Assignment: Project 7

Name 1: Jonathan Smoley

Name 2: Samuel Sovi

GitHub Name: JT2M0L3Y

1. Project 6, Problem 4 asked that you generate a public key and submit it to me in a file called *public_key.txt.* Very soon, possibly even today (4/7), I'll send you via email an encrypted message. The answer to this problem is its decryption. The email will go to the first author for the github repository that you used for problem 6.

plaintext: **dead land**

Hint for problems 2 - 4:
The obvious approach is to do a brute force search of all relevant exponents, stopping at the appropriate time. You may write a Sage list comprehension to produce a list of tuples of the form: (n,q^n mod k) where q is the integer whose order you are looking for, n is the exponent, and k is the modulus. You can determine by inspection the order of n. If you use the brute force technique, show all computations. If you use the sage technique, show the single line list comprehension. In either case, make an argument.

2. Find the order of 2 mod 17

$2^1 \equiv 2 \ (mod\ 17)$

$2^2 \equiv 4 \ (mod\ 17)$

$2^3 \equiv 8 \ (mod\ 17)$

$2^4 \equiv 16 \equiv \ -1 \ (mod\ 17)$

Thus, squaring both sides would result in the form $q^n \equiv 1 \ (mod\ k)$.

$2^8 \equiv 1 \ (mod\ 17)$

By definition then, 2 has order 8 (mod 17).

3. Find the order of 3 mod 19

$3^1 \equiv 3 \ (mod\ 19)$

$3^2 \equiv 9 \ (mod\ 19)$

$3^3 \equiv 8 \ (mod\ 19)$
$3^4 \equiv 5 \ (mod\ 19)$
$3^5 \equiv 15 \ (mod\ 19)$
$3^6 \equiv 7 \ (mod\ 19)$
$3^7 \equiv 2 \ (mod\ 19)$
$3^8 \equiv 6 \ (mod\ 19)$
$3^9 \equiv 18 \ (mod\ 19)$
$3^{10} \equiv 16 \ (mod\ 19)$
$3^{11} \equiv 10 \ (mod\ 19)$
$3^{12} \equiv 11 \ (mod\ 19)$
$3^{13} \equiv 14 \ (mod\ 19)$
$3^{14} \equiv 4 \ (mod\ 19)$
$3^{15} \equiv 12 \ (mod\ 19)$
$3^{16} \equiv 17 \ (mod\ 19)$
$3^{17} \equiv 13 \ (mod\ 19)$
$3^{18} \equiv 1 \ (mod\ 19)$

By definition then, 3 has order 18 (mod 19).

4. Find the order of 5 mod 23

$5^1 \equiv 5 \ (mod\ 23)$
$5^2 \equiv 2 \ (mod\ 23)$
$5^3 \equiv 10 \ (mod\ 23)$
$5^4 \equiv 4 \ (mod\ 23)$
$5^5 \equiv 20 \ (mod\ 23)$
$5^6 \equiv 8 \ (mod\ 23)$
$5^7 \equiv 17 \ (mod\ 23)$
$5^8 \equiv 16 \ (mod\ 23)$
$5^9 \equiv 11 \ (mod\ 23)$
$5^{10} \equiv 9 \ (mod\ 23)$
$5^{11} \equiv 22 \ (mod\ 23)$
$5^{12} \equiv 18 \ (mod\ 23)$

$5^{13} \equiv 21\ (mod\ 23)$
$5^{14} \equiv 13\ (mod\ 23)$
$5^{15} \equiv 19\ (mod\ 23)$
$5^{16} \equiv 3\ (mod\ 23)$
$5^{17} \equiv 15\ (mod\ 23)$
$5^{18} \equiv 6\ (mod\ 23)$
$5^{19} \equiv 7\ (mod\ 23)$
$5^{20} \equiv 12\ (mod\ 23)$
$5^{21} \equiv 14\ (mod\ 23)$
$5^{22} \equiv 1\ (mod\ 23)$

By definition then, 5 has order 22 (mod 23).

5. Prove: if a has order hk mod n then a^h has order k mod n.

Proof:
Assume a has order hk mod n.
Then, $a^{hk} \equiv 1\ (mod\ n)$ by definition.
$(a^h)^k \equiv 1\ (mod\ n)$

By definition then, a^h has order k (mod n).
This is true because:

1) $(a^h)^k \equiv 1\ (mod\ n)$
2) if a has order hk mod n, then by definition, hk is the smallest power of a that is congruent to 1. This means that k is the smallest power of a^h that is congruent to 1 as well.

