Exercise 1. (a) Suppose \(a\) and \(b\) are both relatively prime to the positive integer \(n\). If \(\gcd(\text{ord}_n a, \text{ord}_n b) = 1\), show \(\text{ord}_n(ab) = \text{ord}_n a \cdot \text{ord}_n b\).

(b) Let \(n\) be a positive integer and \(a\) an integer relatively prime to \(n\). If \(\text{ord}_n a = n - 1\), show \(n\) is prime.

Solutions: (a) Set \(\alpha = \text{ord}_n a\), \(\beta = \text{ord}_n b\) and \(\gamma = \text{ord}_n(ab)\). Since
\[
(ab)^{\alpha\beta} = a^{\alpha\beta} b^{\alpha\beta} = (a^\alpha)^\beta (b^\beta)^\alpha \equiv 1^{\beta} 1^{\alpha} = 1 \mod n,
\]
we deduce \(\gamma\) divides \(\alpha\beta\).

Conversely, by definition of order,
\[
1 \equiv (ab)^{\gamma} = a^\gamma b^\gamma \mod n.
\]
Raising everything to \(\alpha\),
\[
1 \equiv 1^\alpha \equiv [a^\gamma b^\gamma]^\alpha = a^{\gamma\alpha} b^{\gamma\alpha} \equiv b^{\gamma\alpha} \mod n,
\]
since \(\gamma\alpha\) is a multiple of the order \(\alpha\) of \(a\). The corollaries to Theorem 1 allow us to conclude that \(\gamma\alpha\) is divisible by \(\beta\), hence the hypothesis \(\gcd(\alpha, \beta) = 1\) yields \(\beta|\gamma\). By symmetry, we also have \(\alpha|\gamma\), hence \(\alpha\beta\) divides \(\gamma\), since \(\alpha\) and \(\beta\) are relatively prime.

Since \(\alpha\), \(\beta\), and \(\gamma\) are all positive, the preceding discussion allows us to conclude \(\gamma = \alpha\beta\), as required.

(b) If \(\text{ord}_n a = n - 1\) then
\[
n - 1|\phi(n).
\]
In particular,
\[
n - 1 \leq \phi(n).
\]
On the other hand, the definition of the Euler phi function yields
\[
n - 1 \geq \phi(n),
\]
hence \(\phi(n) = n - 1\). It was proved in class that the latter condition implies \(n\) is prime. Indeed, let \(d\) be a divisor of \(n\) with \(1 \leq d < n\). Since \(d\) divides \(n\), we have
\[
d = \gcd(d, n) = 1,
\]
the last equality following from the fact \(\phi(n) = n - 1\). We deduce that the only positive divisors of \(n\) are itself and 1, that is \(n\) is prime.

Exercise 3. (a) Let \(p\) and \(q\) be distinct odd primes. Show \(pq\) is a pseudoprime to the base 2 if and only if \(\text{ord}_p 2\) divides \(p - 1\) and \(\text{ord}_p 2\) divides \(q - 1\).

(b) Which of \(13 \cdot 67\), \(19 \cdot 73\), \(23 \cdot 89\), and \(29 \cdot 97\) are pseudoprimes to the base 2?

Solution: (a) Suppose \(pq\) is a pseudoprime to the base 2. Since \(\gcd(2, pq) = 1\),
\[
2^{pq - 1} \equiv 1 \mod pq.
\]
In particular,
\[
2^{pq - 1} \equiv 1 \mod p.
\]
It follows that \(\text{ord}_p 2\) divides \(pq - 1\). On the other hand, Euler’s Theorem ensures that \(\text{ord}_p 2\) divides \(p - 1\). Observing
\[
q - 1 = pq - 1 - q(p - 1),
\]
we deduce that \( \text{ord}_p 2 \) divides \( q - 1 \). By reversing the roles of \( p \) and \( q \), the same argument yields \( \text{ord}_q 2 \) divides \( p - 1 \).

