Number Theory Homework.

Recall that we defined $U(n)$ to be

$$U(n) = \{k : 1 \leq k \leq n, \gcd(k, n) = 1\}$$

and that the Euler ϕ function is the size of this set:

$$\phi(n) = \#U(n).$$

Let us generalize this a bit. If $d \mid n$, set

$$U(u, d) = \{k : 1 \leq k \leq n, \gcd(k, n) = d\}$$

Thus $U(n) = U(n, 1)$. There is an easy description of $U(n, d)$.

Proposition 1. *Let n and d be positive integers with $d \mid n$. Then*

$$U(n, d) = \{d\ell : \ell \in U(n/d)\}$$

thus the equality

$$\#U(n, d) = \#U(n/d) = \phi(n/d)$$

holds.

Problem 1. Prove this. *Hint:* If $k \in U(n, d)$, then $d \mid k$ and therefore $k = d\ell$ for some positive integer ℓ. Show that $1 \leq \ell \leq n/d$ and that $\gcd(\ell, n/d) = 1$. Conversely show if $1 \leq \ell \leq n/d$ and $\gcd(\ell, n/d) = 1$, then show $k = d\ell \in U(n, d)$. $\square$

Let $f \colon \mathbb{Z}_+ \to \mathbb{R}$ be a real valued function on the positive integers. Then for any positive integer n let

$$\sum_{d \mid n} f(d)$$

be the sum of all the numbers $f(d)$ where $d > 0$ and $d \mid n$. For example

$$\sum_{d \mid 6} f(d) = f(1) + f(37), \qquad \sum_{d \mid 6} f(d) = f(1) + f(2) + f(3) + f(6)$$

Note

$$\begin{aligned} \sum_{d \mid 6} f(6/d) &= f(6/1) + f(6/2) + f(6/3) + f(6/6) \\ &= f(6) + f(3) + f(2) + f(1) \\ &= \sum_{d \mid 6} f(d) \end{aligned}$$

This is a general fact.

Lemma 2. *Let f be a real valued function on the positive integers. Then*

$$\sum_{d \mid n} f(d) = \sum_{d \mid n} f(n/d)$$

Problem 2. Prove this. *Hint:* One way is to let $S = \{d : d \mid n\}$ and $T = \{n/d : d \mid n\}$. Then

$$\sum_{d|n} f(d) = \sum_{d\in S} f(d), \qquad \sum_{d|n} f(n/d) = \sum_{k\in T} f(k)$$

so it is enough to show $S = T$. $\square$

Theorem 3. *For any positive integers n*

$$n = \sum_{d|n} \phi(n).$$

Problem 3. Prove this. *Hint:* With the set up we have here, the easiest way is to first show

$$\{1, 2, 3, \dots, n\} = \bigcup_{d|n} U(n, d)$$

and that this union is disjoint (i.e. if $d_1 \neq d_j$ then $U(n, d_1) \cap U(n, d_2) = \varnothing$). Thus

$$n = \#\{1, 2, 3, \dots, n\} = \sum_{d|n} \#U(n, d),$$

and now you can use the results above. $\square$

Proposition 4. *If n is a positive integer and a is an integer with $\gcd(a, n) = 1$, then there is a positive integer k such that*

$$a^k \equiv 1 \mod n$$

Proof. Consider the sequence $a, a^2, a^3, \cdots$. As there are only n residue classes mod n there are integers r and s with $0 < r < s$ and $a^r \equiv a^s \mod n$. Write this as $a^r \equiv a^r a^{s-r} \mod n$. As $\gcd(a^r, n) = 1$ we can cancel the a^r from both sides of $a^r \equiv a^r a^{s-r} \mod n$ to conclude $a^k \equiv 1 \mod n$ with $k = s - r$. $\square$

Problem 4. If $\gcd(a, n) \neq 1$, then there is no positive integer k such that $a^k \equiv 1 \mod n$. $\square$

