CS/MATH111 ASSIGNMENT 2

Problem 1:

Let $n = p_1p_2...p_k$, where $p_1, p_2, ..., p_k$ are different primes. Prove that n has exactly 2^k different divisors. For example, if $n = 105$, then n $= 3 \cdot 5 \cdot 7$, so $k = 3$, and thus n has $2^3 = 8$ divisors. These divisors are: $1, 3, 5, 7, 15, 21, 35, 105$. Hint. You can reduce the problem to counting other objects that we already know how to count. Alternatively, this can be proved by induction on k.

Solution 1. We first show a simple proof based on counting subsets. The idea is that any divisor of n can be obtained by choosing a subset of primes $p_1, p_2, \ldots, p_k$ and multiplying them together. Let $P_n = \{p_1, p_2, \ldots, p_k\}$ be the set of all primes, that are involved in the prime factorization of n. A d is a divisor of n if and only if it is an element or a product of elements of some subset of P_n. Therefore the number of divisors of n is the same as the number of subsets of P_n (or the cardinality of its power set), which is 2^k.

Solution 2. The proof by induction on k. If $k = 0$ then $n = 1$, so it has only one divisor, and $2^k = 1$, thus the claim holds.
In the inductive step, assume that the claim holds for all numbers n' that are a product of k' different primes where $k' < k$. Now consider $n = p_1p_2 \cdots p_k$, where p_i's are different primes. We consider two types of divisors of n:

- Divisors that are not divisible by p_k. These divisors do not have p_k in their factorization so they are divisors of $n' = p_1p_2 \cdots p_{k-1}$. By our assumption, there are exactly 2^{k-1} such divisors.
- Divisors that are divisible by p_k. Each such divisor can be written as xp_k where x is a divisor of $n' = p_1p_2 \cdots p_{k-1}$ and vice versa, if x is a divisor of n' then xp_k is a divisor of n. By induction, there are 2^{k-1} such x's, so there are 2^{k-1} divisors of n of this type.

Adding the number of divisors of both types, we get $2^{k-1} + 2^{k-1} = 2^k$ divisors in total.

Problem 2:

Alice's RSA public key is $P = (e, n) = (23, 55)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 2, B is 3, ..., Z is 27, and blank is 28. Then he uses RSA to encode each number separately.

Bob's encoded message is:

```
51      12      51      39      31      21
14      10      20      17       7      25
14      26      33      52      15       7
27      51       7      49       8      15
51       7       8      25       7      25
10      49      18      52      51       7
 8      25       7      18      26      25
25      10      27      52      51       7
27      33      21       7      20      26
21       7      25      10      49      18
52      51      39
```

Decode Bob's message. Notice that you don't have Bob's secrete key, so you need to "break" RSA to decrypt his message.

For the solution, you need to provide the following:

- (a) Describe step by step how you arrived at the solution.

- (b) Show your work (the computation) for the first three numbers in the message.
- (c) Give Bob's message in plaintext (also, what does it mean and who said it?).
- (d) Show (attach) your code or computations for the remaining numbers. The code can be written in any programming language. If all computations are done by hand, please attach your work as well.

Suggestion: this can be solved by hand, but it will probably be faster to write a short program.

Solution. Not knowing the secret key, the best way to proceed is to try to factor n. Since n is small, this is easy: $55 = 5 \cdot 11$. So $p = 5$ and $q = 11$. Then we can compute $\phi(n) = (p-1)(q-1) = 40$. This allows us to compute the secret key, $d = e^{-1} \pmod{\phi(n)} = 23^{-1} \pmod{40} = 7$. Then we can apply the decryption algorithm: each number c of the ciphertext is converted into $c^7 \pmod{55}$. This way we obtain the numbers on the left (below), which we then convert into letters obtaining the original message on the right (a quote by A. Einstein):

6	23	6	19	26	21
9	10	20	17	28	20
9	16	22	13	5	28
3	6	28	14	2	5
6	28	2	20	28	20
10	14	17	13	6	28
2	20	28	17	16	20
20	10	3	13	6	28
3	22	21	28	15	16
21	28	20	10	14	17
13	6	19			

E	V	E	R	Y	T
H	I	N	G		S
H	O	U	L	D	
B	E		M	A	D
E		A	S		S
I	M	P	L	E	
A	S		P	O	S
S	I	B	L	E	
B	U	T		N	O
T		S	I	M	P
L	E	R			

"Everything should be made as simple as possible, but not simpler." - Albert Einstein.

Problem 3: (a) Compute $11^{-1} \pmod{19}$ by enumerating multiples. Show your work.
Let $a = 11^{-1}$ (where $a \neq 0$ is an integer). Then
$11 \cdot a \equiv 1 \pmod{19}$
$11 \cdot a = 19b + 1$ (for some integer $b \neq 0$)
$11 \cdot a = 11, 22, 33, 44, ..., 77$
$19 \cdot b + 1 = 20, 39, 58, 77$
From $11 \cdot a = 77$, we find $a = 7$, and so $11^{-1} \pmod{19} = 7$.
(b) Compute $11^{-5} \pmod{19}$ using Fermat's Little Theorem. Show your work.
$11^{-5} \pmod{19} \equiv 11^{-5} \cdot 11^{18} \pmod{19} \equiv 11^{13} \pmod{19} \equiv (11^2)^6 \cdot 11 \pmod{19} = ... \equiv 11.$
(c) Use Fermat's Little Theorem to compute $5^{1209640} \pmod{7}$. Show your work.
From Fermat's Little Theorem $5^6 \pmod{7} \equiv 1$.
So $5^{1209640} \pmod{7} \equiv (5^6)^{201606} \cdot 5^4 \equiv 1^{201606} \cdot 5^4 \equiv 5^4 \equiv (5^2)^2 \equiv 4^2 \pmod{7} = 2.$
(d) Find an integer x, $0 \leq x \leq 40$, that satisfies $31x \equiv 3 \pmod{41}$. Show your work.
First, $31^{-1} \pmod{41} \equiv 4$. Then $x \equiv 3 \cdot 4 \pmod{41}$, so $x = 12$.

Submission. To submit the homework, you need to upload the pdf file into ilearn and Gradescope.

Reminders. Remember that only LaTeX papers are accepted.