Conversely, suppose \( \text{ord}_q 2 \) divides \( p - 1 \) and \( \text{ord}_p 2 \) divides \( q - 1 \). Since \( \text{ord}_q 2 \) divides \( p - 1 \),

\[
2^{p-1} \equiv 1 \mod q.
\]

On the other hand, Euler’s Theorem ensures

\[
2^{p(q-1)} \equiv 1 \mod q.
\]

Therefore,

\[
2^{pq-1} = 2^{p(q-1)+p-1} = 2^{p(q-1)}2^{p-1} \equiv 1 \cdot 1 = 1 \mod q. \tag{1}
\]

A similar argument shows that

\[
2^{pq-1} \equiv 1 \mod p. \tag{2}
\]

Since \( p \) and \( q \) are relatively prime, (1) and (2) allows us to deduce

\[
2^{pq-1} \equiv 1 \mod pq,
\]

which shows that \( pq \) is a pseudoprime to the base 2.

(b) If \( \text{ord}_p 2 \) divides \( q - 1 \) then it divides \( d = \gcd(q - 1, \phi(p)) = \gcd(q - 1, p - 1) \).

In particular, one

\[
2^d \equiv 1 \mod p.
\]

Conversely, if the last equation is satisfied then \( \text{ord}_p 2 \) divides \( d \), hence a fortiori it divides \( q - 1 \).

In the case \( pq = 13 \cdot 67 \), we have

\[
\gcd(q - 1, p - 1) = \gcd(66, 12) = 6.
\]

Since

\[
2^6 = 64 \equiv -1 \mod 13,
\]

the preceding discussion shows \( \text{ord}_{13} 2 \) does not divide 66. Part (a) allows us to conclude that \( 13 \cdot 67 \) is not a pseudoprime to the base 2.

In the case \( pq = 19 \cdot 73 \),

\[
\gcd(72, 18) = 18.
\]

Euler’s Theorem ensures that

\[
2^{18} \equiv 1 \mod 19
\]

On the other hand,

\[
2^6 = 64 \equiv -9 \mod 73,
\]

hence

\[
2^{18} = (2^6)^3 \equiv (-9)^3 = -729 \equiv 1 \mod 73.
\]

The preceding discussion shows that \( \text{ord}_{19} 2 \) divides \( 72 \) and \( \text{ord}_{73} 2 \) divides \( 18 \). Part (a) allows us to conclude that \( 19 \cdot 73 \) is a pseudoprime to the base 2.

In the case \( pq = 23 \cdot 89 \),

\[
\gcd(22, 88) = 22.
\]

By Fermat’s Little Theorem,

\[
2^{22} \equiv 1 \mod 23.
\]
Furthermore, direct calculation shows
\[ 2^{11} = 2048 \equiv 1 \pmod{89}. \]
The preceding discussion shows that \( \text{ord}_{89} 2 \) divides 22 and \( \text{ord}_{29} 2 \) divides 88, thus 23 \cdot 89 is a pseudoprime to the base 2.
Finally, in the case \( pq = 29 \cdot 97 \),
\[ \gcd(28, 96) = 4. \]
Observing
\[ 2^4 = 16 \]
is not congruent to 1 modulo 29, the preceding discussion shows that \( \text{ord}_{29} 2 \) does not divide 96. Part (a) allows to deduce that 29 \cdot 97 is not a pseudoprime to the base 2.
In summary, only 19 \cdot 73 and 23 \cdot 89 are pseudoprimes to the base 2.

**Exercise 3.** (a) Show that the integer 20 has no primitive roots.
(b) Find a primitive root modulo each of the following integers.
   (i) 14.
   (ii) 18.
(c) Find a complete set of incongruent primitive roots of 17.

