1. (a) We begin by noting that:

$$0 + 0 = 0 \in S + I$$
$$1 + 0 = 1 \in S + I$$

Let $s_x + a_x, s_y + a_y \in S + I$. We note that $-s_x \in S$ and $-1 \cdot a_x \in I$. Thus:

$$-s_x + (-a_x) = -(s_x + a_x) \in S + I$$

For addition, we get that:

$$s_x + a_x + s_y + a_y = (s_x + s_y) + (a_x + a_y) \in S + I$$

For multiplication, we get that:

$$(s_x + a_x) \cdot (s_y + a_y) = (s_x s_y) + (s_y a_x + s_x a_y + a_x a_y) \in S + I$$

Thus, we conclude that $S + I$ is a subring.

(b) We begin by noting that $0 \in I$ and $0 \in S$, so $0 \in S \cap I$. Let $a, b \in S \cap I$. We note that $a + b \in S$ and $a + b \in I$. Thus, $a + b \in S \cap I$. Lastly, let $s \in S$. We note that $as \in S$ and $as \in I$, so $as \in S \cap I$. This proves $S \cap I$ is an ideal of S.

(c) We first note that $S \subseteq S + I$. Thus, the natural projection map $\pi : S \to (S + I)/I$ where $s \mapsto [s]$ is a ring homomorphism.

We then note that for all $x \in (S + I)/I$, there exists a $s + a$ such that $s \in S$ and $a \in I$ where $x = [s + a] = [s] + [a] = [s]$ because $I \mid a$, which implies $[a] = [0]$. Thus, $x = \pi(s)$. Hence, π is surjective, so it implies $\mathrm{im}(\pi) = (S + I)/(I)$.

For $x \in S \cap I$, $\pi(x) = [x] = [0]$ as $I \mid x$, so $x \in \ker(\pi)$. Meanwhile, for $x \in \ker(\pi)$, we note that $[x] = [0]$, which implies $I \mid x$ or $x \in I$. Thus, we get $x \in S \cap I$ and that $\ker(\pi) = S \cap I$.

By the First Isomorphism Theorem, we get that $S/(S \cap I) \cong (S + I)/I$.

2. (a) We note that $[0] \in J'$, so $0 \in J$. For $a, b \in J$, we get that $[a], [b] \in J'$, so $[a+b] \in J'$ and $a + b \in J$. For $r \in R$, note that $[r] \in R/I$, so $[ra] \in J'$ thus $ra \in J$. This proves J is an ideal of R.

(b) We note that $0 \in J$, so $[0] \in J/I$. For $[a], [b] \in J/I$, we note that $a + b \in J$, so $[a+b] = [a] + [b] \in J/I$. For $[r] \in R/I$, we note that $ra \in J$, so $[ra] = [r] \cdot [a] \in J/I$. This proves J/I is an ideal of R/I.

(c) We note that the natural projection map of $\pi : R \mapsto R/I$ where $r \mapsto [r]_I$ is a ring homomorphism. Meanwhile, the natural projection map of $\hat{\pi} : R/I \to (R/I)/(J/I)$ where $[r]_I \mapsto [[r]_I]_{J/I}$ is a ring homomorphism. Hence, if we denote $\varphi = \hat{\pi} \circ \pi$, we get that $\varphi : R \mapsto (R/I)/(J/I)$ where $r \mapsto [[r]]$ is a ring homomorphism.

For all $x \in (R/I)/(J/I)$, there exists an $[r] \in R/I$ where $x = [[r]]$ and consequently, an $r \in R$ where $[[r]] = \varphi(r)$. This proves *varphi* is surjective, so $\mathrm{im}(\varphi) = (R/I)/(J/I)$.

For $x \in J$, $\varphi(x) = [[x]]$. We also note that $[x] \in J/I$, so $[[x]] = [[0]]$ thus $x \in \ker(\varphi)$. Meanwhile, for $x \in \ker(\varphi)$, $\varphi(x) = [[0]]$, so $[x] \in J/I$, which further implies $x \in J$. Thus, $\ker(\varphi) = J$.

By the First Isomorphism Theorem, $R/J \cong (R/I)/(J/I)$.

