(c) Solve the simultaneous system of congruences

$$x \equiv 1 \bmod 8\,, \qquad x \equiv 2 \bmod 25\,, \qquad \text{and} \qquad x \equiv 3 \bmod 81$$

and the simultaneous system

$$y \equiv 5 \bmod 8\,, \qquad y \equiv 12 \bmod 25\,, \qquad \text{and} \qquad y \equiv 47 \bmod 81.$$

6. Let $f_1(x), f_2(x), \dots, f_k(x)$ be polynomials with integer coefficients of the same degree d. Let $n_1, n_2, \dots, n_k$ be integers which are relatively prime in pairs (i.e., $(n_i, n_j) = 1$ for all $i \neq j$). Use the Chinese Remainder Theorem to prove there exists a polynomial $f(x)$ with integer coefficients and of degree d with

$$f(x) \equiv f_1(x) \bmod n_1\,, \qquad f(x) \equiv f_2(x) \bmod n_2\,, \qquad \dots, \qquad f(x) \equiv f_k(x) \bmod n_k$$

i.e., the coefficients of $f(x)$ agree with the coefficients of $f_i(x) \bmod n_i$. Show that if all the $f_i(x)$ are monic, then $f(x)$ may also be chosen monic. [Apply the Chinese Remainder Theorem in $\mathbb{Z}$ to each of the coefficients separately.]

7. Let m and n be positive integers with n dividing m. Prove that the natural surjective ring projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is also surjective on the units: $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$.

The next four exercises develop the concept of *direct limits* and the "dual" notion of *inverse limits*. In these exercises I is a nonempty index set with a partial order $\le$ (cf. Appendix I). For each $i \in I$ let A_i be an additive abelian group. In Exercise 8 assume also that I is a *directed set*: for every $i, j \in I$ there is some $k \in I$ with $i \le k$ and $j \le k$.

8. Suppose for every pair of indices i, j with $i \le j$ there is a map $\rho_{ij} : A_i \to A_j$ such that the following hold:
   i. $\rho_{jk} \circ \rho_{ij} = \rho_{ik}$ whenever $i \le j \le k$, and
   ii. $\rho_{ii} = 1$ for all $i \in I$.

   Let B be the disjoint union of all the A_i. Define a relation $\sim$ on B by

   $$a \sim b \text{ if and only if there exists } k \text{ with } i, j \le k \text{ and } \rho_{ik}(a) = \rho_{jk}(b),$$

   for $a \in A_i$ and $b \in A_j$.

   (a) Show that $\sim$ is an equivalence relation on B. (The set of equivalence classes is called the *direct* or *inductive limit* of the directed system $\{A_i\}$, and is denoted $\varinjlim A_i$. In the remaining parts of this exercise let $A = \varinjlim A_i$.)

   (b) Let $\overline{x}$ denote the class of x in A and define $\rho_i : A_i \to A$ by $\rho_i(a) = \overline{a}$. Show that if each ρ_{ij} is injective, then so is ρ_i for all i (so we may then identify each A_i as a subset of A).

   (c) Assume all ρ_{ij} are group homomorphisms. For $a \in A_i, b \in A_j$ show that the operation

   $$\overline{a} + \overline{b} = \overline{\rho_{ik}(a) + \rho_{jk}(b)}$$

   where k is any index with $i, j \le k$, is well defined and makes A into an abelian group. Deduce that the maps ρ_i in (b) are group homomorphisms from A_i to A.

   (d) Show that if all A_i are commutative rings with 1 and all ρ_{ij} are ring homomorphisms that send 1 to 1, then A may likewise be given the structure of a commutative ring with 1 such that all ρ_i are ring homomorphisms.

   (e) Under the hypotheses in (c) prove that the direct limit has the following *universal property*: if C is any abelian group such that for each $i \in I$ there is a homomorphism $\varphi_i : A_i \to C$ with $\varphi_i = \varphi_j \circ \rho_{ij}$ whenever $i \le j$, then there is a unique homomorphism $\varphi : A \to C$ such that $\varphi \circ \rho_i = \varphi_i$ for all i.