6. Prove: The odd prime divisors of the integer n^4 +1 are of the form 8k + 1. You'll find the short-cut theorem useful.

Let p be an integer such that:
$n^4 + 1 \equiv 0\ mod\ p$

This means that:
$n^4 \equiv -1\ mod\ p$

Squaring both sides produces:
$n^8 \equiv 1 \, mod \, p$

By the shortcut theorem, if a has order k mod n, then $a^k \equiv 1 \, mod \, n$ if and only if $k|h$, in particular, $k|\phi(n)$.

Translating this to the current problem, n has order 8 mod p as $n^8 \equiv 1 \, mod \, p$.

Then, $\phi(p) = p - 1$.

So, $8 \mid \phi(p) \equiv 8 \mid (p - 1)$.

By divisibility, we can write $p - 1 = 8k$ or $p = 8k + 1$.

Therefore, odd prime divisors of $n^4 + 1$ are of the form $8k + 1$.

7. Using the primitive root test algorithm developed in class, find the primitive roots of 13. You'll also find the algorithm in McAndrew, p. 119. Show all work.

$\phi(13) = 12$
To find the primitive roots of 13, we must test {1,2,3,4,5,6,7,8,9,10,11} (k < $\phi(n)$)

Using shortcut theorem, we can see that if $a^{12} \equiv 1 \, (mod \, 13)$ then only k, a factor of 12, can be a valid power of a such that $a^k \equiv 1 \, (mod \, 13)$

factors of 12 : {1,2,3,4,6}

1:

$1^1 \equiv 1 \, (mod \, 13)$

(1 is not a primitive root since the power 1 < 12)

2:

$2^1 \equiv 2 \, (mod \, 13)$

$2^2 \equiv 4 \, (mod \, 13)$

$2^3 \equiv 8 \, (mod \, 13)$

$2^4 \equiv 3 \, (mod \, 13)$

$2^6 \equiv 12\ (mod\ 13)$

$2^{12} \equiv 1\ (mod\ 13)$

(2 is a primitive root of 13)

3:

$3^1 \equiv 3(mod\ 13)$

$3^2 \equiv 9(mod\ 13)$

$3^3 \equiv 1(mod\ 13)$

(3 is not a primitive root since the power 3 < 12)

4:

$4^1 \equiv 4(mod\ 13)$

$4^2 \equiv 3(mod\ 13)$

$4^3 \equiv 12(mod\ 13)$

$4^4 \equiv 9(mod\ 13)$

$4^6 \equiv 1(mod\ 13)$

(4 is not a primitive root since the power 6 < 12)

5:

$5^1 \equiv 5(mod\ 13)$

$5^2 \equiv 12(mod\ 13)$

$5^3 \equiv 8(mod\ 13)$

$5^4 \equiv 1(mod\ 13)$

(5 is not a primitive root since the power 4 < 12)

6:

$6^1 \equiv 6(mod\ 13)$

$6^2 \equiv 10(mod\ 13)$

$6^3 \equiv 8(mod\ 13)$

$6^4 \equiv 9(mod\ 13)$

$6^6 \equiv 12(mod\ 13)$

$6^{12} \equiv 1(mod\ 13)$

(6 is a primitive root of 13)

7:

$7^1 \equiv 7(mod\ 13)$

$7^2 \equiv 10(mod\ 13)$

$7^3 \equiv 5(mod\ 13)$

$7^4 \equiv 9(mod\ 13)$

$7^6 \equiv 12(mod\ 13)$

$7^{12} \equiv 1(mod\ 13)$

(7 is a primitive root of 13)

8:

$8^1 \equiv 8(mod\ 13)$

$8^2 \equiv 12(mod\ 13)$

$8^3 \equiv 5(mod\ 13)$

$8^4 \equiv 1(mod\ 13)$

(8 is not a primitive root since the power 4 < 12)

9:

$9^1 \equiv 9(mod\ 13)$

$9^2 \equiv 3(mod\ 13)$

$9^3 \equiv 1(mod\ 13)$

(9 is not a primitive root since the power 3 < 12)

10:

$10^1 \equiv 10(mod\ 13)$

$10^2 \equiv 9(mod\ 13)$

$10^3 \equiv 12(mod\ 13)$

$10^4 \equiv 3(mod\ 13)$

$10^6 \equiv 1(mod\ 13)$

(10 is not a primitive root since the power 6 < 12)

11:

$11^1 \equiv 11(mod\ 13)$

$11^2 \equiv 4(mod\ 13)$

$11^3 \equiv 5(mod\ 13)$

$11^4 \equiv 3(mod\ 13)$

$11^6 \equiv 12(mod\ 13)$

$11^{12} \equiv 1(mod\ 13)$

(11 is a primitive root of 13)

Therefore the primitive roots of 13 are: {2,6,7,11}