3. (a) A proper ideal I is prime ideal if and only if $ab \in I$ then $a \in I$ or $b \in I$

(b) Assume (r) is a prime ideal. By contradiction, we assume r is not prime. Then there exists $a, b \in R$ where $r \mid ab$ but $r \nmid a$ and $r \nmid b$. We note that $ab \in (r)$. This implies either $a \in (r)$ or $b \in (r)$. If we assume $a \in (r)$, then there exists a $q \in R$ where $rq = a$, but that would mean $r \mid a$, a contradiction. Thus, if (r) is a prime ideal, then r is prime.

Assume r is prime. By contradiction, we assume (r) is not a prime ideal, so there exists an $ab \in (r)$ where $a, b \notin (r)$. Since $ab \in (r)$, there exists a $q \in R$ where $ab = rq$, so $r \mid ab$. This implies either $r \mid a$ or $r \mid b$. We assume $r \mid a$, so there exists a $q' \in R$ where $q'r = a$. However, this implies $a \in (r)$, a contradiction. Thus, if r is prime, then (r) is a prime ideal.

(c) Assume I is a prime ideal of R. By contradiction, we assume R/I is not an integral domain, so there exists $[a], [b] \neq [0]$ and $[ab] = [0]$. Since $[ab] = [0]$, $I \mid ab$. This implies either $I \mid a$ or $I \mid b$, so either $[a] = [0]$ or $[b] = [0]$, a contradiction. Thus, if I is a prime ideal, R/I is an integral domain.

Assume R/I is an integral domain. By contradiction, I is not a prime ideal of R. Thus, there exists $a, b \notin I$ but $I \mid ab$. This implies $[ab] = [0]$. However, R/I is an integral domain, so either $[a] = [0]$ or $[b] = [0]$. But that implies either $I \mid a$ or $I \mid b$, a contradiction. Thus, if R/I is an integral domain, then I is a prime ideal of R.

(d) We note that $\mathbb{Z}$ is a PID. Thus, for all prime ideals I of $\mathbb{Z}$, there exists an $x \in \mathbb{Z}$ where I = (x). From b), x must be prime. By Euclid's Lemma, all prime numbers are prime, so their principal ideals are also prime ideals. However, 0 satisfies the definition of prime because $\mathbb{Z}$ is an integral domain, so if $0 \mid ab$ then either a or b must be zero, so (0) is also a prime ideal. Thus, all prime ideals of $\mathbb{Z}$ are principal ideals of prime numbers and 0.

(e) From 1b), we note that $S \cap I$ is an ideal. For $a, b \in S$, if $ab \in S \cap I$, then $ab \in I$, which implies either $a \in I$ or $b \in I$. In other words, we get that either $a \in S \cap I$ or $b \in S \cap I$. Thus, $S \cap I$ is a prime ideal.

4. (a) If $[x]^2 = [x]$ for $0 \leq x \leq 2024$, then it implies $[x^2 - x] = [0]$ or $2025 \mid x(x-1)$. We then note that $2025 = 81 \cdot 25$ and that $\gcd(81, 25) = 1$. Thus, we can apply Theorem 7.11, where $m = 81$ and $n = 25$ and note that:

$$\begin{aligned}
[x(x-1)]_{2025} &\mapsto [x(x-1)]_{81} \times [x(x-1)]_{25} \\
[0] &\mapsto [0]_{81} \times [0]_{25}
\end{aligned}$$

We also note that this map is a ring homomorphism, so since $[x^2 - x] = [0]$, it implies that $[x(x-1)] = [0]_{81}$ and $[x(x-1)] = [0]_{25}$. In other words, we get that $81 \mid x(x-1)$ and $25 \mid x(x-1)$. We then note that 25 is a prime power of 5^2. By Euclid's Lemma, either $5 \mid x$ or $5 \mid x - 1$. Since $\gcd(x-1, x) = 1$, only one of the factors could be divisible by 5 and will be the one also divisible by 25. A similar argument can be applied that only one of the factors is divisible by 81. Thus, we get that either and $25 \mid x$ or $25 \mid x - 1$ and $81 \mid x$ or $81 \mid x - 1$. This gives us 4 possible combinations.

