1. (a) Since $n, o_+(a) \in \mathbb{N}$, we can apply the Division Algorithm to get that $n = q \cdot o_+(a) + r$ for some $q, r \in \mathbb{N}$ where $r < o_+(a)$. However, note that

$$\begin{aligned}(q \cdot o_+(a) + r)a &= 0 \\ q \cdot o_+(a) \cdot a + ra &= 0 \\ ra &= 0\end{aligned}$$

But $r \leq o_+(a)$, which contradicts the minimality of $o_+(a)$ if $r \neq 0$, so it must be that $r = 0$. Thus, we get that $o_+(a) \mid n$ as desired.

(b) If $char(R) = 0$, then $o_+(a) \mid 0$ if $o_+(a)$ exists. If $char(R) \neq 0$, then it is the smallest positive integer where $char(R) \cdot 1_R = 0$. Thus, for $a \in R$, and from Exercise 7.3 b), we get that

$$\begin{aligned}char(R) \cdot a &= char(R) \cdot (1_R \cdot a) \\ &= (char(R) \cdot 1_R)a \\ &= 0 \cdot a \\ &= 0\end{aligned}$$

Thus, we get that $char(R) \cdot a = 0$, so from a), it follows that $o_+(a) \mid char(R)$ as desired.

(c) We first prove Exercise 7.5's result:

Proof for Exercise 7.5

If $char(R) = m$, then $m \cdot 1_R = 0$. We then note that every element in $\hat{R} = \{0, 1_R, 2 \cdot 1_R, \cdots, (m-1) \cdot 1_R\}$ is nonzero (except for 0) and unique. If any other element aside from 0 is equal to 0, it would contradict the minimality of $char(R)$. Thus, if there exist $d, e \in \mathbb{Z}$ where $0 \leq d < e \leq (m-1)$ and $d \cdot 1_R = e \cdot 1_R$, we get that $(e-d) \cdot 1_R = 0$ where $0 < (e-d) < char(R)$, which again contradicts the minimality of $char(R)$ and proves uniqueness.

Since $\hat{R}$ contains m elements and the order of R is m, by the pigeonhole principle, there exists a bijective map $g : R \to R$ where for $r \in R$, $r \mapsto d \cdot 1_R$ where $0 \leq d \leq (m-1)$. We now construct a map $f : R \to \mathbb{Z}/m\mathbb{Z}$ where $r \mapsto [d]_m$ for $r = d \cdot 1_R$.

We first prove the map is well-defined. For $r \in R$ where $r = d_1 \cdot 1_R = d_2 \cdot 1_R$ for $d_1, d_2 \in \mathbb{Z}$, we get that $(d_1 - d_2) \cdot 1_R = 0$, which implies $o_+(1) = char(R) = m \mid (d_1 - d_2)$ from (a). Note that $f(d_1 \cdot 1_R) - f(d_2 \cdot 1_R) = [d_1]_m - [d_2]_m = [d_1 - d_2]_m$. Since $m \mid (d_1 - d_2)$, we get that $d_1 - d_2 \equiv 0 \pmod{m}$, thus $[d_1 - d_2]_m = [0]_m$, so $[d_1]_m = [d_2]_m$ as desired.

We now prove it is a ring homomorphism by first showing that:

$$\begin{aligned}f(1) = f(1 \cdot 1_R) = [1]_m \\ f(0) = f(0 \cdot 1_R) = [0]_m\end{aligned}$$

We then prove for any $r_1, r_2 \in R$ where for $d_1, d_2 \in \mathbb{Z}$ and $r_1 = d_1 \cdot 1_R$ and $r_2 = d_2 \cdot 1_R$ that:

$$\begin{aligned}f(r_1 + r_2) &= f((d_1 + d_2) \cdot 1_R) \\ &= [d_1 + d_2]_m \\ &= [d_1]_m + [d_2]_m \\ &= f(r_1) + f(r_2)\end{aligned}$$

$$
\begin{aligned}
f(r_1 \cdot r_2) &= f((d_1 \cdot d_2) \cdot 1_R) \\
&= [d_1 \cdot d_2]_m \\
&= [d_1]_m \cdot [d_2]_m \\
&= f(r_1) \cdot f(r_2)
\end{aligned}
$$

