Composite Numbers With Prime-like Property
Notations:
1) $a|b$: a divides b E.g. $15|45$

2) $(a,b)=d$: GCD of a and b is d E.g. $(15,7)=1$

3) $a \equiv b \pmod{n}$: $n|(a-b)$ E.g. $70 \equiv 25 \pmod{15}$

4) $\phi(n)=$ Number of integers a, such that $1 \leq a \leq (n-1)$ and $(a,n)=1$

E.g. $\phi(11)=10$, because $\{1,2,...,10\}$,
$\phi(9)=6$ because $\{1,2,4,5,7,8\}$, and $\phi(6)=2$ because $\{1,5\}$

Note: For a prime p, $\phi(p)=p-1$,
$\phi(p^2)=p(p-1)=p^2-p$, because $\{1,2,...,p^2-1\} \setminus \{p,2p,3p,....,(p-1)p\}$

Caution: $\tau(n)$= Number of positive divisors of n.
$\phi(n)$= Euler's Totient function

Think of a number line with integers....

For integers m and $n \neq 0$, we have $m=nk+r$ where $0 \leq r < |n|$.

E.g. $m=-34$ and $n=5$. $-34=-7*5+1$.
$m=21$ and $n=5$. $21=4*5+1$. Notice the placements of -34 and 21 on the number line. One distance to the right of -35 and 21 respectively. So for a positive integer n, n distinct remainders give us a way to partition all integers into n "classes"....
So $\{\bar{0},\bar{1},....,\overline{n-1}\}$ is a complete set of "residue classes" modulo n. We eventually will drop the bar for convenience of writing.
So for $n=4$, $\{\bar{0},\bar{1},\bar{2},\bar{3}\}$ or$\{\overline{-7},\overline{-6},\overline{-5},\overline{-4}\}$ which is "lined up" as $\{\bar{1},\bar{2},\bar{3},\bar{0}\}$
or we could consider $\{\overline{-2},\overline{-1},\bar{0},\bar{1}\}$ which is "lined up" as $\{\bar{2},\bar{3},\bar{0},\bar{1}\}$.

Do these have to be consecutive integers? How about $\{\bar{0},\bar{2},\bar{4},\bar{6}\}$?
$\bar{6}=\bar{2}$ since $6 \equiv 2$ mod(4).So not a **Complete Set of Residue Classes (CSRC)**.
How about $\{\bar{0},\bar{3},\bar{6},\bar{9}\}$? This is "lined up" as $\{\bar{0},\bar{3},\bar{2},\bar{1}\}$.

(Extra 1: Prove that if $(k,n)=1$ and $\{\overline{a_1},\overline{a_2},....,\overline{a_n}\}$ is a CSRC then $\{k\overline{a_1},k\overline{a_2},....,k\overline{a_n}\}$ as well as $\{k\overline{a_1}+r,k\overline{a_2}+r,....,k\overline{a_n}+r\}$ are both CSRCs.)

Note: For modulo n, $\bar{a}=\bar{b}$, iff $a \equiv b \pmod{n}$

Note: If $n|a$, $n|b$, and k is an integer, then $n|ka$ and $n|a+b$.

Properties:
If $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, and k an integer, then

i) $a + c \equiv b + d \pmod{n}$. (Think of directed distances adding up)
ii)$a - c \equiv b - d \pmod{n}$. (Think of directed distances subtracting)
iii) $ka \equiv kb \pmod{n}$. (Think of directed distance multiplied by k)
iv) $ac \equiv bd \pmod{n}$. (Not so straight forward) (Explain using Pythagorean Theorem to distance formula to this proof pattern.....)
$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$.

GCD, Euclidean Algorithm, other facts derived from Eu. AL.

(i) Finding GCD: Using Eu.Al. instead of prime factorization.
$(5064, 624)=$?
$5064 = 8 * (624) + 72$
$624 = 8 * (72) + 48$
$72 = 1 * (48) + \underline{24}$
$48 = 2 * (24) + 0$

(ii) Argument that 24 is a common divisor is.....

Now let $d = (5064, 624)$. So $d|5064$ and $d|624$.

$5064 - 8 * (624) = 72$
$624 - 8 * (72) = 48$
$72 - 1 * (48) = \underline{24}$

Argument that $d|24$ is .....
So 24 is the GCD.

(iii)Alternate proof that last non-zero remainder is the GCD:
Observation: $(a, b) = (kb + r, b) = (b, r), so (5064, 624) = (624, 72) = (72, 48) = (48, 24) = 24$

Caution: If $a = kb + r$ then $(a, b) = (b, r)$ but it is not necessary that $(a, b) = (a, r)$. E.g. $70 = 4(15) + 10$, where $(70, 15) = 5 = (15, 10)$ but $(70, 10) = 10$. Actually $(a, b)|(a, r)$

Observation 1: The last non-zero remainder is the GCD.