Case 1 If $25 \mid x$ and $81 \mid x$, since 81 and 25 are co-prime, we get that $2025 \mid x$. The only x that satisfies this is if $x = 0$.

Case 2 If $25 \mid x - 1$ and $81 \mid x - 1$, since 81 and 25 are co-prime, we get that $2025 \mid x - 1$. The only x that satisfies this is if $x - 1 = 0$ or $x = 1$.

Case 3 If $25 \mid x - 1$ and $81 \mid x$, it implies there exist $a, b \in \mathbb{Z}$ where $25a = x - 1$ and $81b = x$. Thus:

$$\begin{aligned}
25a &= 81b - 1 \\
1 &= 81b + 25(-a)
\end{aligned}$$

We apply the Division Algorithm strategy back in Claim 2.7 to compute that $b = 21$, so $x = 21 \cdot 81 = 1701$.

Case 4 If $25 \mid x$ and $81 \mid x - 1$, it implies there exist $a, b \in \mathbb{Z}$ where $25a = x$ and $81b = x - 1$. Thus:

$$\begin{aligned}
81b &= 25a - 1 \\
1 &= 25a + 81(-b)
\end{aligned}$$

We apply the same strategy to compute that $a = 13$ thus $x = 13 \cdot 25 = 325$

Hence, there are 4 idempotent elements in $\mathbb{Z}/2025\mathbb{Z}$.

(b) We note that $0^2 = 0$ and $1^2 = 1$, so $0, 1 \in S$. For $a, b \in S$, we note that:

$$\begin{aligned}
(a+b)^2 &= a^2 + 2ab + b^2 \\
&= a^2 = 2 \cdot 1 \cdot ab + b^2 \\
&= a^2 + b^2 \\
&= a + b
\end{aligned}$$

Thus, $a + b \in S$. Meanwhile::

$$\begin{aligned}
(ab)^2 &= a^2 b^2 \\
&= ab
\end{aligned}$$

Thus, $ab \in S$. Lastly, we note that:

$$\begin{aligned} a + a &= 2a \\ &= 2 \cdot 1 \cdot a \\ &= 0 \end{aligned}$$

Thus, we note that $-a = a$ and since $a \in S$, we get that $-a \in S$. We proved S is a subring of R.

(c) We first note that $(0) = \{r0 : r \in R\} = \{0\}$. Meanwhile, we note that the map $\varphi : R \to R$ where $r \mapsto r$ is a ring homomorphism. Meanwhile, the $\text{im}(\varphi) = R$ and that $\ker(\varphi) = \{0\} = (0)$. By the First Isomorphism Theorem, we get that $R/(0) \cong R$.

For $(e) + (1 - e)$, we note that for all $r \in R$ that

$$er + (1 - e)r = 1r = r$$

Hence, $r \in (e) + (1 - e)$ and $(e) + (1 - e) = R$. This allows us to apply Theorem 8.24 to get that $R/((e)(1 - e)) \cong R/(e) \times R/(1 - e)$. We then note that for any $a, b \in R$, we get that

$$(1 - e)a \cdot (e)b = (e - e^2)ab = 0ab = 0$$

This implies that any finite sum in the form of $\sum (e)a_i(1 - e)b_i$ is a sum of finitely many zeros, which sums to zero. Hence, $(1 - e)(e) = \{0\} = (0)$ and we get that $R \cong R/(0) \cong R/(e) \times R/(1 - e)$ or $R \cong R/(e) \times R/(1 - e)$ as desired.

(d) Let $|R| = 2$ where $R = \{0, 1\}$. By Theorem 7.16, $|R| \cdot 1 = 0$. Thus, $\text{char}(R) = 2$ (we note that $\text{char}(R) = 1$ is impossible because it implies $0 = 1$). By Exercise 7.5 (I proved it in HW5 1c), since $\text{char}(R) = |R|$, we get that $R \cong \mathbb{F}_2$. By induction, we assume all finite commutative ring R where every element is idempotent with $2 \leq |R| \leq k$ for $k \in \mathbb{N}$ is isomorphic to a product of $\mathbb{F}_2$. We now assume such ring R where $|R| = k+1$.

