

CSE 20 Spring 2009
Exam 3

True or False

___F___ 1. An integer n is odd if and only if it can be written in the form $n = 2m + 1$ where m is an even integer

___T___ 2. For positive integers m and n , mn is odd if and only if m is odd and n is odd.

___F___ 3. For positive integers m and n , mn is even if and only if m is even and n is even.

___T___ 4. For non-negative integer x , and positive integer exponent n ,
 $x = 1 \pmod{n} \Rightarrow x^n = 1 \pmod{n}$

___F___ 5. Suppose that $x = x' \pmod{n}$ and $y = y' \pmod{n}$. Then $x/y = x'/y' \pmod{n}$

___T___ 6. Suppose that $x = x' \pmod{n}$ and $y = y' \pmod{n}$. Then $x+y = x'+y' \pmod{n}$

___T___ 7. If the square root of a positive integer is not an integer, then it must be an irrational number.

___T/F___ 8. Suppose that a, b, c, d are rational numbers and that
 $(ax + b)/(cx + d) = 1$. Is x also a rational number?

Explanation for 8. The book lists this as T, and gives a formula for x . But the formula is not valid if $a = c$, since this would result in division by 0! Consider $a = b = c = d = 1$. The equation is satisfied for all x , including x irrational.

Countability

1. Rational numbers. Recall that these are numbers that can be written as a fraction.

In order to show that they were countable, we had to describe a way to put them into a list. In our approach, we organized this into finite groups. The idea was to then list the items in group 1, then group 2, and so on. The groups got larger as we went from one group to the next, but they were still well defined, and finite, and we could specify how to list their members.

What was the basic idea for the groups, i.e. how did we specify group 1, group 2, or in general, group k ?

The way we did it was to group together the rationals a/b for which $|a| + |b|$ was the same integer k . In the book we started with $k = 3$, and put the 0 and 1 (in their various rational forms) first. There was the presumption that the rationals were in reduced form.

There are other ways of grouping also, that we did not cover. If you had one of these (and it was valid) you should have got full credit.

2. Irrational numbers. Recall that these are numbers that are not integers and cannot be written as a fraction. We proved that this set of numbers cannot be written in a list. That means there is no methodical way of specifying the first, then the second, etc, and that this will result in a list with all the reals.

We did this by supposing that we could do it and then getting a contradiction. Suppose that we could write all the reals in a list

$a_1, a_2, \dots$

This allows us to define a number b of the form

$0.b_1b_2b_3\dots$

where b_k is the integer in the k 'th decimal position in b .

We then showed that b could not be in the list, because there is no a_i that it could be equal to. Give the definition that we used for b , by giving the definition for its k 'th decimal point.

Let b_i be an integer that is not equal to the i 'th decimal in a_i . This means that b cannot be in the list, because it would have to be equal to some b_k , and by construction it differs from b_k in the k 'th digit.

In the book they choose b_i to be 2 when the i th digit of a_i is 1, and choose b_i to be 1 when the i 'th digit of a_i is not equal to 1

2. gcd and lcm

a) Suppose that we have two integers m and n which are written as below, as products of the primes p_i , $1 \leq i \leq k$. In the case of m the exponents for the primes are e_i and in the case of n the exponents are f_i .

$$m = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

$$n = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$$

Write $\gcd(m,n)$ and $\text{lcm}(m,n)$ as the product of these primes also. Hint: define the new exponents in terms of the old ones. Hint: if you have trouble remembering which it is, try a few examples.

$$\gcd(m,n) = p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}, \text{ where } g_i = \min(e_i, f_i)$$

$$\text{lcm}(m,n) = p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}, \text{ where } g_i = \max(e_i, f_i)$$

b) Euclid's algorithm

Use Euclid's algorithm to compute $\gcd(37, 11)$. Please show your work.

$$\begin{array}{r} 37 \quad 11 \\ \quad 3 \quad 4 \\ 11 \quad 4 \\ \quad 2 \quad 3 \\ 4 \quad 3 \\ \quad 1 \quad 1 \end{array}$$

Hence $\gcd = 1$

(You did not have to use this exact format, but had to show the process of successive divisions in some way)

c) gcd written as a linear combination

We proved that for two positive integers m, n that $\gcd(m,n)$ could be written in the form $\gcd(m,n) = am + bn$, where a and b are integers (possibly negative). Sometimes we can just guess and find out a and b for a given m and n . Sometimes this is not so easy, but we can get it by using a back substitution process that we defined in class. Write $\gcd(37,11)$ as a linear combination by determining values for a and b in the expression. Use the back substitution method, and show your work.