(iii) Also, working backwards on Eu. Al., we get:
$24 = 72 - 48$
$24 = 72 - (624 - 8 * 72)$
$24 = 9 * 72 - 624$
$24 = 9 * (5064 - 8 * 624) - 624$
$24 = 9 * 5064 - 73 * 624$

Observation 2: The GCD, $(\mathbf{a}, \mathbf{b})$ can be written as a linear combination of a and b.

Note that if $m = ka + rb$, then $(a, b)|m$. So (a, b) is the smallest positive integer that can be a linear combination of a and b and all such positive integers are $d, 2d, 3d....$

Observation 3: The GCD, $(\mathbf{a}, \mathbf{b})$ is the smallest positive integer that can be written as a linear combination of a and b. And all such positive linear combinations are multiples of $(\mathbf{a}, \mathbf{b})$.

If $ra \equiv b \pmod{n}$, then there exists an integer k such that $kn = ra - b$. I.e. $b = ra - kn$. So b is a lin. comb. of a and n. So by Fact 3, $(a, n)|b$. Obviously, if $b = 1$ then $(a, n) = 1 (= b)$.

Observation 4: $\mathbf{ra} \equiv \mathbf{b} \pmod{\mathbf{n}} \implies (\mathbf{a}, \mathbf{n})|\mathbf{b}$ and
$\mathbf{ra} \equiv \mathbf{1} \pmod{\mathbf{n}} \implies (\mathbf{a}, \mathbf{n}) = \mathbf{1}$

Observation 5: If $\mathbf{a} = \mathbf{kb} + \mathbf{r}$ then $(\mathbf{a}, \mathbf{b}) = (\mathbf{b}, \mathbf{r})$ and $(\mathbf{b}, \mathbf{r})|(\mathbf{a}, \mathbf{r})$. E.g. $\mathbf{70} = \mathbf{4} * \mathbf{15} + \mathbf{10}$.

Observation 6:If $\mathbf{a} \equiv \mathbf{b} \pmod{\mathbf{n}} \implies (\mathbf{a}, \mathbf{n}) = (\mathbf{b}, \mathbf{n})$

(Extra 2: Using extra 1 stated above and these six observations, try proving Euler's theorem and Fermat's Little Theorem yourself before looking at the proofs.)
Reminder: **Euler's Totient Function**: $\phi(n)$: For any positive integer n, $\phi(n)$ is the number of all positive integers k less than n that are relatively prime to n.

Also, note that $a^{(n-1)} \equiv 1 \pmod{n}$ means $n|a^{(n-1)} - 1$. There exists an integer k, such that $nk = a^{(n-1)} - 1$. $1 = a^{(n-1)} - nk$. So 1 is a linear combination of a and n. $(a, n) = 1$ (Could have just used Observation 6 here.)

Euler's Theorem: Let a and n be relatively prime positive integers. I.e. $(a, n) = 1$.
Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Fermat's Little Theorem: Let a be a positive integer and p be a prime.
Then $a^p \equiv a \pmod{p}$.

[Side note:] Use this theorem to solve AMC 10B 2017 problem 14 quickly.

Note: For a prime p: Any integer is either a multiple of p or is relatively prime to p.
So, $a \not\equiv 0 \pmod{p} \iff (a, p) = 1$.

So Fermat's Little Theorem can be split into two cases:
case 1: a is a multiple of p. Then $a \equiv 0 \pmod{p}$ and $a^p \equiv 0 \pmod{p}$.
So $a^p \equiv a \pmod{p}$. Not a very interesting fact.

case 2: $(a, p) = 1$. Use Euler's Theorem. $\phi(p) = p - 1$, so
Statement 1: $(a, p) = 1 \Rightarrow a^{(p-1)} \equiv 1 \pmod{p}$.

This means $a^p \equiv a \pmod{p}$

This can be equivalently stated as
Statement 2: $a \not\equiv 0 \pmod{p} \Rightarrow a^{(p-1)} \equiv 1 \pmod{p}$.

Is this true for primes only? The two equivalent statements in case 2 are not equivalent for a non-prime. E.g. 30 is not a multiple of 42 and $(30,42) = 6 \neq 1$.
$(a, n) = 1$ is a stricter condition than $a \not\equiv 0 \pmod{n}$ when n is a composite number.((a,n) could be a proper divisor of n.)

We will prove that the second statement forces n to be a prime while the first statement does not. We will give counter example to show that the first one does not.

If n is a positive integer such that, $a \not\equiv 0 \pmod{n} \Rightarrow a^{(n-1)} \equiv 1 \pmod{n}$ for every positive integer a, then n is a prime.

Comment: $a \not\equiv 0 \pmod{n}$ is not as strict as $(a, n) = 1$, so it has more candidates for a, which means statement 2 has a stronger property to satisfy.
proof: Since 2 and 3 are primes, assume $n > 3$. If n satisfies the property then for any positive integer a,
$a \not\equiv 0 \pmod{n} \Rightarrow a^{(n-1)} \equiv 1 \pmod{n}$.
But $a^{(n-1)} \equiv 1 \pmod{n} \Rightarrow (a, n) = 1$.
So by transitivity,
$a \not\equiv 0 \pmod{n} \Rightarrow (a, n) = 1$.
I.e. $(r, n) = 1$ for $r = 1, 2, ..., n - 1$. n is a prime.

