1 Problem 1

Find order of 2 mod 17, or find the smallest possible positive integer k such that $2^k \ = \ 1 \ (mod\ 17)$

$$
\begin{aligned}
2^k &= 1\ (mod\ 17)\\
2^k\ (mod\ 17) &= 1\\
2^1\ (mod\ 17) &= 0*17+2=2\\
2^2\ (mod\ 17) &= 0*17+4=4\\
2^3\ (mod\ 17) &= 0*17+8=8\\
2^4\ (mod\ 17) &= 0*17+16=16\\
2^5\ (mod\ 17) &= 1*17+15=15\\
2^6\ (mod\ 17) &= 3*17+13=13\\
2^7\ (mod\ 17) &= 7*17+9=9\\
2^8\ (mod\ 17) &= 15*17+1=1
\end{aligned}
$$

Order 2 mod 17 is $k \ = \ 8$

2 Problem 2

Find order of 3 mod 19, or find the smallest possible positive integer k such that $3^k \ = \ 1 \ (mod\ 19)$

$$
\begin{aligned}
3^k &= 1\ (mod\ 19)\\
3^k\ (mod\ 19) &= 1\\
3^1\ (mod\ 19) &= 0*19+3=3\\
3^2\ (mod\ 19) &= 0*19+9=9\\
3^3\ (mod\ 19) &= 1*19+8=8\\
3^4\ (mod\ 19) &= 4*19+5=5\\
3^5\ (mod\ 19) &= 12*19+15=15\\
3^6\ (mod\ 19) &= 38*19+7=7\\
3^7\ (mod\ 19) &= 115*19+2=2\\
&...\\
3^{16}\ (mod\ 19) &= 2265616*19+17=17\\
3^{17}\ (mod\ 19) &= 6796850*19+13=13\\
3^{18}\ (mod\ 19) &= 20390552*19+1=1
\end{aligned}
$$

Order 3 mod 19 is $k \ = \ 18$

3 Problem 3

Find order of 5 mod 23, or find the smallest possible positive integer k such that $5^k = 1 \ (mod\ 23)$

$$
\begin{aligned}
5^k &= 1 \ (mod\ 23) \\
5^k \ (mod\ 23) &= 1 \\
5^1 \ (mod\ 23) &= 0 * 23 + 5 = 5 \\
5^2 \ (mod\ 23) &= 1 * 23 + 2 = 2 \\
5^3 \ (mod\ 23) &= 5 * 23 + 10 = 10 \\
5^4 \ (mod\ 23) &= 13 * 23 + 4 = 4 \\
5^5 \ (mod\ 23) &= 135 * 23 + 20 = 20 \\
5^6 \ (mod\ 23) &= 679 * 23 + 8 = 8 \\
5^7 \ (mod\ 23) &= 3396 * 23 + 17 = 17 \\
&... \\
5^{20} \ (mod\ 23) &= 12 \\
5^{21} \ (mod\ 23) &= 14 \\
5^{22} \ (mod\ 23) &= 1
\end{aligned}
$$

Order 5 mod 23 is $k = 22$

4 Problem 4

Proposition 1 *If a has order hk mod n then* $a * h$ *has order k mod n*

Proof 1 *Let a have order hk modulo n. Then, hk is the smallest possible integer such that* $a^{hk} \equiv 1 \ (mod\ n)$*. Suppose k is not the smallest interger such that* $a^{hk} \equiv 1 \ (mod\ n)$ *and an integer i less than k such that* $a^{ik} \equiv 1 \ (mod\ n)$*. It should be the case that k — i according the the , however, it is assumed that* $k > i$*, meaning that k cannot divide — i.*

So, by contradiction, k is the smallest integer which satisfies $a^{hk} \equiv 1 \ (mod\ n)$*.*

Therefore, a^h *has order k mod n*

5 Problem 5

Proposition 2 *The odd prime divisors of the integer* $n^4 + 1$ *are of the form* $8k + 1$

6 Problem 6

Using the primitive root test algorithm developed in class, find the primitive roots of 13

The primitive root test algorithm: If $a^{\frac{\phi n}{\alpha}} \neq 1\ (mod\ n)$, then a is a primitive root.

