1. Find a pair of integers \(x, y\) so that \(44x + 404y = 20\).

Solution: Using the Euclidean algorithm, we get \(gcd(44, 404) = 4\) and \((46)44 + (-5)404 = 4\) so \(x = 230, y = -25\) is one solution.

2. Determine the least nonnegative integer congruent to \(5^{113}\) modulo 7. Show your work.

Solution: Since \(5^2 \equiv 4 \pmod{7}\) and \(5^3 \equiv 4 \cdot 5 \equiv -1 \pmod{7}\), we have \(5^6 \equiv 1 \pmod{7}\).

Since \(113 = 18 \cdot 6 + 5\), \(5^{113} = (5^6)^{18} \cdot 5^5 \equiv 5^5 \equiv -4 \equiv 3 \pmod{7}\).

3. Solve, if possible, each of the following. If not possible, state why.

(a) Find an integer \(a\) so that \([a]_7 \cdot [3]_7 = [4]_7\).

Solution: Since \(gcd(3, 7) = 1\) and \((-2)3 + (1)7 = 1, (-8)3 + (4)7 = 4\), so \(a = -8\) is a solution, as are \(a = -1\) and \(a = 6\).

(b) Find an integer \(b\) so that \([8]_{24} \cdot [b]_{24} = [7]_{24}\).

Solution: Since \(gcd(8, 24) = 8 \nmid 7\), there is no solution.

(c) Find an integer \(c\) so that \([c]_{27} \cdot [6]_{27} = [9]_{27}\).

Solution: Here \(gcd(6, 27) = 3\) and by Bézout \((-4)6 + (1)27 = 3\), so \((-12)6 + (3)27 = 9\). Hence \(c = -12\) and \(c = 15\) are solutions.

4. For which integers \(m \geq 2\) is it true that

(a) \(3^5 \equiv 5^3 \pmod{m}\)?

Solution: \(3^5 - 5^3 = 243 - 125 = 118 = 2 \cdot 59\) (both prime) so \(m = 2, 59\) or 118.

(b) \([2]^{-1}_m = [13]_m\) in \(\mathbb{Z}/m\mathbb{Z}\)?

Solution: This happens whenever \(2 \cdot 13 \equiv 1 \pmod{m}\), i.e., when \(m \mid 26 - 1 = 25\).

So \(m = 5\) or \(m = 25\).

5. Show that \(24 \mid n(n + 1)(n + 2)\) for any even integer \(n\).

Solution: Since \(n\) is even, we have \(n, n + 2\) congruent to 0 and 2 modulo 4, in some order. Thus 4 divides one of them and 2 divides the other, and so 8 divides \(n(n + 2)\).

On the other hand, modulo 3, \(n, n + 1, n + 2\) are congruent to 0, 1, 2 in some order. Thus 3 divides one of these. Thus 24 divides their product.
6. Show that if $F$ is any field of characteristic 2, then

(a) for any $a \in F$, $-a = a$; and

Solution: In $F$, $1 + 1 = 0$ so $a + a = a(1 + 1) = 0$, so $a = -a$.

(b) for any $a, b \in F$, $(a + b)^2 = a^2 + b^2$.

Solution: $(a + b)^2 = a^2 + ab + ba + b^2 = a^2 + b^2$

(c) Show that the function $f : F \to F$ defined by $f(x) = x^2$ is a ring homomorphism.

Solution: $f(1) = 1^2 = 1$, $f(ab) = (ab)^2 = a^2b^2 = f(a)f(b)$, $f(a + b) = (a + b)^2 = a^2 + b^2 = f(a) + f(b)$

(d) Is $f$ from the previous part one-to-one? Why or why not?

Solution: Yes, since $F$ has no zero divisors, $a \neq 0 \Rightarrow a^2 \neq 0$, so $f(a) \neq 0$. 