46. If $p^k \| n$ for a prime p and a positive integer n, then we have

$$p-1 \mid \phi(p^k) \mid \phi(n) = 20,$$

so every prime p appearing in the prime factorization of n must satisfy $p-1 \mid 20$. Only such primes are $p = 2, 3, 5, 11$ and hence we can write $n = 2^a \cdot 3^b \cdot 5^c \cdot 11^d$ where we allow a, b, c, d to be 0 as well.

- a can be at most 3 because otherwise $8 \mid 2^{a-1} = \phi(2^a) \mid \phi(n) = 20$, which is not possible.
- b can be at most 1 because otherwise $3 \mid 3^{b-1} \mid \phi(3^b) \mid \phi(n) = 20$, which is not possible.
- c can be at most 2 because otherwise $25 \mid 5^{c-1} \mid \phi(5^c) \mid \phi(n) = 20$, which is not possible.
- d can be at most 1 because otherwise $11 \mid 11^{d-1} \mid \phi(11^d) \mid \phi(n) = 20$, which is not possible.

There are $4 \times 2 \times 3 \times 2 = 48$ different possible combinations for the values of a, b, c, d. Trying them all, we find $\phi(n) = 20$ only for $n = 25, 33, 44, 50, 66$.

(You can try them nicely to reduce the computations. For example, if $c = 2$, then we reach 20 only by $\phi(25)$ and the other prime factors shouldn't contribute which is only possible for no other prime factor and for just 2^1. This gives $n = 25$ and $n = 50$ and we can rule out the case of $c = 2$ before continuing).

47. We use the same idea with the previous question. Every prime p appearing in the prime factorization of n must satisfy $p - 1 \mid 14$. Only such primes are $p = 2, 3$ hence we can write $n = 2^a \cdot 3^b$ where we allow a, b to be 0 as well.

- a can be at most 2 because otherwise $4 \mid 2^{a-1} = \phi(2^a) \mid \phi(n) = 14$, which is not possible.
- b can be at most 1 becaue otherwise $3 \mid 3^{b-1} \mid \phi(3^b) \mid \phi(n) = 14$, which is not possible.

Trying the $3 \times 2 = 6$ possible combinations for a and b, we find that there is no n satisfying $\phi(n) = 14$.

48. We first note that $4080 = 2^4 \times 3 \times 5 \times 17$.

Since n is odd, i.e. $\gcd(n, 2) = 1$, we have

$$n^{33} \equiv \left(n^8\right)^4 \cdot n \equiv n \pmod{16}$$

by Euler's theorem.

We also have

$$n^{33} \equiv \left(n^2\right)^{16} \cdot n \equiv n \pmod{3}, \quad n^{33} \equiv \left(n^4\right)^8 \cdot n \equiv n \pmod{5}, \text{ and } n^{33} \equiv \left(n^{16}\right)^2 \cdot n \equiv n \pmod{17}$$

by Fermat's theorem.

Combining these congruences by the Chinese Remainder Theorem, we finally have $n^{33} \equiv n \pmod{4080}$.

49. Note that these numbers can be written as $\frac{10^k-1}{9}$.

Let m an arbitrary positive integer, then by Euler's theorem we have

$$10^{m\cdot\phi(9n)} \equiv 1 \pmod{9n}$$

which means $9n$ divides $10^{m\cdot\phi(9n)} - 1$ and hence n divides $\frac{10^{m\cdot\phi(9n)}-1}{9}$.

50. We first show that 3 is a primitive root modulo 17.

Indeed, $3^8 \not\equiv 1 \pmod{17}$ gives $\mathrm{ord}_{17}(3) \nmid 8$ and since we already know $\mathrm{ord}_{17}(3) \mid 16$, we get $\mathrm{ord}_{17}(3) = 16$, i.e. 3 is a primitive root modulo 17.