If there exists an $e \in R$ where it is non-zero and non-unit, by c), we get that $R \cong R/(e) \times R/(1 - e)$. For all $r \in R$, we note that:

$$[r]_e^2 = [r^2]_e = [r]_e$$
$$[r]_{1-e}^2 = [r^2]_{1-e} = [r]_{1-e}$$

Since the natural projections $R \to R/(e)$ and $R \to R/(1 - e)$ are surjective, we note that all elements in both rings are idempotent. Since both (e) and $(1 - e)$ are the kernels of their respective natural projections, by the pigeonhole principle, a non-injective but surjective map implies $|R/(e)|, |R/(1 - e)| < |R|$. Hence, by the induction hypothesis, both are isomorphic to a product of $\mathbb{F}_2$. Hence, we get that:

$$R \cong (\mathbb{F}_2 \times \cdots \times \mathbb{F}_2) \times (\mathbb{F}_2 \times \cdots \times \mathbb{F}_2)$$
$$R \cong \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$$

Meanwhile, if there is no non-zero and non-unit element in R, then R must be a field because every non-zero element is a unit. For all $a \in R^\times$, there exists a $b \in R^\times$ where $ab = 1$. This implies $a(ab) = a$, but $a^2b = ab$, so $1 = ab = a$. Thus, $R^\times = \{1\}$. Since R is a field, we get that $R = \{0, 1\}$, which contradicts our assumption of $|R| = k + 1$, making it impossible.

We proved that all finite commutative rings R where every element is idempotent is isomorphic to a product of $\mathbb{F}_2$.

5. (a) We first prove that $\text{im}(ev_a)$ is a subring of $\mathbb{C}$. We note that $1, 0 \in \mathbb{Z}[x]$, so $0, 1 \in \text{im}(ev_a)$. For all $d, e \in \text{im}(ev_a)$, there exists a $f, g \in \mathbb{Z}[x]$ where $f(a) = d$ and $g(a) = e$. We note that $-f \in Z[x]$, so $-f(a) = -d \in \text{im}(ev_a)$. Meanwhile, $f + g, fg \in \mathbb{Z}[x]$, so $f(a) + g(a) = d + e, f(a)g(a) = de \in \text{im}(ev_a)$. This proves $\text{im}(ev_a)$ is a subring of $\mathbb{C}$. We also note $x \in \mathbb{Z}[x]$, so $a \in \text{im}(ev_a)$.

We now prove it is the smallest subring containing a. For any subring S containing a, for all $x \in \text{im}(ev_a)$, there also exists an $f \in \mathbb{Z}[x]$ where $f(a) = x$. f is a polynomial and S is closed under addition and multiplication for all of its elements. We also note $\mathbb{Z} \subseteq S$ because we can add $1, -1 \in S$ and we can add them indefinitely. This implies $f(a) = x \in S$, so $\text{im}(ev_a) \subseteq S$. Since all subrings S containing a contains $\text{im}(ev_a)$, it is the smallest subring containing a, which implies $\text{im}(ev_a) = \mathbb{Z}[a]$.

(b) For each β_k, there exists a $f_k \in \mathbb{Z}[x]$ where $f_k(a) = \beta_k$ from our result in (a). We then denote $d = \max\{\deg(f_1), \cdots, \deg(f_k)\} + 1$. Since $-a^d \in \mathbb{Z}[a]$, there exists, $c_1, \cdots, c_n$ where $c_1 f_1(a) + \cdots + c_n f_n(a) = -a^d$. We construct the polynomial:

$$f(x) = x^d + c_1 f_1(x) + \cdots + c_n f_n(x)$$

We note that $f(a) = 0$. Since $\deg(x^d) \geq \deg(f_k)$ for all $1 \leq k \leq n$, the leading coefficient of f is 1. Thus, we constructed a monic polynomial where $f(a) = 0$.

(c) We denote $C = \{c_0 + c_1 a + \cdots + c_{d-1} a^{d-1} : c_0, c_1, \ldots, c_{d-1} \in \mathbb{Z}\}$.