**Solutions :** (a) If \( a \) is relatively prime to 20 then it is relatively prime to 5 and 4. Observing \( \phi(5) = 4 \), Euler’s Theorem yields
\[ a^4 \equiv 1 \pmod{5}. \tag{1} \]
Similarly, since \( \phi(4) = 2 \), Euler’s Theorem yields
\[ a^2 \equiv 1 \pmod{4}, \]
hence
\[ a^4 = (a^2)^2 \equiv 1^2 = 1 \pmod{4}. \tag{2} \]
In light of the fact \( \gcd(4, 5) = 1 \), the identities (1) and (2) combine with the Chinese Remainder Theorem to allow us to conclude
\[ a^4 \equiv 1 \pmod{20}. \]
In particular, \( \text{ord}_{20} a \leq 4 \). Since \( \phi(20) = \phi(4)\phi(5) = 2 \cdot 4 = 8 \), it follows immediately that 20 has no primitive root.
(b) (i) From lectures, we know that 3 is a primitive root of 7. Since 3 is odd and 14 = 2 \cdot 7, Lemma 42 allows us conclude that 3 is a primitive root of 14.
   (ii) From lectures, we know that 2 is a primitive root of 9. It cannot be a primitive root of 18, since 2 is not relatively prime to 18. Consider
\[ 11 = 2 + 9. \]
Since 11 \equiv 2 \pmod{9}, 11 is also a primitive root modulo 9. Since it is odd and 18 = 2 \cdot 9, Lemma 42 allows us to conclude that 11 is a primitive root of 18.
(c) Observing \( \phi(17) = 16 \), if \( a \) is reduced modulo 17 then
\[ \text{ord}_{17} a \in \{1, 2, 4, 8, 16\}. \]
Searching for a primitive root, we first consider the case \( a = 2 \). Calculations show
\[ 2^2 = 4 \not\equiv 1 \pmod{17} \]
\[ 2^4 = 16 \not\equiv -1 \pmod{17} \]
\[ 2^8 = 256 = 1 + 255 = 1 + 15 \cdot 17 \equiv 1 \pmod{17} \]
It follows that $\text{ord}_{17} 2 = 8$. Observing that the order of a power divides that of the base, no power of 2 can be a primitive root of 17. Observing
\[ 1, 2, 4, 8, 16, 32, 64, 128, 256 \]
is a complete set of incongruent powers of 2 modulo 17, it follows that none of
\[ 1, 2, 4, 8, 16, 15, 13, 9, 1 \]
is a primitive root of 17. Modulo 17, the primitive roots must lie among
\[ 3, 5, 6, 7, 10, 11, 12, 14 \] (1)
On the other hand, from lectures we know that one has
\[ \phi(16) = \phi(2^4) = 2^3 = 8 \]
incongruent primitive roots of 17. It follows immediately that (1) is a complete listing of the primitive roots of 17.

**Alternate Solution** : Observing $\phi(17) = 16$, if $a$ is reduced modulo 17 then
\[ \text{ord}_{17} a \in \{1, 2, 4, 8, 16\}. \]
Taking $a = 3$, we note
\[
\begin{align*}
3 &\not\equiv 1 \pmod{17} & 3^2 = 9 &\not\equiv 1 \pmod{17} \\
3^4 = 81 &\equiv -4 \not\equiv \pmod{17} & 3^8 = (3^4)^2 &\equiv (-4)^2 = 16 \not\equiv 1 \pmod{17}
\end{align*}
\]
In light of the restrictions on $\text{ord}_{17} 3$, the preceding calculations allows us to deduce
\[ \text{ord}_{17} 3 = 16 = \phi(17), \]
i.e. 3 is a primitive root of 17.
Since 3 is a primitive root of 17,
\[ 3^k, \quad 1 \leq k \leq 16 \]
is a reduced residue system modulo 17. Recalling that $3^k$ is a primitive root if and only if $\gcd(k, 16) = 1$, we deduce
\[ 3, 3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15} \]
is a complete set of incongruent primitive roots of 17.