Thus, we get that f is a ring homomorphism. We now prove injectivity. We first assume $r_1, r_2 \in R$ with $r_1 = d_1 \cdot 1_R$ and $r_2 = d_2 \cdot 1_R$ for $d_1, d_2 \in \mathbb{Z}$ where $f(r_1) = f(r_2)$, then $f(r_1 - r_2) = f(0) = 0$. Thus, $[d_1 - d_2]_m = [0]_m$, which implies $d_1 - d_2 \equiv 0 \pmod m$, so $m \mid (d_1 - d_2)$. There exists an integer q where $mq = d_1 - d_2$, so $(d_1 - d_2) \cdot 1_R = q \cdot (m \cdot 1_R) = q \cdot 0 = 0$. Thus, $r_1 - r_2 = 0$ or $r_1 = r_2$. Note that R and $\mathbb{Z}/m\mathbb{Z}$ both have order m. By the pigeonhole principle, injective maps between sets of the same size are also surjective. Hence, f is bijective, which gives us $R \cong \mathbb{Z}/m\mathbb{Z}$ as desired. **(End of proof for Exercise 7.5)**

We now return to c). We first denote $\hat{R} = \{0, a, 2 \cdot a, \cdots, (m-1) \cdot a\}$. Note that each element is non-zero (except for 0) or else they contradict the minimality of $o_+(a) = m$. If there exist $d, e \in \mathbb{Z}$ where $0 \le d < e \le (m-1)$ and $d \cdot a = e \cdot a$, we get that $(e-d) \cdot a = 0$ where $0 < (e-d) < m$, which again contradicts the minimality of $o_+(a)$ and proves uniqueness.

Note that the size of $\hat{R}$ is m, which is the order of R. By the pigeonhole principle, it implies there exists a bijective map $g : R \to R$ where for every $r \in R$, $r \mapsto d \cdot a$ for $0 \le d \le (m-1)$ for some $d \in \mathbb{Z}$. Thus, for $a^2 = ka$ and $1_R = ba$ for some integers k, b and $0 \le k, b \le m-1$. We get as follows:

$$
\begin{aligned}
a \cdot 1_R &= ba^2 \\
&= bka \\
&= a
\end{aligned}
$$

Since $bka = a$, we note that $(bk-1)a = 0$. By (a), this implies $m \mid (bk-1)$. This implies there exists an integer q where $bk - 1 = qm$, so $bk - qm = 1$. This implies that $\gcd(m, b) = 1$. Let $t \cdot 1_R = 0$ where t is a non-negative integer and $t \cdot 1_R = tb \cdot a = 0$. This implies that $m \mid tb$. By Corollary 2.20, since $\gcd(m, b) = 1$, we get that $m \mid t$. The smallest positive integer t can be is m. Thus, $\mathrm{char}(R) = m$. Thus, we can apply Exercise 7.5 and get $R \cong \mathbb{Z}/m\mathbb{Z}$ as desired.

(d) We claim that $o_+(a+b) = mn$. By contradiction, we assume t as a positive integer where $t(a+b) = 0$ and $t < mn$. By the Exercise 7.3 b), note that:

$$
\begin{aligned}
m(ta + tb) &= 0 \\
t(ma) &= -mtb \\
0 &= -mtb
\end{aligned}
$$

This implies $n \mid mt$, but $\gcd(m, n) = 1$, so by Corollary 2.20, $n \mid t$. If we then do $n(ta+tb)$, it follows that we can conclude $m \mid t$. We then note that since $gcd(m, n) = 1$, we get that $\gcd(m, n) \cdot \mathrm{lcm}(m, n) = \mathrm{lcm}(m, n) = |nm| = nm$. By Exercise 4.1, since $n \mid t$ and $m \mid t$, we get that by Exercise 4.1 that $mn \mid t$. This is a contradiction since $t < mn$. Thus, $o_+(a+b) = mn$.

(e) By contradiction, we assume $char(R)$ is neither 0 or a prime. If $char(R) = 1$, then $1_R = 0$, which is impossible for a ring. Meanwhile, if $char(R) \neq 1, 0,$ or any prime p, we get that there exist positive integers m, n where $m, n \neq 1, char(R)$ and $mn = char(R)$. Note that since $1 < m, n < char(R)$, $m \cdot 1$ and $n \cdot 1$ are non-zero elements of the ring or it contradicts the minimality of $char(R)$. However, we get that $(m \cdot 1_R) \cdot (n \cdot 1_R) = mn \cdot 1_R = 0$. This is a contradiction to the definition of an integral domain.

2. (a) For the reflexive property, we note that:

$$f(x) = f(x+0) \quad \forall x \in \mathbb{F}_p$$

Thus, we get that $f \sim f$.

For the symmetric property, assume a $g \in S(r)$ where $f \sim g$, we get that there exist an $a \in \mathbb{F}_p$ where

$$\begin{aligned} f(x) &= g(x+a) \quad \forall x \in \mathbb{F}_p \\ f(x-a) &= g(x) \\ g(x) &= f(x+(-a)) \end{aligned}$$

Thus, we get that $g \sim f$.