9. Let I be the collection of open intervals $U = (a, b)$ on the real line containing a fixed real number p. Order these by reverse inclusion: $U \leq V$ if $V \subseteq U$ (note that I is a directed set). For each U let A_U be the ring of continuous real valued functions on U. For $V \subseteq U$ define the *restriction maps* $\rho_{UV} : A_U \to A_V$ by $f \mapsto f|_V$, the usual restriction of a function on U to a function on the subset V (which is easily seen to be a ring homomorphism). Let $A = \varinjlim A_U$ be the direct limit. In the notation of the preceding exercise, show that the maps $\rho_U : A_U \to A$ are *not* injective but are all surjective (A is called the ring of *germs of continuous functions* at p).

We now develop the notion of *inverse limits.* Continue to assume I is a partially ordered set (but not necessarily directed), and A_i is a group for all $i \in I$.

10. Suppose for every pair of indices i, j with $i \leq j$ there is a map $\mu_{ji} : A_j \to A_i$ such that the following hold:

i. $\mu_{ji} \circ \mu_{kj} = \mu_{ki}$ whenever $i \leq j \leq k$, and
ii. $\mu_{ii} = 1$ for all $i \in I$.

Let P be the subset of elements $(a_i)_{i \in I}$ in the direct product $\prod_{i \in I} A_i$ such that $\mu_{ji}(a_j) = a_i$ whenever $i \leq j$ (here a_i and a_j are the i^{th} and j^{th} components respectively of the element in the direct product). The set P is called the *inverse* or *projective limit* of the system $\{A_i\}$, and is denoted $\varprojlim A_i$.)

(a) Assume all μ_{ji} are group homomorphisms. Show that P is a subgroup of the direct product group (cf. Exercise 15, Section 5.1).

(b) Assume the hypotheses in (a), and let $I = \mathbb{Z}^+$ (usual ordering). For each $i \in I$ let $\mu_i : P \to A_i$ be the projection of P onto its i^{th} component. Show that if each μ_{ji} is surjective, then so is μ_i for all i (so each A_i is a quotient group of P).

(c) Show that if all A_i are commutative rings with 1 and all μ_{ji} are ring homomorphisms that send 1 to 1, then P may likewise be given the structure of a commutative ring with 1 such that all μ_i are ring homomorphisms.

(d) Under the hypotheses in (a) prove that the inverse limit has the following *universal property*: if D is any group such that for each $i \in I$ there is a homomorphism $\pi_i : D \to A_i$ with $\pi_i = \mu_{ji} \circ \pi_j$ whenever $i \leq j$, then there is a unique homomorphism $\pi : D \to P$ such that $\mu_i \circ \pi = \pi_i$ for all i.

11. Let p be a prime let $I = \mathbb{Z}^+$, let $A_i = \mathbb{Z}/p^i\mathbb{Z}$ and let μ_{ji} be the natural projection maps

$$\mu_{ji} : a \ (\text{mod } p^j) \longmapsto a \ (\text{mod } p^i).$$

The inverse limit $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ is called the ring of *p-adic integers*, and is denoted by $\mathbb{Z}_p$.

(a) Show that every element of $\mathbb{Z}_p$ may be written uniquely as an infinite formal sum $b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$ with each $b_i \in \{0, 1, \dots, p-1\}$. Describe the rules for adding and multiplying such formal sums corresponding to addition and multiplication in the ring $\mathbb{Z}_p$. [Write a least residue in each $\mathbb{Z}/p^i\mathbb{Z}$ in its base p expansion and then describe the maps μ_{ji}.] (Note in particular that $\mathbb{Z}_p$ is uncountable.)

(b) Prove that $\mathbb{Z}_p$ is an integral domain that contains a copy of the integers.

(c) Prove that $b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$ as in (a) is a unit in $\mathbb{Z}_p$ if and only if $b_0 \neq 0$.

(d) Prove that $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$ and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ (where $p = 0 + 1p + 0p^2 + 0p^3 + \cdots$). Prove that every nonzero ideal of $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$ for some integer $n \geq 0$.

(e) Show that if $a_1 \not\equiv 0 \pmod p$ then there is an element $a = (a_i)$ in the inverse limit $\mathbb{Z}_p$ satisfying $a_j^{p-1} \equiv 1 \pmod{p^j}$ and $\mu_{j1}(a_j) = a_1$ for all j. Deduce that $\mathbb{Z}_p$ contains $p - 1$ distinct $(p-1)^{\text{st}}$ roots of 1.