Definition 5. If n and a are integers with n positive and $\gcd(a, n) = 1$, then the ***order of*** a ***modulo*** n, written $\mathrm{ord}_n(a)$, is the smallest positive integer such that $a^k \equiv 1 \mod n$. (When the number n is clear from context we will write $\mathrm{ord}(a)$ rather that $\mathrm{ord}_n(a)$ and say "the order of a" rather than "order of a modulo n".) $\square$

Proposition 6. *Let $\gcd(a, n) = 1$ and let m be any integer with*

$$a^m \equiv 1 \mod n.$$

Then

$$\mathrm{ord}(a) \mid m$$

Problem 5. Prove this. *Hint:* Use the division algorithm to divide $\operatorname{ord}(a)$ into m to get $m = q\operatorname{ord}(a) + r$ where $0 \le r < \operatorname{ord}(a)$. Use that $a^{\operatorname{ord}(a)} \equiv a^m \equiv 1 \mod n$ to deduce $a^r \equiv 1 \mod n$. Now use the minimality of $\operatorname{ord}(a)$ to conclude $r = 0$. $\square$

Corollary 7. *If* $\gcd(a,n) = 1$ *then* $\operatorname{ord}_n(a) \mid \phi(n)$. *Therefore* $\operatorname{ord}_n(a) \le \phi(n)$.

Proof. By Euler's theorem $a^{\phi(n)} \equiv 1 \mod n$ and thus this is a direct consequence Proposition 7. $\square$

Here are tables of powers of a^k reduced modulo n for $2 \le n$, $1 \le a \le n$, $\gcd(a,n) = 1$ and $1 \le k \le \phi(n)$

$n=2$		
a	a	$\operatorname{ord}_3(a)$
1	1	1

$n=3$			
a	a	a^2	$\operatorname{ord}_3(a)$
1	1	1	1
2	2	1	2

$n=4$				
a	a	a^2	a^3	$\operatorname{ord}_4(a)$
1	1	1	1	1
3	3	1	3	2

$n=5$					
a	a	a^2	a^3	a^4	$\operatorname{ord}_5(a)$
1	1	1	1	1	1
2	2	4	3	1	4
3	3	4	2	1	4
4	4	1	4	1	2

$n=7$							
a	a	a^2	a^3	a^4	a^5	a^6	$\operatorname{ord}_7(a)$
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

$n=6$			
a	a	a^2	$\operatorname{ord}_6(a)$
1	1	1	1
5	5	1	2

$n=9$							
a	a	a^2	a^3	a^4	a^5	a^6	$\operatorname{ord}_9(a)$
1	1	1	1	1	1	1	1
2	2	4	8	7	5	1	6
4	4	7	1	4	7	1	3
5	5	7	8	4	2	1	6
7	7	4	1	7	4	1	3
8	8	1	8	1	8	1	2

$n=8$					
a	a	a^2	a^3	a^4	$\operatorname{ord}_8(a)$
1	1	1	1	1	1
3	3	1	3	1	2
5	5	1	5	1	2
7	7	1	7	1	2

$n=10$					
a	a	a^2	a^3	a^4	$\operatorname{ord}_{10}(a)$
1	1	1	1	1	1
3	3	9	7	1	4
7	7	9	3	1	4
9	9	1	9	1	2

We single out the elements a that achieve the upper bound of $\operatorname{ord}_n(a) = \phi(n)$.

Definition 8. The integer a is a ***primitive element*** modulo n if $\operatorname{ord}_n(a) = \phi(n)$. $\square$

For some n there will be no primitive elements.

Problem 6. Use the tables above to find for which n there exists a primitive element modulo n. In the case that there is a primitive element, list all of them. $\square$

Proposition 9. *If n is positive integer and a is an integer with $\gcd(a, n) = 1$, then for any positive integers j*

$$\operatorname{ord}(a^j) = \frac{\operatorname{ord}(a)}{\gcd(j, \operatorname{ord}(a))}.$$

Thus $\operatorname{ord}(a^j) = \operatorname{ord}(a)$ if and only if $\gcd(j, \operatorname{ord}(a)) = 1$.

