"Direct" proof of Theorem 11.7 (Euler's Theorem)

The proof will be accomplished in three steps. All congruences are modulo n.

STEP 1: Define a relation $\mathcal{R}$ on $\mathbb{Z}_n^\times$ as follows:

$$x \,\mathcal{R}\, y \quad \Leftrightarrow \quad \exists\, i \in \mathbb{Z} : \; x \equiv a^i y.$$

I claim that $\mathcal{R}$ is an equivalence relation.

Reflexivity: $x \,\mathcal{R}\, x$ for any x since $x \equiv a^0 x$.
Symmetry: $x \equiv a^i y \Rightarrow y \equiv a^{-i} x$. Note that $a^{-i} \pmod{n}$ makes sense, since a is invertible mod n.
Transitivity: If $x \equiv a^i y$ and $y \equiv a^j z$, then because of associativity, $x \equiv a^i(a^j z) \equiv (a^i a^j)z \equiv a^{i+j} z$.

STEP 2: Since $\mathcal{R}$ is an equivalence relation, it partitions $\mathbb{Z}_n^\times$ into equivalence classes. Let H denote the class containing the element a itself. By definition of $\mathcal{R}$, H consists of all integer powers of a (mod n). Note that there must be only finitely many of these, up to repititions, since $\mathbb{Z}_n^\times$ is a finite set, of size $\phi(n)$. Hence, there must exist positive integers $i < j$ such that $a^j \equiv a^i$. Multiplying both sides by $a^{-i} \pmod{n}$, it follows that $a^{j-i} \equiv 1$. Thus, there is *some* positive integer k such that $a^k \equiv 1$. I claim that

$$|H| = \min\{k \in \mathbb{N} : a^k \equiv 1\}.$$

Let l denote the smallest positive integer such that $a^l \equiv 1$. If the powers $a = a^1,\, a^2,\, \dots,\, a^l \equiv 1$ were not all distinct mod n, then there would be some $1 \le i < j \le l$ such that $a^i \equiv a^j$ and, arguing as above, it would follow that $a^{j-i} \equiv 1$. But $j - i$ is a positive integer strictly less than l, which contradicts the definition of l. Hence the powers $a^1,\, a^2,\, \dots,\, a^l$ are all distinct modulo n, which proves that $|H| \ge l$.

On the other hand, let $t \in \mathbb{N}$ be any number greater than l. We can write $t = ql + r$, where $q \in \mathbb{N}$ and $0 \le r < l$. Then $a^t = a^{ql+r} = (a^l)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r$. So every power a^t is congruent to one of $1 = a^0 = a^l,\, a^1,\, a^2,\, \dots,\, a^{l-1}$, modulo n, which proves that $|H| \le l$. Thus $|H| = l$, v.s.v.

STEP 3: Suppose we can show that every equivalence class of $\mathcal{R}$ has the same size. Then the size of the whole set $\mathbb{Z}_n^\times$ must be a multiple of the size of any single class, that is a multiple of $|H|$. In other words, l must divide $\phi(n)$, say $\phi(n) = q \cdot l$. But then $a^{\phi(n)} = a^{ql} = (a^l)^q \equiv 1^q \equiv 1$, v.s.v.

To show that every class has the same size, we just have to note that, by the definition of $\mathcal{R}$, for any $x \in \mathbb{Z}_n^\times$, the map

$$a^i \mapsto a^i x \pmod{n}, \; i = 1,\, 2,\, \dots,\, l,$$

establishes a 1-1 correspondence between the elements of the class H and the class containing x.