

ANSWERS FOR PROBLEM SET VI

Section 12A, page 261.

8. The first two congruences, $x \equiv 5 \pmod{14}$ and $x \equiv 7 \pmod{8}$, reduce to the single congruence $x \equiv 47 \pmod{56}$. Combining that with the third congruence, $x \equiv 13 \pmod{18}$, leads to the single congruence

$$x \equiv 103 \pmod{504}.$$

Section 12D, page 280.

47.

$+$		$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
---	---	---	---	---	---
$(0, 0)$		$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 1)$		$(0, 1)$	$(0, 0)$	$(1, 1)$	$(1, 0)$
$(1, 0)$		$(1, 0)$	$(1, 1)$	$(0, 0)$	$(0, 1)$
$(1, 1)$		$(1, 1)$	$(1, 0)$	$(0, 1)$	$(0, 0)$
\times		$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
---	---	---	---	---	---
$(0, 0)$		$(0, 0)$	$(0, 0)$	$(0, 0)$	$(0, 0)$
$(0, 1)$		$(0, 0)$	$(0, 1)$	$(0, 0)$	$(0, 1)$
$(1, 0)$		$(0, 0)$	$(0, 0)$	$(1, 0)$	$(1, 0)$
$(1, 1)$		$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$

(After making these tables, we can compare them with the tables for \mathbb{Z}_4 . The ring \mathbb{Z}_4 is *not* isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.)

Section 13A, page 287.

2. Evaluating $p(x)$ as a polynomial function on \mathbb{Z}_6 , we find that

$$p(0) = 0, \quad p(1) = 1, \quad p(2) = 2, \quad p(3) = 3, \quad p(4) = 4, \quad p(5) = 5.$$

What luck! We can simply take $q(x) = x$.

Section 13B, page 289.

5. For one direction, assume that p has degree 0. That is, p is a non-zero constant a in the field F . Then the constant polynomial $q(x) = a^{-1}$ is a multiplicative inverse for p , so p is a unit in $F[x]$.

In the other direction, first suppose p has degree $-\infty$. Then $p = 0$, which is not a unit. Secondly, if $\deg p > 0$, then for any non-zero q we have $\deg pq > 0$ (a field has no zero divisors). So $pq \neq 1$. Either way, p is not a unit in $F[x]$.

Section 13D, page 293.

11. Following the suggestion on page 582, we find that $h(x)$, the difference between the polynomials, has the values

$$h(0) = 0, \quad h(1) = 6, \quad h(2) = 510.$$

We want determine those primes p for which this function is constantly 0 on \mathbb{Z}_p .

To get $h(1) \equiv 0 \pmod{p}$, we require $p = 2$ or $p = 3$. And both of those primes do give us the constantly 0 function, because $510 \equiv 0 \pmod{3}$.

We conclude that the given polynomials agree for $p = 2$ and $p = 3$ only.

Section 14A, page 298.

5. The division theorem in this case leads to the equation

$$x^4 + x^3 + x + 4 = (x - 3)(x^3 + 4x^2 + 12x + 37) + 115$$

and of course this decomposition is unique.

(i) No, $x - 3$ does not divide $x^4 + x^3 + x + 4$ in those rings.

(ii) If $m = 5$, $m = 23$, or $m = 115$, then $x - 3$ does divide $x^4 + x^3 + x + 4$ in \mathbb{Z}_m . The first two values of m give us fields.

(It is also possible to apply the Root Theorem, which does not really require that F be a field.)

7. We are given

$$f = (x^2 - 3)(x + 1)q + (x^2 + 2x + 5)$$

for some quotient polynomial q . This equation can be converted to

$$f = (x^2 - 3)(x + 1)q + (x^2 - 3) + (2x + 8)$$

which shows that the remainder under division by $x^2 - 3$ is $2x + 8$

8. When we evaluate that polynomial p at k , we find that $p(k) = -k + 3$. So by the Root Theorem, we conclude that $x - k$ divides p iff $k = 3$.