For the transitive property, assume $g, h \in S(r)$ where $f \sim g$ and $g \sim h$. We note that there exist an $a, b \in \mathbb{F}_p$ where $f(x) = g(x+a)$ and $g(x) = h(x+b)$. Hence:

$$\begin{aligned} g(x+a) &= h((x+a)+b) \\ f(x) &= h((x+a)+b) \\ f(x) &= h(x+(a+b)) \end{aligned}$$

Thus, we get that $f \sim h$. Since the relation satisfies all the property of an equivalence relation, it is an equivalence relation.

(b) Let $f \in S(r)$. We first consider the case where f is a constant function: for all $x \in \mathbb{F}_p$, $f(x) = d$ for some $d \in R$. Thus, for any $g \in S(r)$ with $f \sim g$, we note that its output must also be constant, so $f = g$. Since only $f \sim f$, it follows that the only element in its equivalence class is itself. Thus, the size is 1.

Meanwhile, we consider the case where f is not a constant function. Let $a \in \mathbb{F}_p$, and define $g_a(x) = f(x+a)$. By Lemma 1.1, the map $x \mapsto x+a$ for $x \in \mathbb{F}_p$ is bijective. Thus there do not exist $x_1 \neq x_2$ in $\mathbb{F}_p$ with $x_1 + \hat{a} = x_2 + \hat{a}$, and hence there exists a unique $\hat{x} \in \mathbb{F}_p$ with $g_a(\hat{x}) = f(x)$. Hence,

$$\sum_{x \in \mathbb{F}_p} f(x) = \sum_{\hat{x} \in \mathbb{F}_p} g_a(\hat{x}) = r.$$

Thus, $g_a \in S(r)$ and $f \sim g_a$. Let $G = \{g_a : a \in \mathbb{F}_p\}$ and note that $f \in G$ because $f = g_0$. For all $g \in G$, they are equivalent to each other since we proved $f \sim g$. Let $a, b \in \mathbb{F}_p$ with $a \neq b$, we prove that $g_a \neq g_b$. By contradiction, suppose $g_a = g_b$. This implies that

$$f(x+a) = f(x+b) \quad \forall x \in \mathbb{F}_p.$$

Denote $c = b - a$ and we get that:

$$\begin{aligned} f(x+a-b+c) &= f(x+b-b+c), \\ f(x) &= f(x+c). \end{aligned}$$

We also have $f(x+c) = f(x+c+c)$, so by repeating this k times for any positive integer k we get $f(x) = f(x+kc)$. Since $a \neq b$, we have $c \neq 0$. We now show that $x, x+c, x+2c, \ldots, x+(p-1)c$ are all distinct. By contradiction, there exist integers $i \neq j$ with $0 \leq i < j \leq p-1$ such that $x + ic = x + jc$ in $\mathbb{F}_p$.

Then $jc - ic = (j-i)c = 0$ in $\mathbb{F}_p$, i.e., $(j-i)c \equiv 0 \pmod{p}$. However, $c \neq 0$ in $\mathbb{F}_p$, so $c \not\equiv 0 \pmod{p}$. Thus, by Euclid's Lemma, $p \mid (j-i)$, which is a contradiction since $0 < (j-i) \leq p-1$.

Since $x, x+c, x+2c, \ldots, x+(p-1)c$ are p distinct elements of $\mathbb{F}_p$ and $|\mathbb{F}_p| = p$, they represent every element of $\mathbb{F}_p$. Hence $f(x) = f(x+kc)$ for all k implies that f is constant, a contradiction. Thus, $g_a \neq g_b$. Since there are p distinct elements in $\mathbb{F}_p$, there are also p distinct functions in G. Thus, the equivalence class size is p.

3. Let I be an ideal of R. If $I = \{0\}$, then $I = (0)$, which is a principal ideal. If $I \neq \{0\}$, let the set $P = \{N(x) : x \in I,\ x \neq 0\}$. Since P is nonempty as $I \neq \{0\}$ and $P \subset \mathbb{Z}$, by the well-ordering principle, there exists a smallest element. We denote $d \in I$ where $N(d)$ is the smallest element of P. We note that $(d) \subseteq I$. Let $n \in I$, since R is a Euclidean domain, there exist $q, r \in R$ where $n = dq + r$. We note that $r = n - dq \in I$ since $n, d \in I$. However, we note that $N(r) < N(d)$ if r is nonzero, which contradicts the minimality of $N(d) \in P$. Hence, it must be that $r = 0$, so $d \mid n$ and $n \in (d)$. This proves $I \subseteq (d)$, which implies $I = (d)$. Hence, every ideal $I \in R$ is a principal ideal, so R is a PID.