For all $c \in \mathbb{Z}[a]$, there exists $f \in \mathbb{Z}[x]$ with $f(a) = c$ as proven in (a). By Proposition 9.4, $f(x) = q(x)g(x) + r(x)$ for $q, r \in \mathbb{Z}[x]$ since $g(x)$ is monic, so its leading coefficient is a unit and $\deg r < \deg g$. Since $g(a) = 0$, we get $f(a) = r(a)$. Since $\deg r \leq d - 1$, we get that $r(a)$ is a sum of integer coefficients up to a^{d-1}, so $r(a) = c \in C$.

For all $c \in C$, we have $c = c_0 + c_1 a + \cdots + c_{d-1} a^{d-1}$. The polynomial $f(x) = c_0 + c_1 x + \cdots + c_{d-1} x^{d-1} \in \mathbb{Z}[x]$, so $f(a) = c \in \mathbb{Z}[a]$. Hence, $\mathbb{Z}[a] = C$.

6. (a) We note that $(0)_{n=1}^{\infty}, (1)_{n=1}^{\infty} \in \varprojlim R_n$ because $f_n(0) = 0$ and $f_n(1) = 1$ for all $n \in \mathbb{N}$. Let $(a_n)_{n=1}^{\infty}, (b_n)_{n=1}^{\infty} \in \varprojlim R_n$. We get that $(a_n + b_n)_{n=1}^{\infty} \in \varprojlim R_n$ because $f_n(a_{n+1} + b_{n+1}) = f_n(a_{n+1}) + f_n(b_{n+1}) = a_n + b_n$. We also get that $(a_n b_n)_{n=1}^{\infty} \in \varprojlim R_n$ because $f_n(a_{n+1}b_{n+1}) = f_n(a_{n+1})f_n(b_{n+1}) = a_n b_n$. Lastly, we get that $-(a_n)_{n=1}^{\infty} = (-a_n)_{n=1}^{\infty} \in \varprojlim R_n$ because $f_n(-a_{n+1}) = -f_n(a_{n+1}) = -a_n$. Thus, $\varprojlim R_n$ is a subring of $\prod_{n=1}^{\infty} R_n$.

(b) By contradiction, $\mathbb{Z}_p$ does not have characteristic 0. This implies there exist a positive integer m where $m \cdot (1)_{n=1}^{\infty} = (0)_{n=1}^{\infty}$. In other words, for all $n \in \mathbb{N}$, we get that $m \cdot 1 \equiv 0 \pmod{p^n}$. However, there exist large enough a $k \in \mathbb{N}$ where $p^k > m$, so $m \not\equiv 0 \pmod{p^k}$. This is a contradiction, so the characteristic of $\text{char}(\mathbb{Z}_p)$ must be 0.

(c) We prove that φ is injective. We assume $\varphi((a_n)_{n=1}^{\infty}) = \varphi((b_n)_{n=1}^{\infty}) = (r_n)_{n=1}^{\infty}$ for $(r_n)_{n=1}^{\infty} \in \mathbb{Z}_p$ and $(a_n)_{n=1}^{\infty}, (b_n)_{n=1}^{\infty} \in S^{\mathbb{N}}$.

We prove by induction that $a_n = b_n$ for all $n \in \mathbb{N}$. For $n = 1$, we note that $[a_1]_p = [b_1]_p$, so $a_1 - b_1 \equiv 0 \pmod{p}$. However, $a_1, b_1 \in S$, so $-(p-1) \leq a_1 - b_1 \leq p - 1$. The only option for $p \mid (a_1 - b_1)$ is that $a_1 - b_1 = 0$ or $a_1 = b_1$. Let $k \in \mathbb{N}$. We assume that the induction hypothesis holds true for all $1 \leq m \leq k$. For $n = k + 1$, we get that:

$$[a_1 + \cdots + a_{k+1}p^k]_{p^{k+1}} = [b_1 + \cdots + b_{k+1}p^k]_{p^{k+1}}$$

or that:

$$(a_1 - b_1) + \cdots + (a_{k+1} - b_{k+1})p^k \equiv 0 \pmod{p^{k+1}}$$

Because of the induction hypothesis that all $1 \leq m \leq k$ has $a_m - b_m = 0$. Thus:

$$(a_{k+1} - b_{k+1})p^k \equiv 0 \pmod{p^{k+1}}$$

This implies that $p \mid (a_{k+1} - b_{k+1})$. It follows from the same reasoning from $n = 1$ that $a_{k+1} - b_{k+1}$ must be equal to 0, thus $a_{k+1} = b_{k+1}$. This proves that $(a_n)_{n=1}^{\infty} = (b_n)_{n=1}^{\infty}$ and that φ is injective.

We now prove that $\text{im}(\varphi) = \mathbb{Z}_p$. Let $(r_n)_{n=1}^{\infty} \in \text{im}(\varphi)$. We get that $r_{n+1} = [a_1 + \cdots + a_{n+1}p^n]_{p^{n+1}}$. We then note that:

$$f_n(r_{n+1}) = [a_1 + \cdots + a_n p^{n-1} + a_{n+1}p^n]_{p^n} = [a_1 + \cdots + a_n p^{n-1}]_{p^n} = r_n$$

Thus, we proved that $(r_n)_{n=1}^{\infty} \in \mathbb{Z}_p$, so $\text{im}(\varphi) \subseteq \mathbb{Z}_p$. Meanwhile for $(r_n)_{n=1}^{\infty} \in \mathbb{Z}_p$, we note that for all $n \in \mathbb{N}$, we get that $r_n = [x_n]_{p^n}$ where $0 \leq x_n \leq p^n - 1$. We then denote $a_n = \lfloor x_n / p^{n-1} \rfloor$ and note that $0 \leq a_n \leq p - 1$, so $a_n \in S$. We note that

$$r_n = a_n p^{n-1} + x_n \% p^{n-1}$$

Observe that $f_{n-1}(r_n) = [x_n \% p^{n-1}]_{p^{n-1}} = r_{n-1}$, so we get that $x_n \% p^{n-1} = x_{n-1}$. We repeat the same procedure for r_{n-1} and get that $x_{n-1} = a_{n-1}p^{n-2} + x_{n-2}$. We can repeat this until we reach x_1 where $x_1 = a_1 \cdot p^0 = a_1 = x_2 \% p$. Hence we get that:

$$r_n = [a_n p^{n-1} + a_{n-1}p^{n-2} + \cdots + a_1]_{p^n}$$

Note that for all $1 \leq k \leq n$, $a_k \in S$ by our construction. Hence, there exists a $(a_n)_{n=1}^{\infty} \in S^{\mathbb{N}}$ where $\varphi((a_n)_{n=1}^{\infty}) = (r_n)_{n=1}^{\infty}$. Hence, $(r_n)_{n=1}^{\infty} \in \text{im}(\varphi)$, so $\text{im}(\varphi) \supseteq \mathbb{Z}_p$ and we conclude that $\text{im}(\varphi) = \mathbb{Z}_p$.

(d) **Lemma:** For $(r_n)_{n=1}^{\infty} \in \mathbb{Z}_p$, $(r_n)_{n=1}^{\infty}$ is a unit iff $r_1 \neq 0$.

We assume $r_1 = 0$, so there does not exist an element a in $\mathbb{Z}/p\mathbb{Z}$ where $a \cdot r_1 = 1$ because $a \cdot r_1 = 0$. We note that $1 = (1)_{n=1}^{\infty} \in \mathbb{Z}_p$. Since there does not exist a $(\hat{r}_n)_{n=1}^{\infty} \in \mathbb{Z}_p$ where $r_1 \cdot \hat{r}_1 = 1$, the inverse of $(r_n)_{n=1}^{\infty}$ does not exist, so it is not a unit. Hence, we get that if $(r_n)_{n=1}^{\infty}$ is a unit, then $r_1 \neq 0$.