Claim: There exist composite numbers that satisfy the property in the first statement. How do we find one?

If $n = pq$, a product of two distinct primes, then for any positive integer a, $(a, n) = 1 \Rightarrow (a, p) = 1$ and $(a, q) = 1$. We could use FLT to get $a^{(p-1)} \equiv 1 \pmod{p}$ and $a^{(q-1)} \equiv 1 \pmod{q}$. Now if $p - 1|n - 1$ and $q - 1|n - 1$, then we will have $a^{(n-1)} \equiv 1 \pmod{p}$ and $a^{(n-1)} \equiv 1 \pmod{q}$. I.e. $p|a^{(n-1)} - 1$ and $q|a^{(n-1)} - 1$. $(p, q) = 1$, so $pq|a^{(n-1)} - 1$. I.e. $n|a^{(n-1)} - 1$ and we will be done.

Notice $p|n$ and $p - 1|n - 1$ is rare. It doesn't happen very often. E.g. $17 = 1 * 17$ but $16 = 2^4$. Even for composite numbers: $50 = 2 * 5^2$ but $49 = 7^2$.

We need to search for suitable primes. $n = 2q$ won't work because $n - 1$ would be odd and $q - 1$ even meaning $q - 1 \not| n - 1$. $n = 3q$ $(p = 3)$ is a good candidate because $2|n - 1$. Now we need q such that $q - 1|n - 1$.

Notice that $3q - 1 = 3(q - 1) + 2$. The remainder is 2 when $n - 1$ is divided by $q - 1$. So $n = 3q$ won't work either. In fact $n = pq$ won't work for any two distinct primes: Let $p < q$. $pq - 1 = p(q - 1) + p - 1$. So remainder is p-1...
Well, maybe we need three distinct primes! $p = 3$ is still a promising candidate. $q = 11$ is easy to work with because we just need to make n to end with 1. So $n = pqr = 33r$. r=7 or 17 or 37 ...? Need to try them. $r = 7$ doesn't work since $3 * 7 * 11 = 231$ and $6 \nmid 230$. $r = 17$? $3 * 17 * 11 = 51 + 510 = 561$, and $2|560, 10|560, 16|560$. 561 is a Carmichael number.
The interesting fact is that this process is not just convenient but the only way to create Carmichael numbers.
Why $p - 1|n - 1$?:
Definitions:
1) For positive integers a, n such that $(a, n) = 1$, *order* of a mod n is the least $m \geq 1$ such that $a^m \equiv 1 \pmod{n}$.
2) Also, if $m = n - 1$, a is called the *primitive root* of n.
Fact we need:(proof not included here but refer to the document referenced at the end to develop more understanding): For every prime p, there exist a primitive root. So there exists an a with order $p - 1$.
Claim: Existence of a primitive root implies that $p - 1|n - 1$ if $p|n$ for a Carmichael number n and a prime p.
Thought Process: If $p - 1 \nmid n - 1$, then there is a positive remainder r, giving $n - 1 = k(p - 1) + r$.
So $a^{(n-1)} = a^{k(p-1)+r} = a^{k(p-1)}a^r$.
If we can find a primitive root a for one of the prime factors of n, such that $(a, n) = 1$,then $a^{(n-1)} \equiv 1 \pmod{n}$, since n is Carmichael, so $a^{(n-1)} \equiv 1 \pmod{p}$.
$a^{(p-1)} \equiv 1 \pmod{p}$ by FLT, so $a^{k(p-1)} \equiv 1 \pmod{p}$.
So $1 \equiv a^r \pmod{p}$. $r < (p - 1)$, but order of a is $p - 1$. Contradiction. This proves that $p - 1|n - 1$.

Need **Chinese Remainder Theorem:** For positive integers $n_1, n_2, ..., n_k$ and integers $a_1, a_2, ..., a_k$,
i) $x \equiv a_1 \pmod{n_1}$
$x \equiv a_2 \pmod{n_2}$
.
.
.
$x \equiv a_k \pmod{n_k}$
ii) $(n_i, n_j) = 1$ for $1 \leq i, j \leq k$
iii) then this system has a solution and the solution is unique modulo $N = n_1 n_2 ... n_k$.

Example: A box has gold coins. When divided among 6 people, 4 coins are left over, 5 people, 3 coins are left over. How many coins in the box? Notice that $(6, 5) = 1$. Answer: $30n + 28$.

https://kconrad.math.uconn.edu/blurbs/ugradnumthy/carmichaelkorselt.pdf

https://kconrad.math.uconn.edu/blurbs/ugradnumthy/ordersmodm.pdf

https://en.wikipedia.org/wiki/Carmichael_number