**Exercise 4.** (a) Let $r$ be a primitive root of a prime $p$. If $p \equiv 1 \pmod{4}$, show $-r$ is also a primitive root.
(b) Find the least positive residue of the product of a set of $\phi(p-1)$ incongruent primitive roots modulo a prime $p$.
(c) Let $p$ be a prime of the form $p = 2q + 1$ where $q$ is an odd prime. If $a$ is an integer with $1 < a < p - 1$, show $p - a^2$ is a primitive root modulo $p$.

**Solution** : (a) Recalling
\[ r^{\phi(p)/2} \equiv -1 \pmod{p}, \]
we deduce
\[ -r \equiv r^{\phi(p)/2} r = r^{(\phi(p)+2)/2} \pmod{p}. \]
Writing
\[ p = 4n + 1, \]
we have
\[ \phi(p) = 4n \quad \text{and} \quad \frac{\phi(p) + 2}{2} = 2n + 1. \]

Observing
\[ 1 = (2n - 1)(2n + 1) - (4n), \]
we deduce
\[ \gcd(\phi(p), (\phi(p) + 2)/2) = 1. \]
Since \( \text{ord}_p r = \phi(p) \), the preceding allows us to conclude
\[ \text{ord}_p(-r) = \text{ord}_p r^{(\phi(p)+2)/2} = \frac{\phi(p)}{\gcd(\phi(p), (\phi(p) + 2)/2)} = \phi(p). \]

(b) If \( p = 2 \) then 1 is the unique primitive root modulo 2, so the product of a set of representatives of the primitive roots modulo 2 is congruent to 1 mod 2. In the case \( p = 3, -1 \) is the unique primitive root modulo 3, so the product of a set of representative of the primitive roots modulo 3 is congruent to \(-1 \equiv 2 \mod 3\).

If \( p > 3 \) then \( p - 1 > 2 \), hence \( \phi(p - 1) \) is even. Let \( r \) be a primitive root modulo \( p \). Observing \( r \) is reduced, it has an inverse \( \bar{r} \) modulo \( p \). In fact, the identity
\[ r^{p-1} \equiv 1 \mod p \]
allows us to deduce
\[ \bar{r} \equiv r^{p-2} \mod p. \]
Observing \( \gcd(p-1, p-2) = 1 \), we conclude that \( \bar{r} \) has order \( p-1 \), hence is a primitive root of \( p \). If \( r \equiv \bar{r} \mod p \) then
\[ r^2 = r \cdot r \equiv r \cdot \bar{r} \equiv 1 \mod p. \]
In this case, \( p - 1 = \text{ord}_pr \) would divide 2, hence \( p \leq 3 \), a contradiction.

Consider a product of \( \phi(p - 1) \) incongruent roots of \( p \). In light of the previous paragraph, each root can be paired with its inverse, yielding \( \phi(p - 1)/2 \) pairs of factors. Since the product of each pair is congruent to 1 modulo \( p \), we deduce that the product of all the factors is congruent to 1 modulo \( p \).

In summary, if \( p = 2 \) or \( > 3 \) then the least positive residue of the product of \( \phi(p - 1) \) incongruent primitive roots of \( p \) is 1. In the case \( p = 3 \), the least positive residue is 2.

(c) Observing
\[ \phi(p) = 2q, \]
the fact \( q \) is an odd prime allows us to conclude that if \( x \) is reduced modulo \( p \) then
\[ \text{ord}_p x \in \{1, 2, q, 2q\}. \]
Now consider \( p - a^2 \). In light of Fermat’s Little Theorem,
\[ (p - a^2)^q \equiv (-a^2)^q = (-1)^qa^{2q} \equiv -1 \mod p, \]
since \( q \) is odd. It follows that \( p - a^2 \) does not have order \( q \).

If \( p - a^2 \) is not a primitive root of \( p \) then the preceding discussion shows that its order is either 1 or 2, i.e. divides 2. In this case, one would have
\[ 1 \equiv (p - a^2)^2 \equiv (-a^2)^2 = a^4 \mod p. \]
In particular, \( \text{ord}_pa \) must divide 4, hence is either 1 or 2. Observing that 1 is the unique residue class of order 1 and \(-1 \) is that of order 2, it would follow that
\[ a \equiv \pm 1 \mod p. \]
This contradicts the assumption $1 < a < p - 1$. We conclude $p - a^2$ is a primitive root of $p$, as required.