For the converse, we assume $r_1 \neq 0$. We will construct a $(b_n)_{n=1}^{\infty} \in \mathbb{Z}_p$ where $(r_n)_{n=1}^{\infty} \cdot (b_n)_{n=1}^{\infty} = (1)_{n=1}^{\infty}$ to show that the inverse exists. For b_1, we note that r_1 is non-zero and since $\mathbb{Z}/p\mathbb{Z}$ is a field, we can denote $b_1 = r_1^{-1}$. We then assume for b_n that $b_n \cdot r_n = 1$. For b_{n+1}, we first note that $f_n(r_{n+1}) = r_n$ and $f_n(b_{n+1}) = b_n$. We then note that there exist $r, b \in \mathbb{Z}$ where $0 < r, b < p^n$ and $r_n = [r]_{p^n}$ and $b_n = [b]_{p^n}$. This implies non-negative integers c, d that:

$$\begin{aligned} r_{n+1} &= [cp^n + r]_{p^{n+1}} \\ b_{n+1} &= [dp^n + b]_{p^{n+1}} \end{aligned}$$

Hence, we get that:

$$\begin{aligned} r_{n+1} \cdot b_{n+1} &= [cdp^{2n} + drp^n + cbp^n + rb]_{p^{n+1}} \\ &= [drp^n + cbp^n + rb]_{p^{n+1}} \end{aligned}$$

Since $rb \equiv 1 \pmod{p^n}$, there exists a non-negative integer e where $rb = ep^n + 1$. Hence we now get that:

$$\begin{aligned} r_{n+1} \cdot b_{n+1} &= [drp^n + cbp^n + ep^n + 1]_{p^{n+1}} \\ &= [p^n(dr + cb + e) + 1]_{p^{n+1}} \end{aligned}$$

To achieve the desired $p^n(dr+cb+e)+1 \equiv 1 \pmod{p^{n+1}}$, we need to make $p \mid dr+cb+e$. In other words, we can express this as $[dr + cb + e]_p = [0]_p$ in $\mathbb{Z}/p\mathbb{Z}$. We first note that $[r]_p$ is non-zero because r_1 is non-zero and $r_1 = f_1 \cdots \circ f_{n-1} \circ f_n(r) = [r]_p$, so $[r]_p^{-1}$ exists. Hence, if we denote d as the positive integer where $[d]_p = [r]_p^{-1} \cdot (-[cb + e])$. We get that $([r]_p^{-1} \cdot (-[cb+e]))[r]_p + [cb+e]_p = [0]_p$ as desired. Hence, by denoting $b_{n+1} = [dp^n + b]_{p^{n+1}}$, we get that $b_{n+1} \cdot r_{n+1} = [(dp^n + b)(cp^n + r)]_{p^{n+1}} = [1]_{p^{n+1}}$. We have inductively created $(b_n)_{n=1}^{\infty}$ that serves as the inverse of $(r_n)_{n=1}^{\infty}$, so we proved $(r_n)_{n=1}^{\infty}$ is a unit.

Remark For $(a_n)_{n=1}^{\infty} \in S^{\mathbb{N}}$ where $\varphi((a_n)_{n=1}^{\infty})$ is equal to $(u_n)_{n=1}^{\infty} \in \mathbb{Z}_p$, we note that $[a_1]_p = u_1$. The Lemma implies that $(u_n)_{n=1}^{\infty}$ is a unit iff a_1 is non-zero.

We assume $\nu_p(a) = m$. Let $(a_n)_{n=1}^{\infty} \in S^{\mathbb{N}}$ and $\varphi((a_n)_{n=1}^{\infty}) = a$. By the definition of ν_p, we note that $a_1, \cdots, a_m$ are all equal to 0. Hence, we note that:

$$\sum_{n=1}^{\infty} a_n p^{n-1} = p^m \cdot \sum_{n=m+1}^{\infty} a_n p^{n-m-1}$$

Hence, we denote the series $(a_{n+m})_{n=1}^{\infty}$. Since a_{m+1} is non-zero, which is the first term of the series, we note that $\sum_{n=m+1}^{\infty} a_n p^{n-m-1}$ is a unit from the Remark. Thus, $a = p^m u$ for some unit $u \in \mathbb{Z}_p$.

