

1. Suggestion: Easy ways are easier than hard ways.

- 8 (a) How many units does the ring \mathbb{Z}_{99} have? (Support your answer.)
 68 (b) Evaluate $6^{68} \pmod{67}$.
 6 (c) Evaluate $5^{62} \pmod{99}$.

$$(a) \quad \varphi(99) = \varphi(9) \cdot \varphi(11).$$

$$\varphi(9) = 9 - 3 = 6$$

$$\varphi(11) = 10$$

$$\text{So } \varphi(99) = \boxed{60}.$$

(b) 67 is prime, $6 \not\equiv 0 \pmod{67}$.

So by Fermat's theorem, $6^{66} \equiv 1 \pmod{67}$.

$$\therefore 6^{68} \equiv \boxed{36} \pmod{67}.$$

(c) $(5, 99) = 1$ and $\varphi(99) = 60$.

By Euler's theorem,

$$5^{60} \equiv 1 \pmod{99}.$$

$$\therefore 5^{62} \equiv \boxed{25} \pmod{99}.$$

2. For each system of congruences, either find the general solution (which may be expressed by a single congruence), or explain why there is no solution.

7 (a) $x \equiv 8 \pmod{11}$ and $x \equiv 2 \pmod{12}$

7 (b) $x \equiv 8 \pmod{10}$ and $x \equiv 2 \pmod{12}$

6 (c) $x \equiv 9 \pmod{10}$ and $x \equiv 2 \pmod{12}$

(a) $x \equiv 74 \pmod{132}$

One way to obtain this:

$$(1)(12) + (-1)(11) = 1$$

$$6(12) + (-6)(11) = 8 - 2$$

$$2 + 6(12) = 8 + 6(11) = 74.$$

(b) $x \equiv 38 \pmod{60}$

One way to obtain this:

$$(1)(12) + (-1)(10) = 2$$

$$(3)(12) + (-3)(10) = 8 - 2$$

$$2 + 3(12) = 8 + 3(10) = 38.$$

(c) No solution

because $(10, 12) = 2$ and
2 does not divide $9 - 2$.

- 5 3. (a) How many polynomials of degree four are there in $\mathbb{Z}_3[x]$?
- 5 (b) Exhibit a cubic (i.e., degree-3) polynomial in $\mathbb{Z}_3[x]$ for which the corresponding polynomial function is constantly zero on \mathbb{Z}_3 .
- 5 (c) Explain why there is no quadratic (i.e., degree-2) polynomial in $\mathbb{Z}_3[x]$ for which the corresponding polynomial function is constantly zero on \mathbb{Z}_3 .
- 5 (d) Define the function $h : \mathbb{Z}_3[x] \rightarrow \mathbb{Z}_3[x]$ by the equation $h(p) = p^3$. (So for example, $h(x^2) = x^6$.) Show that h is a homomorphism and that it is one-to-one.

(a) We want $a + bx + cx^2 + dx^3 + ex^4$
with $e \neq 0$.

$$3^4 \times 2 = 81 \times 2 = \textcircled{162}.$$

The point: We are counting strings of coefficients from \mathbb{Z}_3 .

(b) $x(x-1)(x-2) = x(x^2+2) = \textcircled{x^3 + 2x}$.
Another solution is $2x^3 + x$.

(c) By D'Alembert's theorem, a quadratic has at most two roots in the field \mathbb{Z}_3 .

(d) $h(0) = 0$, $h(1) = 1$.

$$h(pq) = (pq)^3 = p^3 q^3 = h(p)h(q)$$

$$\begin{aligned} h(p+q) &= (p+q)^3 = p^3 + 3p^2q + 3pq^2 + q^3 \\ &= p^3 + q^3 = h(p) + h(q). \end{aligned}$$

One-to-one: $\deg h(p) = 3 \deg p$.

So if $h(p) = 0$ then $p = 0$. $\ker h = \{0\}$.

Note: h is not onto $\mathbb{Z}_3[x]$.

- 10 4. (a) Assume that $h : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ is a homomorphism (between rings with identity, so that $h(1) = 1$). Explain why $h(x) = x$ for all x in \mathbb{Z}_4 .
- 10 (b) In the ring $\mathbb{Z}_4[x]$, find a polynomial of degree 1 that is a unit. Suggestion: Seek an inverse that also has degree 1.

(a) $h(0) = 0$, $h(1) = 1$
 for a homomorphism between rings with identity.
 Halfway done.
 $h(2) = h(1+1) = h(1) + h(1) = 1+1 = 2$.
 $h(3) = 3$ similarly.

Note: \mathbb{Z}_4 could have been \mathbb{Z}_m . The ring \mathbb{Z}_m is "rigid"; that is, it has no non-trivial automorphisms.

(b) $(a + bx)(c + dx) = ac + (b+d)x + bd x^2$.
 We need $bd = 0$, so we must take $b = d = 2$.
 We need $b + d = 0$, which it is.
 We need $ac = 1$, so either $a = c = 1$
 or $a = c = 3$. We get two units of
 degree 1:

$$(2x + 1), (2x + 3)$$

(This can't happen in $F[x]$ for a field F .)

5. Assume that $h : F[x] \rightarrow R$ is a homomorphism from $F[x]$ (where F is a field) to a ring R . Suppose that the kernel of h contains more than 0, and that we take p to be a nonzero member of the kernel with least possible degree. Let M_p be the set of multiples of p , that is, $M_p = \{pq \mid q \in F[x]\}$. Show that the kernel equals the set M_p . Suggestion: Do both inclusions. One way to show that something is a multiple of p is to divide it by p and then look at the remainder.

$$8 \quad \underline{M_p \subseteq \ker h}$$

$$h(pq) = h(p)h(q) = 0 \cdot h(q) = 0.$$

$$\therefore pq \in \ker h.$$

$$12 \quad \underline{\ker h \subseteq M_p}$$

Suppose $g \in \ker h$, so $h(g) = 0$.

Write $g = pq + r$, where $\deg r < \deg p$.

Then $r \in \ker h$ (apply h to the above equation). $\therefore r = 0$ by the leastness of

$\deg p$. $\therefore g \in M_p$.

Remark: This shows that in $F[x]$ (for a field F), every ideal is a "principal ideal" generated by a single element p .