Problem 7. Prove this along the following lines. Let $k = \operatorname{ord}(a)$ and $d = \gcd(j, n)$. Write $j = dj'$ and $n = dk'$ where d' and k' are integers and, as we have seen in similar arguments, $\gcd(j', k') = 1$. In this notation the goal is to show $\operatorname{ord}(a^j) = k/d = k'$.

(a) Show that $(a^j)^{k'} = (a^k)^{j'}$ and therefore $(a^j)^{k'} \equiv 1 \mod n$. Thus $\operatorname{ord}(a^j) \leq k'$.
(b) If $\ell > 0$ and $(a^j)^\ell \equiv 1 \mod n$, then by Proposition 6 we have $k \mid j\ell$, that is $dk' \mid dj'\ell$. Use this to show $k' \mid \ell$. Now let $\ell = \operatorname{ord}(a^j)$ to conclude $k' \leq \operatorname{ord}(a^j)$. $\square$

Lemma 10. *Let k and n be positive integers and assume that the congruence*

$$x^k = 1 \mod n$$

has at most k solutions in $\mathbb{Z}_n$. Then there are at most $\phi(k)$ elements of order k in $\mathbb{Z}_n$.

Problem 8. Prove this along the following lines. If there are no elements of order k then the result holds, so assume that there is at least one element, a, of order k. Let S be the set

$$S = \{1, a, a^2, \dots, a^{k-1}\}.$$

(a) Show all the elements of S are distinct modulo n, and thus S has k elements modulo n.
(b) Show that every element of S satisfies $x^k \equiv 1 \mod n$.
(c) Show that if b satisfies $x^k \equiv 1 \mod n$, then $b \equiv a^j \mod n$ for some $j \in \{0, 1, 2, \dots, k-1\}$.
(d) Show if $\operatorname{ord}(b) = k$, then b must be in S and therefore $b \equiv a^j$ for some j with $1 \leq j \leq k$ and $\gcd(j, k) = 1$.
(e) Show that there are exactly $\phi(k)$ element of order k in $\mathbb{Z}_n$. $\square$

Lemma 11. *If p is a prime number and k is any positive integer, then*

$$x^k \equiv 1 \mod p$$

has at most k solutions modulo p.

Proof. This is a special case of the result that we have seen earlier that an polynomial with integer coefficients of degree k and with lead coefficient not divisible by p has at most k solutions modulo p. $\square$

Theorem 12 (Gauss' Theorem on the existence of primitive elements)**.** *For any prime p there is at least one primitive element modulo p.*

Problem 9. Prove this along the following lines. As p is prime $\phi(p) = p-1$. By Proposition 7 for any a with $\gcd(a,p) = 1$ we have $\operatorname{ord}_p(a)|(p-1)$. For any $d > 0$ with $d \mid (p-1)$ let

$$S(d) = \{a : 1 \leq a \leq (p-1), \operatorname{ord}_p(a) = d\}.$$

Note that $S(d-1)$ is the set of elements order $\phi(p) = (p-1)$, so $S(p-1)$ is the set of primitive elements. Therefore our goal is to show $\#S(p-1) > 0$.

(a) Explain why

$$\{1, 2, \ldots, (p-1)\} = \bigcup_{d|(p-1)} S(d).$$

(b) Show

$$(p-1) = \sum_{d|(p-1)} \#S(d).$$

(c) Show

$$\#S(d) \leq \phi(d)$$

Hint: Combine Lemmas 10 and 11.

(d) Use parts (b), (c), and Theorem 3 to show

$$(p-1) = \sum_{d|(p-1)} \#S(d) \leq \sum_{d|(p-1)} \phi(d) = (p-1)$$

and there we have $\#S(d) = \phi(d)$ for all d that divides $(p-1)$.

(e) Finish the proof by noting that the last part shows that $\#S(p-1) = \phi(p-1) > 0$. This not only shows that there is a primitive element modulo p, it shows there are exactly $\#S(p-1) = \phi(p-1)$ of them. $\square$

Proposition 13. *If p is prime, the number of primitive element modulo p is $\phi(p-1)$.*

Proof. This is a direct corollary to the proof of the last theorem. $\square$