Now, all the units modulo 17 can be written as 3^k with $1 \le k \le 16$. Since $\mathrm{ord}_{17}(3^k) = \frac{16}{\gcd(16,k)}$ is equal to 16 for the values of k satisfying $\gcd(16, k) = 1$, the primitive roots of $\mathbb{Z}_{17}$ are

$$\begin{aligned} 3^1 &\equiv 3 \pmod{17} & 3^3 &\equiv 10 \pmod{17} \\ 3^5 &\equiv 5 \pmod{17} & 3^7 &\equiv 11 \pmod{17} \\ 3^9 &\equiv 14 \pmod{17} & 3^{11} &\equiv 7 \pmod{17} \\ 3^{13} &\equiv 12 \pmod{17} & 3^{15} &\equiv 6 \pmod{17}. \end{aligned}$$

51. We first note that $g^{\frac{p-1}{2}} \equiv -1 \pmod p$. This is very easy to prove and a very short proof can be found in page 3 of Lecture 17 notes.

Assume first that $-g$ is a primitive root modulo p, then we must also have $(-g)^{\frac{p-1}{2}} \equiv -1 \pmod p$ and we get

$$-1 \equiv (-g)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot g^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \pmod p \Longrightarrow 1 \equiv (-1)^{\frac{p-1}{2}} \pmod p \Longrightarrow p \equiv 1 \pmod 4.$$

Assume now that $p \equiv 1 \pmod 4$, say $p = 4k+1$. Then we have $-g \equiv (-1) \cdot g \equiv g^{\frac{p-1}{2}} \cdot g \equiv g^{\frac{p+1}{2}} \equiv g^{2k+1} \pmod p$ and

$$\mathrm{ord}_p(-g) = \mathrm{ord}_p(g^{2k+1}) = \frac{4k}{\gcd(4k, 2k+1)} = 4k,$$

i.e. $-g$ is also a primitive root modulo p.

52. Let $m = 2^n - 1$, then clearly we have $\mathrm{ord}_m(2) = n$ becasue $2^n \equiv 1 \pmod m$ while $1 < 2^k < m$ for all $1 \le k \le n$ while . Therefore, we have $\mathrm{ord}_m(2) \mid \phi(m)$, i.e. $n \mid \phi(2^n - 1)$.

53. Since $\mathrm{ord}_p(u) = 3$, we have $u^3 \equiv 1 \pmod p$ and $u \not\equiv 1 \pmod p$. Therefore $u^3 - 1 = (u-1)(u^2+u+1)$ must be divisible by p and since $p \nmid u - 1$ we must have $u^2 + u + 1$ divisible by p, i.e. $u^2 + u + 1 \equiv 0 \pmod p$.

For the second statement, it is enough to prove that

$$(1+u)^6 \equiv 1 \pmod p$$

so that $\mathrm{ord}_p(1+u) \mid 6$ and

$$(1+u)^3 \not\equiv 1 \pmod p$$

so that $\mathrm{ord}_p(1+u) \nmid 3$ and

$$(1+u)^2 \not\equiv 1 \pmod p$$

so that $\mathrm{ord}_p(1+u) \nmid 2$. Indeed, we have

$$(1+u)^2 = u^2 + 2u + 1 \equiv (u^2+u+1) + u \equiv u \not\equiv 1 \pmod p$$

since $\mathrm{ord}_p(u) \neq 1$, and

$$(1+u)^3 \equiv (1+u) \cdot (1+u)^2 \equiv (1+u) \cdot u \equiv u^2 + u \equiv -1 \not\equiv 1 \pmod p$$

since $\mathrm{ord}_p(u) > 2 \Longrightarrow p \neq 2$, and

$$(1+u)^6 \equiv (1+u)^3 \cdot (1+u)^3 \equiv (-1) \cdot (-1) \equiv 1 \pmod p.$$

54. Since g is a primitive root modulo p, the numbers $g, g^2, g^3, \cdots, g^{p^2-p}$ should be different modulo p^2. In $\mathbb{Z}_{p^2}$, there are p values that are 1 modulo p : $1, p+1, 2p+1, \cdots, (p-1)\cdot p + 1$. We already know by Fermat's theorem that $g^{p-1}, g^{2(p-1)}, \cdots, g^{p(p-1)}$ are 1 modulo p. So, there cannot be any other number which is 1 modulo p. In particular, $g, g^2, \cdots, g^{p-2} \not\equiv 1 \pmod p$. Therefore, g is a primitive root of $\mathbb{Z}_p$ as well.

