p.50 E5 Let \(2\mathbb{N}\) denote the even integers \(> 0\). Say that a number \(a\) in \(2\mathbb{N}\) is irreducible if there are no numbers \(b, c \in 2\mathbb{N}\) so that \(a = b \cdot c\).

i. Show that if \(n\) is an odd number, then \(2n \in 2\mathbb{N}\) and is irreducible; conversely, every irreducible number in \(2\mathbb{N}\) is twice an odd number.

ii. Show that every number \(a \in 2\mathbb{N}\) factors into a product of irreducible numbers in \(2\mathbb{N}\).

iii. Show that factorization of numbers in \(2\mathbb{N}\) into products of irreducibles in \(2\mathbb{N}\) is not unique.

iv. Show that the analogue of Lemma 2 fails in \(2\mathbb{N}\).

Solution:

i. Obviously, \(2n \in 2\mathbb{N}\). Suppose that \(2n = a \cdot b\), where \(a, b \in 2\mathbb{N}\), say \(a = 2a_1, b = 2b_1\). Then \(2n = ab = 2a_12b_1 = 2(2a_1b_1)\) which means \(n = 2a_1b_1\) so \(n\) is even, a contradiction. Thus, no such factorization exists and \(2n\) is irreducible.

Suppose conversely that \(n\) is even. Then \(n = 2n_1\) for some integer \(n_1\), so \(2n = 2(2n_1)\) and \(2, 2n_1 \in 2\mathbb{N}\). Hence, since we can factor \(2n\) in \(2\mathbb{N}\), it is not irreducible.

ii. Let \(n \in 2\mathbb{N}\). Then \(n = 2^rm\) where \(m\) is an odd number. Hence \(n = 2 \cdot 2 \cdots 2 \cdot 2m\) is a factorization of \(n\) into a product of the irreducibles \(2\) and \(2m\).

iii. Consider the number \(300 = 4 \cdot 3 \cdot 5^2\). It can be factored as \(300 = 6 \cdot 50\) (note that both 6 and 50 are irreducible) or as \(300 = 30 \cdot 10\) (30 and 10 are both irreducible).

iv. The analogue of Lemma 2 would be: If \(p, a, b \in 2\mathbb{N}\), \(p\) is irreducible, and \(p\) divides \(ab\), then \(p\) divides \(a\) or \(p\) divides \(b\). This is false. Let \(p = 30, a = 10, b = 6\). Thirty is irreducible and divides \(ab = 60\) but it does not divide either 10 or 6.

p.65 E7 Show that if \(n > 4\) is not prime, then \((n-1)! \equiv 0 \pmod{n}\).

Solution:

First of all, note that if \(m < n-1\) then \(m|(n-1)!\) since \((n-1)! = (m-1)!((m)(m+1)) \cdots (n-1)\). Now, if \(n > 4\) and \(n\) is not prime, then \(n = a \cdot b\) where \(a, b < n\). If \(a < b\), then \((n-1)! = (a-1)!(a)(a+1) \cdots (b-1)(b)(b+1) \cdots (n-1)\) so, as \(a\) and \(b\) both appear in this factorization, \(n = ab\)\((n-1)!\). If \(a = b\) (i.e. \(n = a^2\)), then, since \(n > 4\), \(a \neq a(a-1) < a^2 - 1 = n - 1\). Hence \((n-1)! = (a-1)!(a)(a+1) \cdots (a(a-1))(a(a-1)+1) \cdots (n-1)\). Since both \(a\) and \(a(a-1)\) appear in this factorization, \(n = a^2|(n-1)!\).

P 65 E8 Prove: If \(x \equiv y \pmod{m}\) then \((x, m) = (y, m)\).

Suppose \(x \equiv y \pmod{m}\). Then \(x = y + rm\) for some \(r \in \mathbb{Z}\). Let \(d = (x, m)\). Then there exist \(s, t \in \mathbb{Z}\) such that \(xs + mt = d\). But then \((y + rm)s + mt = d\), that is, \(ys + (r + t)m = d\). Hence, by Proposition 4, \((y, m)|d\). However, we also know that \(y = x + (-r)m\), so by a similar argument, we know that \(d|(y, m)\). Hence \((y, m) = d = (x, m)\).
p67 E6 Find the least nonnegative residue of:

i. $5^{18} \pmod{7}$;

ii. $6^{105} \pmod{13}$; and

iii. $6^{47} \pmod{12}$.

Solution:

i. $5^{18} \equiv (-2)^{18} \equiv ((-1)^32^3)^6 \equiv (-1)^6 \equiv 1 \pmod{7}$

ii. $6^{105} \equiv 3^{105} \equiv (3^3)^{35} \equiv 1^{35} \equiv 1 \pmod{13}$

iii. $6^{47} = 6^26^{45} \equiv 0 \cdot 6^{45} \equiv 0 \pmod{12}$.

p 67 E8 Show that $5^e + 6^e \equiv 0 \pmod{11}$ for all odd numbers $e$.

Solution:

$5^e + 6^e \equiv 5^e + (-5)^e \equiv 5^e + (-1)^e5^e \equiv 5^e - 5^e$ (since $e$ is odd) $\equiv 0 \pmod{11}$.

p 89 E6 In $\mathbb{Z}/11\mathbb{Z}$, solve:


Solution:


p 89 E7 In $\mathbb{Z}/10\mathbb{Z}$, solve:

(a) $[367]X = [15]$;

(b) $[43]X = [34]$;

Solution:
