Divij Singh March 24, 2019

CS-302 Problem Set 3

Collaborators: *Jyotica, Mayukh*

Problem 1-1

(a) This is because for a prime number, the only factors it has are the number 1, and itself. As the number set does not include n itself, it is not possible to multiply it with 1, and thus create n for the modulo operation, to get 0.

(b) Two zero divisors for Z_{39} are 3 and 13, as $3 * 13 = 39$.

(c) The first element is $(5^5 mod 39)$.

(d) Possibly, although it is unlikely to be feasible to process it as 39 does not correspond to any integer raised to the power of another integer, meaning that the answer lies somewhere in the realm of real numbers.
As RSA moduli are prime factors, it is unlikely to be feasible for the same reasons as above.

(e) Yes, it it possible. Simply find some number that corresponds to an integer power of another integer. For instance, Z_4.
$x = 2, k = 2$
$x^k = 2^2 = 4$
$4(mod 4) \equiv 0$

Problem 1-2

For this, we take the first number, a_1. Since we are looking for the GCD of ALL the numbers, we can use any number and compare it to the others.
Then, we iterate over the list, testing a_1 and a_k (k being the current index, $k > 1$) for their GCD using the Euclidean algorithm.

Upon finding the GCD of a_1 and a_k, if it is smaller than the current total GCD, it is set as the new total GCD (total GCD being the GCD of ALL numbers).
At the end of the loop, we have the final GCD for all numbers in the sequence.

Problem 1-3

For this, we check if the number is prime. Since it isn't, we then try to break the number down into primes and prime powers.
$2200 = 2 * 2 * 2 * 5 * 5 * 11 = 2^3 * 5 * 2 * 11$
$\phi(2200) = 800$

Problem 1-4

We already know that $\phi(2200) = 800$.
According to Euler's theorem, we know that $a^{\phi(n)} \equiv 1(mod n)$
Applying this, we get $3^{739*800+7} \equiv (3^{800})^{739} * 3^7 \equiv 1 * 3^7 \equiv 2187(mod 2200)$

Problem 1-5

i	r_i	u_i	v_i	q_i
1	539	1	0	0
2	1387	0	-1	0
3	539	1	0	2
4	309	-2	-1	1
5	230	3	1	1
6	79	-5	-2	2
7	72	13	5	1
8	7	-18	-7	10
9	2	193	75	3
10	1	-597	-232	2
11	0	1387	539	0

Thus the answer is $x = -597, y = -232$

Problem 1-6

$n = pq = 2491$
$\phi(n) = (p - 1)(q - 1) = pq - p - q - 1$
Subtracting the second from the first, we get $p + q = 100$

$p = 100 - q | q = 100 - p$
$p^2 - 100p + 2491 = 0 | q^2 - 100q + 2491 = 0$
$p = 47, 53 | q = 47, 53$
$47 * 53 = 2491$

Therefore the factors are 47 and 53.

Problem 1-7

One primitive root is 6.

Lucas test:
g is a primitive root of p iff
$g^{(p-1)/q} \not\equiv 1 (mod p)$ for all $q > 1$ such that $p|(q-1)$
Factors of 760: 1, 2, 4, 5, 8, 10, 19, 20, 38, 40, 76, 95, 152, 190, 380, 760.
$6^{760/2} (mod p) \equiv 760$
$6^{760/4} (mod p) \equiv 39$
$6^{760/5} (mod p) \equiv 67$
$6^{760/8} (mod p) \equiv 62$
$6^{760/10} (mod p) \equiv 593$
$6^{760/19} (mod p) \equiv 498$
$6^{760/20} (mod p) \equiv 648$
$6^{760/38} (mod p) \equiv 487$
$6^{760/40} (mod p) \equiv 208$
$6^{760/76} (mod p) \equiv 160$
$6^{760/95} (mod p) \equiv 89$
$6^{760/152} (mod p) \equiv 166$
$6^{760/190} (mod p) \equiv 535$
$6^{760/380} (mod p) \equiv 36$
$6^{760/760} (mod p) \equiv 6$

Thus, it is a primitive root.

Problem 1-8

$\phi(n) = 1404$
$p = 19$

$q = 79$
PFA the code under the name ”$randomfactorise.py$”

Problem 1-9

PFA the code and README

Problem 1-10

No