8.1 | 4 order of a mod n is h, order of b mod n is k } Then the order of ab mod n divides hk.

pf.: Let α = order of ab mod n. Then $hk = q\alpha + r$, $0 \le r < \alpha$,

$(ab)^{hk} = a^h b^k \equiv 1 \pmod n$, and $(ab)^{hk} = (ab)^{q\alpha+r} \equiv (ab)^r \pmod n$.

since $a^h \equiv 1$ & $b^k \equiv 1$

since $(ab)^\alpha \equiv 1$

Thus, $(ab)^r \equiv 1 \pmod n \Longrightarrow r = 0$, since $r < \alpha$ and α is the order of ab, so $\alpha \mid hk$. ∎ Corollary: $\gcd(h,k) = 1 \Longrightarrow ab$ has order hk.

6(a) p prime, p odd, $p \mid n^2+1 \Longrightarrow p = 4k+1$:

$p \mid n^2+1 \Longleftrightarrow n^2 \equiv -1 \pmod p \Longrightarrow n^4 \equiv 1 \pmod p \Longrightarrow 4 \mid \varphi(p) = p-1$,

so $p-1 = 4k \Longrightarrow p = 4k+1$. ∎

6(b) p prime, p odd, $p \mid n^4+1 \Longrightarrow p = 8k+1$:

$p \mid n^4+1 \Longleftrightarrow n^4 \equiv -1 \pmod p \Longrightarrow n^8 \equiv 1 \pmod p \Longrightarrow 8 \mid \varphi(p) = p-1$

$\Longrightarrow p-1 = 8k \Longrightarrow p = 8k+1.$ ∎

6(c) p prime, p odd, $p \neq 3$, $p \mid n^2+n+1 \Longrightarrow p = 6k+1$:

$p \mid n^2+n+1 \Longleftrightarrow n^2+n \equiv -1 \pmod p \Longrightarrow n^3+n^2 \equiv -n \pmod p$

$\Longrightarrow n^3 \equiv -n^2-n \equiv 1 \pmod p$

$\Longrightarrow 3 \mid p-1$. (Here, use the fact that $p \neq 3$.)

Since p is odd, $p-1$ is even. Thus, $6 \mid p-1 \Longrightarrow p = 6k+1$. ∎

8.2 | 3 primitive roots of 11, 19, 23

11: $\varphi(11) = 10$, divisors of 10 are 1, 2, 5, 10

$2^1 = 2$, $2^2 = 4$, $2^5 = 32 \equiv -1 \pmod{11} \Longrightarrow 2^{10} \equiv 1 \pmod{11}$ &

2 is a primitive root of 11. others are 2^h with $\gcd(h, 10) = 1$,

i.e., $\{2^1, 2^3, 2^7, 2^9\} \equiv \{2, 8, 7, 6\}$. (Note: $\varphi(10) = 4$)

19: $\varphi(19) = 18$, divisors of 18 are 1, 2, 3, 6, 9, 18.

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^6 = 64 \equiv 7$, $2^9 \equiv 56 \equiv -1$, $2^{18} \equiv 1$ $\varphi(18) = 6$

Thus, 2 is a primitive root of 19. All of them: $\{2, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}\}$.

23: $\varphi(23) = 22$, divisors are 1, 2, 11, 22

2^1, $2^2 = 4$, $2^{11} = 32 \equiv 9$, $2^{10} \equiv 81 \equiv 12$, $2^{11} \equiv 1$ X

3, $3^2 = 9$, $3^4 = 81 \equiv 12$, $3^5 \equiv 17$, $3^{10} \equiv 169 \equiv 8$, $3^{11} \equiv 1$ X

5, $5^2 = 25 \equiv 2$, $5^{10} \equiv 9$, $5^{11} \equiv -1$, $5^{22} \equiv 1 \Longrightarrow 5$ is a primitive root of 23.

$\varphi(22) = 10$ All of them: $\{5, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}\}$

4 Given: 3 is a primitive root of 43.

(a) integers of order 6 mod 43 : 3^h such that $\gcd(h, 42) = 7$

$\Rightarrow h = 7, 35 \Rightarrow 3^7, 3^{35}$ have order 6. (Note: $\varphi(6) = 2$)

reduce mod 43: $3 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 81 \equiv 38$, $3^5 \equiv 114 \equiv 28$,

$3^6 \equiv 84 \equiv -2$, $3^7 \equiv -6 \equiv \underline{37}$

$3^6 \equiv -2 \Rightarrow 3^{30} \equiv -32 \equiv 11 \Rightarrow 3^{35} \equiv 308 \equiv \underline{7}$.