4. (a) We first note that $(0,1)$ is not a unit because if it is, there exist $(a,b) \in \mathbb{Z}^2$ with $(0,1)\cdot(a,b) = (1,1)$. Then $0 \cdot a = 1$, which is impossible for any given $a \in \mathbb{Z}$. Thus, since $(0,1) = (0,1)\cdot(0,1)$, it can be expressed as the product of non-units, so it is not irreducible.

   Meanwhile, let $(a,b),(p,q) \in \mathbb{Z}^2$. If $a = 0$, then we set $q = b$, and we get that $(0,1)\cdot(p,q) = (0,b)$. Thus, $(0,1) \mid (a,b)$. Hence, we also note the contrapositive that if $(0,1) \nmid (a,b)$, then $a \neq 0$.

   By contradiction, $(0,1)$ is not prime, so there exist $(a,b),(c,d) \in \mathbb{Z}^2$ where $(0,1) \mid (ac,bd)$ but $(0,1) \nmid (a,b)$ and $(0,1) \nmid (c,d)$. This implies both $a, c \neq 0$, and since $\mathbb{Z}$ is an integral domain, $ac \neq 0$. However, since $(0,1) \mid (ac,bd)$, it is also implied that $ac = 0$, which is a contradiction. Thus, $(0,1)$ is prime.

   (b) By Lemma 9.2, for any $f, g \in R$, we get that $\deg(fg) = \deg(f)+\deg(g)$. By contradiction, x is not irreducible, so there exist two non-unit polynomials f, g where $fg = x$. However, from the lemma, we note that since the degree of polynomials are non-negative integers, either $\deg(f) = 1$ and $\deg(g) = 0$ or vice versa. Assume $\deg(f) = 0$, which implies $f \in \mathbb{Q}$ as it is a constant. However, since $f \in \mathbb{Q}$ and $f \neq 0$ and $\mathbb{Q}$ is a field, $f^{-1} \in \mathbb{Q} \subset R$. Thus, f is a unit, which is a contradiction. Thus, x is irreducible.

   Meanwhile, note that $(\sqrt{2}x)\cdot(\sqrt{2}x) = 2x^2 = 2x \cdot x$. Thus, $x \mid (\sqrt{2}x)\cdot(\sqrt{2}x)$. However, we note that if $x \mid (\sqrt{2}x)$, then there exists a $q \in R$ where $xq = \sqrt{2}x$. R is an integral domain and since $x(q - \sqrt{2}) = 0$, it implies $q = \sqrt{2}$. This is a contradiction because $\sqrt{2} \notin R$. Thus, $x \nmid (\sqrt{2}x)$, which proves x is not prime.

   (c) Assume r is prime, then if $r \mid ab$, then $r \mid a$ or $r \mid b$. By contradiction, assume r is not irreducible, so $r = de$ where $d, e \in R$ and are non-units. Since $r = de$, we assume $r \mid d$, thus there exist $d \in R$ where $d = rq$. Hence, we get that $r = rqe$. Since R is a PID, it is an integral domain, thus:

$$
\begin{aligned}
r &= rqe \\
0 &= r(qe-1) \\
qe &= 1
\end{aligned}
$$

   This implies e is a unit, which is a contradiction! Thus, if r is prime, then r is irreducible.

   For the converse, assume r is irreducible. By contradiction, r is not prime, so there exist a $r \mid ab$, but $r \nmid a$ and $r \nmid b$. We then denote the ideal $(r,a) = \{rx + ay : x, y \in R\}$. Since R is a PID, there exist a principal ideal (d) for $d \in R$ where $(r,a) = (d)$. Since $r \in (r,a)$, we note that $d \mid r$ and $d \mid a$.

   Since $d \mid r$, there exists a $u \in R$ where $du = r$. If d is a non-unit, we note that u must be a unit or it contradicts that r is irreducible. However, this implies that $u^{-1}r = d \cdot 1$. Since $d \mid a$, there exist an $k \in R$ where $a = dk = (u^{-1}r)k$. This implies that $r \mid a$, which is a contradiction. Thus, d is a unit, so $(d) = (1)$ by Lemma 8.5.

   Since $(r,a) = (1)$, we get that $1 \in (r,a)$, so there exist $x, y \in R$ where $rx + ay = 1$. Thus, if we multiply both sides by b, we get that $brx + bay = b$. Since $r \mid ab$, so there exist a $z \in R$ where $rz = ab$. We get that $r(bx + zy) = b$. This implies $r \mid b$, which is a contradiction to r being not prime. Hence, if r is irreducible, then r is prime.