**Exercise 5.** (a) Find a primitive root for each of the following moduli.

(i) $17^2$.
(ii) 26.
(iii) $2662$.
(iv) $37^k$, $k$ is a positive integer.

(b) Find all the primitive roots modulo 38.

**Solution:**
(a) (i) From exercise 3(c), 3 is a primitive root of 17. Noting

$$3^4 = 81 = -4 + 5 \cdot 17$$

we have

$$3^8 = (3^4)^2 = (-4 + 5 \cdot 17)^2$$

$$\equiv -16 - 40 \cdot 17 \equiv -1 - 7 \cdot 17 \pmod{17^2}.$$

Therefore,

$$3^{16} = (3^8)^2 \equiv (-1 - 7 \cdot 17)^2 \equiv 1 + 14 \cdot 17 \pmod{17^2}.$$ 

In particular, $3^{16} \not\equiv 1 \pmod{17}$. The proof of Theorem 9 allows us to conclude that 3 is a primitive root of $17^2$.

(ii) We note $26 = 2 \cdot 13$. Observing

$$\phi(13) = 12,$$

if $a$ is relatively prime to 13 then $\text{ord}_{13} a$ divides 12. Observing

$$2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16 \equiv 3 \pmod{13}, \quad 2^6 = 64 \equiv -1 \pmod{13},$$

we deduce that 2 is a primitive root of 13. Since 2 is an even primitive root of 13, Theorem 42/3 allows us conclude that

$$2 + 13 = 15$$

is a primitive root of 26.

(iii) We observe that $2662 = 2 \cdot (11)^3$. As

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

the order of 2 modulo 11 is neither 1, 2, or 5. Since it is a divisor of $\phi(11) = 10$, we deduce that

$$\text{ord}_{11} 2 = 10.$$ 

In particular, 2 is a primitive root of 11.

We calculate

$$2^{10} = (2^5)^2 = (32)^2 = (-1 + 33)^2 \equiv 1 - 66 = -65 \pmod{121}.$$ 

In particular, $2^{10} \not\equiv 1 \pmod{121}$, so Theorem 9 tells us that 2 is a primitive root of $121 = (11)^2$. Theorem 11 allows us to conclude 2 is a primitive root for any positive power of 11; in particular, it is a primitive root of $1331 = (11)^3$.

Since 2 is a even primitive root of 1331, we conclude

$$2 + 1331 = 1333$$

is a primitive root of $2 \cdot 1331 = 2662$.

(iv) We first note

$$\phi(37) = 36.$$
Furthermore,

\[
\begin{align*}
2^2 &= 4, & 2^3 &= 8, \\
2^4 &= 16, & 2^6 &= 64 \equiv -10 \mod 37, \\
2^9 &= 512 \equiv -6 \mod 37, & 2^{12} &= 4096 \equiv 26 \mod 37, \\
2^{18} &\equiv (-6)^2 = 36 \equiv -1 \mod 37.
\end{align*}
\]

Observing \( \text{ord}_{37} 2 \) divides 36, the preceding calculations allow us to conclude that 2 is a primitive root of 37. Since

\[
2^9 = -6 + 14 \cdot 37,
\]

we have

\[
2^{18} \equiv (-6 + 14 \cdot 37)^2 \equiv 36 - 168 \cdot 37 \equiv 36 + 17 \cdot 37 \equiv -1 \mod 37^2
\]

In particular, 2\(^{18} \) is not congruent to 1 modulo 37. It follows from Theorem 9 that 2 is a primitive root of 37. Theorem 11 allows us to conclude that 2 is a primitive root of \((37)^k\) for all \(k \geq 1\).

