1.

2	3	5	
8	16	16	mod 17
18	18	9	mod 19
11	11	22	mod 23

all via thm 8.1

2. a. if $a^{hk} \equiv 1 \pmod n$ then $(a^h)^k \equiv 1 \pmod n$

$(a^h)^k \equiv a^{hk} \equiv 1 \pmod n$ ⨳

b. if $a^{2k} \equiv 1 \pmod p$ then $a^k \equiv -1 \pmod p$

$r \mid \phi(p) \Rightarrow r \mid \ldots$
$r \mid 2k$

$a^{2k}-1 \equiv (a^k-1)(a^k+1) \equiv 0 \pmod p$

$a^k \equiv 1 \pmod p$ or $\underline{a^k \equiv -1 \pmod p}$ ⨳

Because the order is 2k, a smaller exponent, k, cannot be congruent to 1, thus a contradiction !!!

This leaves $a^k \equiv -1 \pmod p$ as the only remaining term, thus proving the proposition

c. if $a^{n-1} \equiv 1 \pmod n$ then n is prime $(n-1) \mid$

Because n-1 must divide $\phi(n)$ the only way for this to occur is if n is prime #

$\phi(n) = n-1$ when n is prime or
$\phi(n) < n-1$ otherwise

d. $a^h \equiv 1 \pmod n$ $b^k \equiv 1 \pmod n$ $\Rightarrow (ab)^r \equiv 1 \pmod n$ st. $r \mid hk$

$(ab)^{hk} \equiv a^{hk} b^{kh} \equiv (a^h)^k (b^k)^h \equiv (1)^k (1)^h \equiv 1 \pmod n$

Because $(ab)^{hk}$ is congruent to 1 modulo n, it must be divisible by the order of a mod n. By thm 8.1

3. a. odd prime divisors of n^2+1 are of form $4k+1$

$n^2+1 \equiv 0 \pmod p$ $\forall$ odd primes, p st $p \mid n^2+1$

$n^2 \equiv -1 \pmod p$

$(n^2)^2 \equiv (-1)^2 \pmod p$

$n^4 \equiv 1 \pmod p$

Thrm 8.1 $\therefore 4 \mid \phi(p)$

Thrm 7.1 $4 \mid p-1$

$p-1 = 4k$

$p = 4k+1$

Because $n^4 \equiv 1$ and the only number which smaller than it greater than 1 which it divides is 2, we can that the order of n mod p and cannot be 2 trivially

b. $n^4+1 \equiv 0 \pmod p$

$n^4 \equiv -1 \pmod p$

$(n^4)^2 \equiv (-1)^2 \pmod p$

$n^8 \equiv 1 \pmod p$

$8 \mid \phi(p)$

$8 \mid p-1$

$p-1 = 8k$

$p = 8k+1$

Because $n^8 \equiv 1 \pmod p$ and its only factors are 2 and 4 and $n^4 \not\equiv 1 \pmod p$ and $2 \mid 4$ thus the order of n mod p must be 8. and cannot be one of the others all powers of $n^k \equiv 1 \pmod p$

c. odd primes p st. $p \mid n^2+n+1$ $p \in 6k+1$ except 3

$$n^3-1 \equiv (n^2+n+1)(n-1) \equiv 0 \pmod p$$

either

$n^2+n \equiv -1 \pmod p$ $\qquad$ $n \equiv 1 \pmod p$

$n(n+1) \equiv -1 \pmod p$

3. a. odd prime divisors of n^2+1 are of form $4k+1$

$n^2+1 \equiv 0 \pmod{p}$ $\forall$ odd primes, p st $p \mid n^2+1$

$n^2 \equiv -1 \pmod{p}$

$(n^2)^2 \equiv (-1)^2 \pmod{p}$

$n^4 \equiv 1 \pmod{p}$

Thm 8.1 $\therefore 4 \mid \phi(p)$

Thm 7.1 $4 \mid p-1$

$p-1 = 4k$

$p = 4k+1$

Because $n^4 \equiv 1$ and the only [illegible] which smaller than it greater than [illegible] it divides is 2, we can that [illegible] and cannot be 1 trivially order of n mod p.

b. $n^4+1 \equiv 0 \pmod{p}$

$n^4 \equiv -1 \pmod{p}$

$(n^4)^2 \equiv (-1)^2 \pmod{p}$

$n^8 \equiv 1 \pmod{p}$

$8 \mid \phi(p)$

$8 \mid p-1$

$p-1 = 8k$

$p = 8k+1$

Because $n^8 \equiv 1 \pmod{p}$ and its only factors are 2 and 4 and $n^4 \not\equiv 1 \pmod{p}$ and $2 \mid 4$ thus the order of n mod p must be 8. and cannot be one of the others all powers of $n^k \equiv 1 \pmod{p}$

c. odd primes p st. $p \mid n^2+n+1$. $p \in 6k+1$ except 3

$n^3-1 \equiv (n^2+n+1)(n-1) \equiv 0 \pmod{p}$

either

$n^2+n \equiv -1 \pmod{p}$

$n(n+1) \equiv -1 \pmod{p}$

$n \equiv 1 \pmod{p}$

4. a. $p \neq q$ primes ($\neq 2$) + $q \mid a^p - 1 \Rightarrow \begin{cases} q \mid a-1 \\ q = 2kp+1 \end{cases}$ $, k \in \mathbb{Z}$ either

$a^p \equiv 1 \pmod q$ because p is prime the order of a mod q must be either 1 or p

order is 1 — order is p

$a \equiv 1 \pmod q$ — $p \mid \phi(q)$

$\therefore q \mid a-1$ ✓

$p \mid q-1 \Rightarrow kp = q-1$

$q = kp+1$ — because odd primes?

$2 \nmid p$ $2 \nmid q$ $\longrightarrow q = 2kp+1$ ✓

Because both cases hold the proposition is true

b. p is odd prime $\Rightarrow$ prime divisors of $2^p - 1$ are of form $2kp+1$

$2^p - 1 \equiv 0 \pmod q$ where q is any odd prime divisor. q cannot include 2 as $2^p - 1$ must be odd, ~~additionally~~

$2^p \equiv 1 \pmod q$

$p \mid \phi(q)$ — The order of 2 mod q cannot be 1 as q is an odd prime and thus at least 3 and $(2^1 - 1) \bmod 3 = -2$

$p \mid q-1$

$q = 2kp+1$ using result of proof for A

c. 17 + 29 are both odd primes ✓

$2^{17} - 1 = (2^{17} - 1)(1)$ $\therefore$ it's prime

$2^{29} - 1 = 233 \cdot 1103 \cdot 2089$

See sagemath code

4. a. a has order $\phi(n)$ mod n => a^k has order $\phi(n)$ iff $\gcd(k, \phi(n)) = 1$

according to theorem 8.3, order a^k mod n = $\phi(n)/\gcd(k, \phi(n))$

in order for the order of a^k mod n to be $\phi(n)$ and thus a primitive root, the gcd $(k, \phi(n))$ must be 1 giving $\phi(n)$

b. via sagemath the order

order $(3, 17) = 16 = \phi(n)$ therefore 3 is a primitive root of 17

c. via sagemath

[3, 5, 6, 7, 10, 11, 12, 14]

although not ~~taking into account~~ using a or b.