55. Assume first that $x^k \equiv a \pmod n$ has a solution. Since a is a unit, clearly x must be a unit as well. Then, we have

$$a^{\frac{\phi(n)}{\gcd(k,\phi(n))}} \equiv \left(x^k\right)^{\frac{\phi(n)}{\gcd(k,\phi(n))}} \equiv x^{\frac{k\cdot\phi(n)}{\gcd(k,\phi(n))}} \equiv x^{\mathrm{lcm}[k,\phi(n)]} \equiv 1 \pmod n$$

by Euler's theorem and from the fact that $\phi(n) \mid \mathrm{lcm}[k, \phi(n)]$.

Assume now that

$$a^{\frac{\phi(n)}{\gcd(k,\phi(n))}} \equiv 1 \pmod n$$

and let g be a primitive root modulo n. Since a is a unit, we can write $a \equiv g^m \pmod n$ for some m. Then, we must have $\mathrm{ord}_n(a) = \frac{\phi(n)}{\gcd(m,\phi(n))}$ and hence

$$\frac{\phi(n)}{\gcd(m,\phi(n))} \mid \frac{\phi(n)}{\gcd(k,\phi(n))} \Longrightarrow \gcd(k,\phi(n)) \mid \gcd(m,\phi(n)) \Longrightarrow \gcd(k,\phi(n)) \mid m.$$

Since $\gcd(k,\phi(n)) \mid m$, there exists an integer t such that $tk \equiv m \pmod{\phi(n)}$ and now $x \equiv g^t \pmod n$ satisfy the congruence $x^k \equiv a \pmod n$ because

$$x^k \equiv \left(g^t\right)^k \equiv g^{tk} \equiv g^m \equiv a \pmod n.$$

56. Since $117 = 9 \times 13$, we will first consider the congruence

$$x^4 \equiv 61 \equiv 7 \pmod{9}$$

in $\mathbb{Z}_9$. Using the fact that 2 is a primitive root of $\mathbb{Z}_9$ and $7 \equiv 2^4 \pmod{9}$, we can re-write the congruence as

$$2^{4a} \equiv 2^4 \pmod{9}$$

by replacing x with 2^a for some $1 \leq a \leq 6$. Then, we have

$$2^{4a} \equiv 2^4 \pmod{9} \iff 4a \equiv 4 \pmod{6} \iff 2a \equiv 2 \pmod{3} \iff a \equiv 1 \pmod{3}.$$

So, there are two solutions $x \equiv 2^1, 2^4 \pmod{9}$.

Next, we consider the congruence

$$x^4 \equiv 61 \equiv 9 \pmod{13}$$

in $\mathbb{Z}_{13}$. Using the fact that 2 is a primitive root of $\mathbb{Z}_{13}$ and $9 \equiv 2^8 \pmod{13}$, we can re-write the congruence as

$$2^{4a} \equiv 2^8 \pmod{13}$$

by replacing x with 2^a for some $1 \leq a \leq 12$. Then, we have

$$2^{4a} \equiv 2^8 \pmod{13} \iff 4a \equiv 8 \pmod{12} \iff a \equiv 2 \pmod{3}.$$

So, there are four solutions $x \equiv 2^2, 2^5, 2^8, 2^{11} \pmod{1}3$.

Combining them by the Chinese Remainder Theorem, there are $2 \times 4 = 8$ solutions in $\mathbb{Z}_{117}$.