(b) We first note 38 = 2 \cdot 19. Observing

\[
\begin{align*}
2^2 &= 4, & 2^3 &= 8, \\
2^6 &= 64 \equiv 7 \mod 19, & 2^9 &= 2^3 \cdot 2^6 \equiv 8 \cdot 7 = 56 \equiv -1 \mod 19,
\end{align*}
\]

the fact \( \text{ord}_{19} 2 \) divides \( \phi(19) = 18 \) allows us to conclude that 2 is a primitive root of 19. Since 2 is even, Theorem 42/3 allows us to conclude that

\[
2 + 19 = 21
\]

is a primitive root of 38. Observing \( \phi(38) = \phi(2)\phi(19) = 18 \), every reduced residue class modulo 38 can be uniquely expressed in the form

\[
21^k, \quad 1 \leq k \leq 18.
\]

Such a class is a primitive root if and only if it has order 18 = \( \text{ord}_{38} 21 \). As this occurs precisely when \(k\) is relatively prime to 18 = \( \phi(38) \), we deduce

\[
21, 21^5, 21^7, 21^{11}, 21^{13}, 21^{17}
\]

is a complete listining of the incongruent primitive root modulo 38.

**Exercise 6.** Let \( p \) be an odd prime and \( t \) a positive integer. Show that \( p^t \) and \( 2p^t \) have the same number of primitive roots.

**Solution:** From the lectures, there exists \( r \) which is a primitive root of both \( p^t \) and \( 2p^t \). Observing

\[
\phi(p^t) = \phi(p^{2t}),
\]

it follows that

\[
r^k, \quad 1 \leq k \leq \phi(p^t)
\]

is a reduced residue system for both \( p^t \) and \( 2p^t \). In each cases, the primitive roots correspond to the exponents \( k \) with \( \gcd(k, \phi(p^t)) = 1 \), hence we see that there are

\[
\phi(\phi(p^t)) = \phi(\phi(2p^t))
\]

primitive roots in each case.

**Bonus Question.** Suppose \( n \) be a positive integer possessing a primitive root \( r \). Using \( r \) show that the product of all positive integers less than \( n \) and relatively prime to \( n \) is congruent to \(-1\) modulo \( n \). (This is an extension of Wilson’s Theorm, which is the special case \( n = p \) is prime.)
Solution: The case \( n = 1 \) or \( n = 2 \) are trivial. We consider the case \( n > 2 \), in which case \( \phi(n) \) is even. Since \( r \) is a primitive root,
\[
r^k, \quad 1 \leq k \leq \phi(n),
\]
is a reduced residue system modulo \( n \). Since the set of positive integers less than \( n \) and relatively prime to \( n \) also form a reduced residue system modulo \( n \), we deduce that that product of the latter elements is congruent modulo \( n \) to
\[
\prod_{k=1}^{\phi(n)} r^k = r^{\sum_{k=1}^{\phi(n)} k} = r^{\phi(n)(\phi(n)+1)/2}.
\]

Consider the element \( r^{\phi(n)/2} \). We note that it has order 2. On the other hand, if \( 1 \leq k \leq \phi(n) \) has the property that \( r^k \) has order 2 then the formula for the order of \( r^k \) yields
\[
\gcd(k, \phi(n)) = \frac{\phi(n)}{2}.
\]
In particular,
\[
\frac{\phi(n)}{2} | k | \phi(n).
\]
Since \( r^k \) does not have order 1, we deduce
\[
k = \frac{\phi(n)}{2}.
\]

The preceding paragraph allows us to conclude that \( r^{\phi(n)/2} \) is the unique reduced residue of order 2. Observing that \(-1\) is a reduced residue of order 2, we conclude that
\[
r^{\phi(n)/2} \equiv -1 \mod n.
\]
Thus,
\[
\prod_{k=1}^{\phi(n)} r^k = r^{\phi(n)(\phi(n)+1)/2} = \left(r^{\phi(n)/2}\right)^{\phi(n)+1} \equiv (-1)^{\phi(n)+1} = -1 \mod n,
\]
since \( \phi(n) + 1 \) is odd.