(b) integers of order 21 mod 43 : 3^h s.t. $\gcd(h, 42) = 2$

$\Rightarrow$ exponents are $\{2, 4, 8, 10, 16, 20, 22, 26, 32, 34, 38, 40\}$

Note: $\varphi(21) = \underline{12}$

reduce mod 43: $3^2 = \underline{9}$ ✓; $3^4 = 81 \equiv \underline{38}$ ✓; $3^8 \equiv 38^2 = 1444 \equiv \underline{25}$ ✓;

$3^{10} \equiv 225 \equiv \underline{10}$ ✓; $3^{16} \equiv 625 \equiv \underline{23}$ ✓; $3^{20} \equiv 23 \times 38 \equiv \underline{14}$ ✓;

$3^{22} \equiv 126 \equiv -3 \equiv \underline{40}$ ✓; $3^{26} \equiv 40 \times 38 \equiv \underline{15}$ ✓;

$3^{32} \equiv 9 \times 38 \times 15 \equiv \underline{13}$ ✓; $3^{34} \equiv 117 \equiv \underline{31}$ ✓; $3^{38} \equiv \underline{17}$ ✓;

$3^{40} \equiv 153 \equiv \underline{24}$ ✓.

Answer:
9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40

5 All integers < 61 having order 4 mod 61 : $\underline{11, 50}$

2 is a primitive root of 61 :

$2 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 16,\ 2^5 \equiv 32,\ 2^6 \equiv 3,\ 2^{10} \equiv 48,$

$2^{12} \equiv 9,\ 2^{15} \equiv 11,\ 2^{20} \equiv 47,\ 2^{30} \equiv 60 \equiv -1 \Rightarrow \underline{2^{60} \equiv 1}$ ✓

Then 2^h has order 4 iff $\gcd(h, 60) = 15 \Rightarrow h = 15, 45$

$2^{15} \equiv \underline{11}$, $2^{45} \equiv -11 \equiv \underline{50}$ (Note: $\varphi(4) = 2$.)

---

9 r a primitive root of the prime $p \equiv 1 \pmod 4 \Rightarrow r^{\frac{p-1}{4}}$ satisfies $x^2 + 1 \equiv 0 \pmod p$

$p \equiv 1 \pmod 4 \Rightarrow p = 4k+1,\ p-1 = 4k,\ r^{4k} \equiv 1 \pmod p$

$\Rightarrow p \mid r^{4k} - 1 = (r^{2k}+1)(r^{2k}-1)$

$\Rightarrow p \mid r^{2k} + 1$ or $\underbrace{p \mid r^{2k} - 1}$

can't happen since $4k$ is the order of r

$\Rightarrow r^{2k} \equiv -1 \pmod p$, and $r^{2k} = (r^k)^2 = \left(r^{\frac{p-1}{4}}\right)^2$.

∎

10 p prime $\Longrightarrow$ p has a primitive root r, $r^{p-1} \equiv 1 \pmod{p}$

Then $\{r, r^2, \ldots, r^{p-1}\} \equiv \{1, 2, \ldots, p-1\}$ modulo p

$$\Longrightarrow \quad r \cdot r^2 \cdot \ldots \cdot r^{p-1} \equiv (p-1)! \pmod{p}$$

$$\Longrightarrow \quad r^{1+2+\ldots+p-1} \equiv (p-1)! \pmod{p}$$

$$\Longrightarrow \quad r^{\frac{(p-1)p}{2}} \equiv (p-1)! \pmod{p}$$

If $r^{\frac{(p-1)p}{2}} \equiv \alpha \pmod{p}$, then $\alpha^2 \equiv 1 \pmod{p}$ (since $\alpha^2 \equiv (r^{p-1})^p$)

$$\Longrightarrow p \mid \alpha^2 - 1 \Longrightarrow \underbrace{p \mid \alpha - 1}_{\text{violates fact that order of } r \text{ is } (p-1)} \text{ or } p \mid \alpha + 1$$

$$\Longrightarrow p \mid \alpha + 1 \Longrightarrow \alpha = p - 1 \equiv -1.$$

Thus, $r^{\frac{(p-1)p}{2}} \equiv -1 \equiv (p-1)! \pmod{p}$, Wilson's Theorem! ∎