For the converse, we assume $a = p^m u$ where u is a unit in $\mathbb{Z}_p$. We note that we can express u as

$$u = \sum_{n=1}^{\infty} a_n p^{n-1}$$

where a_1 is non-zero from the Remark since u is a unit. If we multiply p^m, we note that it is equivalent to:

$$p^m u = p^m \cdot \sum_{n=1}^{\infty} a_n p^{n-1} = \sum_{n=1}^{\infty} a_n p^{n+m-1}$$

Hence, we denote a $(b_n)_{n=1}^{\infty} \in S^{\mathbb{N}}$ where for $n \leq m$, we get that $b_n = 0$ and for $n > m$, we get that $b_n = a_{n-m}$. Hence,

$$\sum_{n=1}^{\infty} b_n p^{n-1} = \sum_{n=1}^{m} 0 p^{n-1} + \sum_{n=1}^{\infty} a_n p^{n+m-1} = p^m u$$

Hence, we get that $\nu_p(a) = \nu(p^m u) = \nu_p(\sum_{n=1}^{\infty} b_n p^{n-1}) = m + 1 - 1 = m$ as desired as the first non-zero term is b_{m+1}.

(e) We first prove that $\mathbb{Z}_p$ is an integral domain. Let $a, b \in \mathbb{Z}_p$ and both are non-zero. We denote $m = \nu_p(a)$ and $n = \nu_p(b)$. We also get that there exist units u, v where $a = p^m u$ and $b = p^n v$. We then express $u = (u_n)_{n=1}^{\infty}$ and $v = (v_n)_{n=1}^{\infty}$. Since $u_1, v_1 \in \mathbb{Z}/p\mathbb{Z}$, from the Lemma, since u and v are units, u_1 and v_1 are non-zero, which implies $u_1 \cdot v_1$ is non-zero because $\mathbb{Z}/p\mathbb{Z}$ is a field (thus an integral domain). By the Lemma again, this further implies that uv is a unit. Thus, we have that $ab = p^{m+n}(uv)$, and it follows that $\nu_p(ab) = m + n$. We then denote $(d_n)_{n=1}^{\infty} \in S^{\mathbb{N}}$ where $\varphi((d_n)_{n=1}^{\infty}) = ab$ and we get that d_{m+n+1} is non-zero. Hence, $(d_n)_{n=1}^{\infty} \neq (0)_{n=1}^{\infty}$, so $ab \neq 0$. This proves that $\mathbb{Z}_p$ is an integral domain.

We can now prove that it is a Euclidean domain. We first denote ν_p as the $N(x)$ tied to $\mathbb{Z}_p$. Let $a, b \in \mathbb{Z}_p$ where $a \neq 0$. We consider the cases as follows with $q, r \in \mathbb{Z}_p$ for the form $b = aq + r$:

Case 1: If $b = 0$, then it follows that $q = 0$ and $r = 0$ where $0 = a0 + 0 = 0$.

For the remaining cases, we assume $b \neq 0$. Thus, we can denote $\nu_p(b) = m$ and $\nu_p(a) = n$ and that $b = p^m u$ and $a = p^n v$ with u, v being units in $\mathbb{Z}_p$.

Case 2: If $m > n$, then it follows that $r = 0$ and $q = p^{m-n}(v^{-1}u)$. Thus, $b = (p^n v)(p^{m-n}(v^{-1}u)) = p^m u = b$. (Take notice that we had earlier shown with the integral domain proof that the multiplication between two arbitrary units in $\mathbb{Z}_p$ is still a unit, so $v^{-1}u$ is a unit.)

Case 3: If $m = n$, then it follows that $r = 0$ and $q = (v^{-1}u)$. Thus, $b = (p^n v)((v^{-1}u)) = p^m u = b$.

Case 4: If $m < n$, then it follows that $r = p^m u$ and $q = 0$. Thus, $b = (p^n v)0 + p^m u = p^m u = b$. Since $\nu_p(r) = m$, we get that $\nu_p(r) < \nu_p(a)$.

We showed that in all cases, it is either $r = 0$ or $\nu_p(r) < \nu_p(a)$. This proves that $\mathbb{Z}_p$ is a Euclidean domain.