$$1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (11 - 2 \cdot 4) = 37 - 3 \cdot 11 - 1 \cdot (11 - 2 \cdot (37 - 3 \cdot 11)) = 3 \cdot 37 - 10 \cdot 11$$

3. Crypto

a) Diffie-Hellman. Recall that DH can be used for establishing a common key between two communicators A and B. This is done using a combination of public and private information. Suppose that the public information consists of:

prime modulus $p = 5$

base $b = 3$

Suppose that the private information known only to A is

$s = 2$

(which satisfies the requirement that $1 < s < p-1$)

The private information known only to B is

$t = 4$

(which also satisfies the requirement that $1 < t < p$)

DH now goes through the following steps

i) A sends a message S to B, and B sends a message T to A.

For the above values of p, b, s, t , what will S and T be??

$$S = 3^2 \pmod{5} = 9 \pmod{5} = 4$$

$$T = 3^4 \pmod{5} = 81 \pmod{5} = 1$$

ii) A then performs a calculation on T to get a key K

Show the calculation that A performs to get K

$$K = 1^2 \pmod{5} = 1 \pmod{5} = 1$$

iii) B then performs a calculation on S to get a key K'

Show the calculations that B performs to get K'

$$K' = 4^4 \pmod{5} = 256 \pmod{5} = 1$$

iv) Are K and K' equal? (Hint, they better be or else A and B will not have the same shared key for doing their encryption/decryption.)

Yes

(Note: the parameters used in this example are such that $t = 4$ does not satisfy the required $1 < t < p-1$, where $p = 5$. However, in this case the Keys still turn out OK. If you pointed this out and then did not do the work because the condition would be violated, you would have also got full credit. If you made mistakes in applying the DH process, which would have nothing to do with this, you would have gotten partial credit depending on the nature of the error).

b) RSA

Recall that RSA can be used to securely send a message M between A and B. This is done with a combination of private and public information.

i) Suppose that the public information consists of modulus $N = 10$

ii) The private information consists of the secret prime factors of N , which in this case are $10 = 2 \times 5$

The value of the Euler function $\phi(N)$ is also private because to easily compute it we need to know p and q . We know that $\phi(N) = (p-1)(q-1)$ which in this case gives us $\phi(10) = 4$. Now if A wants to allow B to communicate with it, it chooses two parameters d and e such that

$$d \cdot e = 1 \pmod{\phi(10)} = 1 \pmod{4}.$$

In this case, suppose that A chooses $d = 3$, and $e = 3$.

We can see that $3 \cdot 3 = 9 = 1 \pmod{4}$, (because $9 = 1 + k \cdot 4$ for some integer k .)

A publicly transmits one of these two parameters, say d , to B, and keeps the other secret.

ii) encrypting and decrypting

B now uses d to encrypt its message M . It is required that M be an integer in the range $1 \leq M < N$, and also that $\gcd(M, N) = 1$.

Suppose B wants to send the (plaintext) message consisting of the number 2.

What is the ciphertext C , using the above choices of N, d, e , that is actually sent from B to A? Show your work.

$$C = 2^3 \pmod{10} = 8 \pmod{10} = 8$$

iii) decryption

When A receives C , it has to decipher it. Show the computation that is made, using the given choices for N, d, e . (Hopefully the result of this calculation will be M !)

Let M' be the deciphered message.

$$M' = 8^3 \pmod{10} = 512 \pmod{10} = 2 = M.$$

(Note: This application of RSA has B sending a message M of 2, and M is supposed to be such that $\gcd(M, N) = \gcd(2, 10) = 1$. But $\gcd(2, 10) = 2$. If in your answer you simply said the application of RSA is invalid for this message, you got full credit.

If you applied RSA to this message and did it correctly you also got full credit. In this case RSA will work and give the correct message.

If you did not apply RSA correctly, you may have got full credit depending on what you did. Some people had the method seriously wrong, and did not get much, if any credit. For example, 1 person applied the DH process instead.)

One person noticed that the message M did not have the gcd property and changed M to another message that did, and worked it out for that. - also got full credit.)