i.e., write them as direct sums of smaller groups, or determine whether they are cyclic.

In  $U_{16}$ :

$$\langle 3 \rangle = \{1, 3, 9, 11\}$$

$$\langle 15 \rangle = \{1, 15\}$$

Since  $|\langle 3 \rangle| \times |\langle 15 \rangle| = 8$  and  $\langle 3 \rangle \cap \langle 15 \rangle = \{1\}$ , we have

$$U_{16} = \langle 3 \rangle \oplus \langle 15 \rangle \cong \mathbf{Z}_4 \oplus \mathbf{Z}_2$$

In  $U_{15}$ :

$$\langle 2 \rangle = \{1, 2, 4, 8\}$$

$$\langle 14 \rangle = \{1, 14\}$$

Since  $|\langle 2 \rangle| \times |\langle 14 \rangle| = 8$  and  $\langle 2 \rangle \cap \langle 14 \rangle = \{1\}$ , we have

$$U_{15} = \langle 2 \rangle \oplus \langle 14 \rangle \cong \mathbf{Z}_4 \oplus \mathbf{Z}_2$$

In  $U_{20}$ :

$$\langle 3 \rangle = \{1, 3, 9, 7\}$$

$$\langle 19 \rangle = \{1, 19\}$$

Since  $|\langle 3 \rangle| \times |\langle 19 \rangle| = 8$  and  $\langle 3 \rangle \cap \langle 19 \rangle = \{1\}$ , we have

$$U_{15} = \langle 3 \rangle \oplus \langle 19 \rangle \cong \mathbf{Z}_4 \oplus \mathbf{Z}_2$$

The maximum order of an element of  $\mathbf{Z}_4 \oplus \mathbf{Z}_2$  is 4, since this is the largest value of  $\text{lcm}(o(a), o(b))$  for  $a \in \mathbf{Z}_4$  and  $b \in \mathbf{Z}_2$ . But  $\mathbf{Z}_8$  has an element of order 8. So these groups are not isomorphic.

So  $U_{15}$ ,  $U_{16}$  and  $U_{20}$  are isomorphic to each other, and not isomorphic to  $\mathbf{Z}_8$ .

- **Question** Write down explicitly an isomorphism from  $Z_6, +$  to  $U_9, \times$ . Write the image of every element under this isomorphism.

**Solution** Both these groups are abelian, order 6, so they are isomorphic, and the isomorphism is determined by mapping a generator of one to a generator of the other.

1 is a generator of  $Z_6$ .

$U_9 = \{1, 2, 4, 5, 7, 8\}$  We have  $2^2 = 4, 2^3 = 8$ , so 2 does not have order 1, 2, 3, so must have order 6, and so is a generator of  $U_9$ .

We have an isomorphism given by

$$f : i \mapsto 2^i$$

explicitly, the images of all elements of  $Z_6$  are as follows:

$$\begin{array}{l} 0 \mapsto 1 \\ 1 \mapsto 2 \\ 2 \mapsto 4 \\ 3 \mapsto 8 \\ 4 \mapsto 7 \\ 5 \mapsto 5 \end{array}$$

- **Question** What are the possible orders of elements of  $Z_{10}, +$ ? How many elements have each order?

**Solution** Since  $|Z_{10}| = 10$ , possible orders of elements are 1, 2, 5, 10.

To determine the number of elements of each order, we can just take powers of each element, or use the following method:

We know that  $Z_{10} \cong Z_2 \oplus Z_5$ , and we know that  $o((a, b)) = \text{lcm}(o(a), o(b))$  for  $(a, b) \in Z_2 \oplus Z_5$ . We can make a table of orders of elements:

|     |        |             |    |    |    |    |
|-----|--------|-------------|----|----|----|----|
|     | $b$    | 0           | 1  | 2  | 3  | 4  |
|     | $o(b)$ | 1           | 5  | 5  | 5  | 5  |
| $a$ | $o(a)$ | $o((a, b))$ |    |    |    |    |
| 0   | 1      | 1           | 5  | 5  | 5  | 5  |
| 1   | 2      | 2           | 10 | 10 | 10 | 10 |

So there is one element of order 1, one element of order 2, 4 elements of order 5 and 4 elements of order 10.

- **Question** Write  $U_{23}$  as a direct sum of two subgroups, neither of which is  $\{1\}$ .

**Solution**

First note that  $|U_{23}| = 22$ .

Now compute to find that

$$\langle 2 \rangle = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$$

and

$$\langle 22 \rangle = \{1, 22\}.$$

Since  $|\langle 2 \rangle| \times |\langle 22 \rangle| = 22$  and  $\langle 2 \rangle \cap \langle 22 \rangle = \{1\}$ , we have

$$U_{23} = \langle 2 \rangle \oplus \langle 22 \rangle$$

- **Question** What is the order of  $\bar{3}$  in  $U_{23}, \times$ ?

**Solution**

In  $U_{23}$ , we have  $\langle 3 \rangle = \{1, 3, 9, 4, 12, 13, 16, 2, 6, 18, 8\}$ , so the order of  $\bar{3}_{23}$  in  $U_{23}$  is 11.

(Note, the only possible orders are 1, 2, 11 and 22, so we could just compute  $3^1, 3^2 = 9$ , and  $3^{11} = 3^{8+2+1} = 3^8 3^2 3$ , and since  $3^4 = 81 = 12$ , so  $3^8 = 12^2 = 6$ , so  $3^{11} = 6 \times 9 = 1$ .)

- **Question** What is the order of  $\bar{3}$  in  $Z_{23}, +$ ?

**Solution** Since  $(3, 23) = 1$ , we know that 3 generates  $Z_{23}$ , and so must have order 23.

- **Question** Is  $U_{11}$  cyclic? If it is, find a generator, if not, explain why not.

**Solution** We know that  $|U_{11}| = 10$ . Compute to find that in  $U_{11}$ ,

$$\langle 2 \rangle = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}, \text{ so } U_{11} \text{ is cyclic, generated by } 2.$$

- **Question** What are the components of  $\overline{15}_{22}$  in the direct sum  $\mathbf{Z}_{22} = \langle \overline{2} \rangle \oplus \langle \overline{11} \rangle$ ?

Find the order of each component, and use this to determine the order of  $\overline{15}$  in  $\mathbf{Z}_{22}$ .

**Solution**

In  $\mathbf{Z}_{22}$ , we have

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$$

$$\langle 11 \rangle = \{0, 11\},$$

so we see we can decompose 15 as  $15 = 4 + 11$ .

$\langle 2 \rangle$  has order 11, which is prime, so any non 0 element of this subgroup has order 11. So 4 has order 11.

For a similar reason, 11 has order 2.

So the order of 15 is  $\text{lcm}(11, 2) = 22$ .

- **Question** What are the components of  $\overline{15}_{22}$  in the direct sum  $U_{22} = \langle \overline{3} \rangle \oplus \langle \overline{21} \rangle$ ?

Find the order of each component, and use this to determine the order of  $\overline{15}$  in  $U_{22}$ .

**Solution** We have  $U_{22} = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$ .

In  $U_{22}$ ,

$$\langle 3 \rangle = \{1, 3, 9, 5, 15\}$$

$$\langle 21 \rangle = \{1, 21\}$$

So 15 decomposes as  $15 \times 1$ .

Since 15 is in a subgroup of order 5, and is not the identity, the order of 15 is 5.