CS 235
Spring 2010

Exam 2

Part I (15 points): Multiple Choice: Each of the following multiple choice questions is worth 3 points. There is no partial credit for this sections and each question has 1 and only 1 correct answer.

THE ANSWERS TO THE MULTIPLE CHOICE QUESTIONS ARE:

1. d (or e) 2. d 3. d 4. b 5. a

1. Consider the ring Z_{27}.
   Two questions: What is $\Phi(27)$? and,
   Which of the following are the possible orders of units in Z_{27}
   (a) $\Phi(27) = 18$ and the possible orders are 1, 3, 18
   (b) $\Phi(27) = 16$ and the possible orders are 1, 3, 6, 9
   (c) $\Phi(27) = 21$ and the possible orders are 1, 3, 7, 21
   (d) $\Phi(27) = 18$ and the possible orders are 1, 3,6, 9 and 18
   (e) None of the above

2. Consider the 4 element set $Z_4 = \{0,1,2,3\ \}$ with the usual mod 4 addition and multiplication. Z_4 is not a field. Why not ? That is, which of the following axioms for fields fails for Z_4 ?
   (a) the axiom stating there is an identity element for multiplication.
   (b) one of the distributive axioms.
   (c) the axiom stating there is an additive inverse for every element
   (d) the axiom stating there is a multiplicative inverse for every element
   (e) Z_4 is not closed under multiplication

3. Now let's change the addition and multiplication for $\{0,1,2,3\}$ in the last problem to be different than the usual Z_4 and given by the following addition and multiplication tables. Assuming this addition and multiplication make $\{0,1,2,3\ \}$ a field, what are the values of A and B in the multiplication table below.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	A	1
3	0	3	1	B

   According to the axioms for fields, the value for the letters A and B in the multiplication table have to be

(a) A = 1, B = 1

(b) A = 2, B = 2

(c) A = 2, B = 3

(d) A = 3, B = 2

(e) none of the above

4. Which of the following is an inverse of 3 mod 70 ?

   (a) 67

   (b) 47

   (c) 59

   (d) 42

   (e) There is no inverse of 3 (mod 70)

5. Assume F is a field and you are give three different non-zero elements a,b,c of F. Consider the following statements about F.

   (a) $\exists$ x $\in$ F, ax + b = cx

   (b) $\exists$ x $\in$ F, xx=a

   (c) $\exists$ x $\in$ F, a^x = c

   (d) $\forall$ x $\in$ F, ax+bx = (ab)x

   Which of the 4 statements above is true for every field F and a,b,c as above.

Part II (16 points): Short answer - Do any 2 of the following 3 problems. Each counts 8 points.

6. Show that if n is a product of two distinct primes, n = qp, p,q prime, then for any a, $a^{\phi(n)+1} = a$ (mod n).

   (Hints: i. You can use the fact that in this case $\phi(n)$ = (p-1)(q -1).

   ii. You can directly use Euler's theorem to get this result for many a, for the rest you need to give a short direct proof.)

   Answer: If a is relatively prime to n, then Euler's theorem directly applies to yield $a^{\phi(n)} = 1$ (mod n)and hence, multiplying by a a on each side of the equation yields $a^{\phi(n)+1} = a$ (mod n).

   So we need only handle the case where (a,n) >1.

   In this case a mod n < n and one (but not both) of p,q is a factor of a.

   Without loss of generality say p is not factor of a and q is a factor of a, so (a, p)=1 and so $a^{\phi(p)+1} = a$ (mod p).

   This implies that $a^{\phi(n)+1} = a$ (mod p) (this is easy by the fact that $\phi(n) = (p-1)(q-1)$.)

   and this in turn implies that $a^{\phi(n)} = a$ (mod n).

   This last implication follows from the fact that, since q | a and $a^{\phi(n)+1} = a$ (mod p), q | $(a^{\phi(n)+1} - a)$, and p also divides $(a^{\phi(n)+1} - a)$, so pq | $(a^{\phi(n)+1} - a)$ and so $a^{\phi(n)+1} = a$ (mod n).

(Hints: i. You can use the fact that in this case $\phi(n)$ = (p-1)(q- 1)(r-1).

ii. You can directly use Euler's theorem to get this result for many a, for th e rest you need to give a short direct proof.)

7. (i) Prove that for any integer n with n and 12 co-prime, $6n^{11} + 9n^9 + 2n^7 + 4n^3 + 3n$ is evenly divisible by 12.

   Ans: $\phi(12) = 4$ so by Euler's theorem, for any co-prime with 12, $n^4 = 1$ mod (12).

   In particular, this gives $n^{11} \equiv n^3$ mod (12), $n^9 \equiv n$ mod (12), $n^7 \equiv n^3$ mod (12).

   It follows that $6n^{11} + 9n^9 + 2n^7 + 4n^3 + 3n$ mod 12 = $6n^3 + 9n + 2n^3 + 4n^3 + 3n$ mod 12 = $12n^3 + 12n$ mod 12 =0, when n and 12 are co-prime.

   (ii) Give an example of an integer n where $6n^{11} + 9n^9 + 2n^7 + 4n^3 + 3n$ is not evenly divisible by 12.

   Ans: Some n with (n,12) > 1. 2 is easiest to verify.

8. Recall that the order of a (mod m) is the least number t>0 such that a^t = 1 (mod m).

   Prove that if ab = 1 (mod m) then the order of a (mod m) = the order of b (mod m).

   Ans: Let s be the order of a mod n and t the order of t mod n. We need to prove that s=t. We do this by showing s $\leq t$ and $t \leq s$.

   We have that 1 = $(ab)^s = a^s b^s = 1b^s = b^s$ mod n since s is the order of a. Hence t = order of b $\leq$ s.

   Similarly, we can see that 1 = $(ab)^t = a^t$ mod n and hence s $\leq$ t.

   Hence we have s=t.