$\phi^{(13)} = 13 - 1 = 12$ and the factors of 12, d is equal to $d = 2, 3, 4$

$$a^{\frac{\phi^{(13)}}{d}} \neq 1\ (mod\ 13)$$

$$1^{\frac{\phi^{(13)}}{2}} = 1^{\frac{12}{2}} = 1\ (mod\ 13)$$

$$1^{\frac{\phi^{(13)}}{3}} = 1^{\frac{12}{3}} = 1\ (mod\ 13)$$

$$1^{\frac{\phi^{(13)}}{4}} = 1^{\frac{12}{4}} = 1\ (mod\ 13)$$

$$2^{\frac{\phi^{(13)}}{2}} = 2^{\frac{12}{2}} = 2^6 = 64 = 1\ (mod\ 13)$$

$$2^{\frac{\phi^{(13)}}{3}} = 2^{\frac{12}{3}} = 2^4 = 16 = 12\ (mod\ 13)$$

$$2^{\frac{\phi^{(13)}}{4}} = 2^{\frac{12}{4}} = 2^3 = 8 = 8\ (mod\ 13)$$

2 is a primitive root

$$3^{\frac{\phi^{(13)}}{2}} = 3^{\frac{12}{2}} = 3^6 = 729 = 1\ (mod\ 13)$$

$$3^{\frac{\phi^{(13)}}{3}} = 3^{\frac{12}{3}} = 3^4 = 81 = 3\ (mod\ 13)$$

$$3^{\frac{\phi^{(13)}}{4}} = 3^{\frac{12}{4}} = 3^3 = 27 = 1\ (mod\ 13)$$

...

$$4^{\frac{\phi^{(13)}}{2}} = 4^{\frac{12}{2}} = 4^6 = 4096 = 1\ (mod\ 13)$$

...

$$5^{\frac{\phi^{(13)}}{2}} = 5^{\frac{12}{2}} = 5^6 = 12\ (mod\ 13)$$

$$5^{\frac{\phi^{(13)}}{3}} = 2^{\frac{12}{3}} = 5^4 = 1\ (mod\ 13)$$

...

$$6^{\frac{\phi^{(13)}}{2}} = 6^{\frac{12}{2}} = 6^6 = 12\ (mod\ 13)$$

$$6^{\frac{\phi^{(13)}}{3}} = 6^{\frac{12}{3}} = 6^4 = 9\ (mod\ 13)$$

$$6^{\frac{\phi^{(13)}}{4}} = 6^{\frac{12}{4}} = 6^3 = 8\ (mod\ 13)$$

6 is a primitive root

$$7^{\frac{\phi^{(13)}}{2}} = 7^{\frac{12}{2}} = 7^6 = 12\ (mod\ 13)$$

$$7^{\frac{\phi^{(13)}}{3}} = 7^{\frac{12}{3}} = 7^4 = 9\ (mod\ 13)$$

$$7^{\frac{\phi^{(13)}}{4}} = 7^{\frac{12}{4}} = 7^3 = 5\ (mod\ 13)$$

7 is a primitive root

$$8^{\frac{\phi(13)}{2}} = 8^{\frac{12}{2}} = 8^6 = 12\ (mod\ 13)$$

$$8^{\frac{\phi(13)}{3}} = 8^{\frac{12}{3}} = 8^4 = 1\ (mod\ 13)$$

...

$$9^{\frac{\phi(13)}{2}} = 9^{\frac{12}{2}} = 9^6 = 1\ (mod\ 13)$$

...

$$10^{\frac{\phi(13)}{2}} = 10^{\frac{12}{2}} = 10^6 = 1\ (mod\ 13)$$

...

$$11^{\frac{\phi(13)}{2}} = 11^{\frac{12}{2}} = 11^6 = 12\ (mod\ 13)$$

$$11^{\frac{\phi(13)}{3}} = 11^{\frac{12}{3}} = 11^4 = 3\ (mod\ 13)$$

$$11^{\frac{\phi(13)}{4}} = 11^{\frac{12}{4}} = 11^3 = 5\ (mod\ 13)$$

11 is a primitive root

$$12^{\frac{\phi(13)}{2}} = 12^{\frac{12}{2}} = 12^6 = 1\ (mod\ 13)$$

...

The primitive roots of 13 are $2, 6, 7, 11$