Assignment #10 Solutions

Page 307, 35.1  Calculate:

(a) \( \gcd(20, 25) \)

(c) \( \gcd(123, -123) \)

(e) \( \gcd(54321, 50) \).

(a) Use Euclid’s algorithm: \( \gcd(20, 25) = \gcd(20, 5) = 5 \).

(c) Clearly 123 is a common divisor and there cannot be any larger common divisor, so \( \gcd(123, -123) = 123 \).

(e) Use Euclid’s algorithm: \( \gcd(54321, 50) = \gcd(50, 21) = \gcd(21, 8) = \gcd(8, 5) = \gcd(5, 3) = \gcd(3, 2) = \gcd(2, 1) = 1 \).

Page 307, 35.2  For each pair of integers \( a, b \) in the previous problem, find integers \( x \) and \( y \) such that \( ax + by = \gcd(a, b) \).

(a) Use the extended form of Euclid’s algorithm shown on p. 306 of your text:

\[
\begin{align*}
25 & = 1 \times 20 + 5 \\
20 & = 4 \times 5 + 0, \text{ so} \\
5 & = 1 \times 25 - 1 \times 20.
\end{align*}
\]

(c) Clearly \( 123 = 1 \times 123 + 0 \times (-123) \).

(e) Using the method of (a), we find

\[
\begin{align*}
54321 & = 1086 \times 50 + 21 \\
50 & = 2 \times 21 + 8 \\
21 & = 2 \times 8 + 5 \\
8 & = 1 \times 5 + 3 \\
5 & = 1 \times 3 + 2 \\
3 & = 1 \times 2 + 1, \text{ so} \\
1 & = 3 - 1 \times 2 \\
& = 3 - 1 \times (5 - 1 \times 3) \\
& = 2 \times 3 - 1 \times 5 \\
& = 2 \times (8 - 1 \times 5) - 1 \times 5 \\
& = 2 \times 8 - 3 \times 5 \\
& = 2 \times 8 - 3 \times (21 - 2 \times 8) \\
& = -3 \times 21 + 8 \times 8 \\
& = -3 \times 21 + 8 \times (50 - 2 \times 21) \\
& = 8 \times 50 - 19 \times 21 \\
& = 8 \times 50 - 19 \times (54321 - 1086 \times 50) \\
& = -19 \times 54321 + 20642 \times 50.
\end{align*}
\]
Consecutive integers must be relatively prime.

Use Euclid’s algorithm. For any integer $n$, $\gcd(n + 1, n) = \gcd(n, 1) = 1$, so $n$ and $n + 1$ are relatively prime.

Let $a$ be an integer. Prove that $2a + 1$ and $4a^2 + 1$ are relatively prime.

Note $(2a + 1)(2a - 1) = 4a^2 - 1$, $2a + 1$ is odd, and $2$ is even, so Euclid’s algorithm gives $\gcd(4a^2 + 1, 2a + 1) = \gcd(2a + 1, 2) = \gcd(2, 1) = 1$.

Suppose $a, b, n \in \mathbb{Z}$ with $n > 0$. Suppose that $ab \equiv 1 \pmod{n}$. Prove that both $a$ and $b$ are relatively prime to $n$.

Note that we can write $ab = \ell \times n + 1$ for some $\ell \in \mathbb{Z}$. This may be rewritten as $a \times b - n \times \ell = 1$ and as $b \times a - n \times \ell = 1$, which shows that $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ by Corollary 35.9.

Suppose $a, n \in \mathbb{Z}$ with $n > 0$. Suppose that $a$ and $n$ are relatively prime. Prove that there is an integer $b$ such that $ab \equiv 1 \pmod{n}$.

Since $a$ and $n$ are relatively prime, we can find integers $x$ and $y$ such that $ax + ny = 1$. Then $b = x$ satisfies $ab \equiv 1 \pmod{n}$.

Solve the following equations for $x$ in the $\mathbb{Z}_n$ specified.

(a) $3 \otimes x = 4$ in $\mathbb{Z}_{11}$.
(b) $4 \otimes x \oplus 8 = 9$ in $\mathbb{Z}_{11}$.
(c) $3 \otimes x \oplus 8 = 1$ in $\mathbb{Z}_{10}$.
(d) $342 \otimes x \oplus 448 = 73$ in $\mathbb{Z}_{1003}$.

(a) The extended Euclid’s algorithm (or guess-and-check) gives $3^{-1} = 4$, since $3 \times 4 - 11 \times 1 = 1$, so $x = 4 \otimes 4 = 5$.
(b) Add $8$ to both sides: $4 \otimes x = 6$. From (a), $4^{-1} = 3$, so $x = 6 \otimes 3 = 7$.
(c) Subtract $8$ from both sides: $3 \otimes x = 3$. The extended Euclid’s algorithm (or guess-and-check) gives $3^{-1} = 7$, since $3 \times 7 - 10 \times 2 = 1$, so $x = 1$. (Or, guess-and-check immediately suggests $x = 1$.)
(d) Subtract $448$ from both sides: $342 \otimes x = 628$. The extended Euclid’s algorithm gives $342^{-1} = 349$, since $342 \times 349 - 1003 \times 119 = 1$, so $x = 628 \otimes 349 = 518$. 
Prove Proposition 36.4. Why is this proposition restricted to \( n \geq 2 \)?

Let \( a, b, c \in \mathbb{Z}_n \). Then:

(i) \( a \oplus b = (a + b) \mod n = b \oplus a \) and \( a \odot b = (ab) \mod n = (ba) \mod n = b \odot a \).

(ii) \( a \oplus (b \oplus c) = (a + (b + c)) \mod n = ((a + b) + c) \mod n = (a \oplus b) \oplus c \) and \( a \odot (b \odot c) = (a(bc)) \mod n = (ab)c \mod n = (a \odot b) \odot c \).

(iii) \( a \oplus 0 = (a + 0) \mod n = a \mod n = a \), \( a \odot 1 = (a \times 1) \mod n = a \mod n = a \), and \( a \odot 0 = (a \times 0) \mod n = 0 \mod n = 0 \).

(iv) \( a \odot (b \oplus c) = (a(b + c)) \mod n = (ab + ac) \mod n = a \odot b \oplus a \odot c \).

We require \( n \geq 2 \) so that \( 1 \in \mathbb{Z}_n \).

Let \( n \) be a positive integer and suppose \( a, b \in \mathbb{Z}_n \) are both invertible. Prove or disprove each of the following statements:

(a) \( a \oplus b \) is invertible.

(b) \( a \oplus b \) is invertible.

(c) \( a \odot b \) is invertible.

(d) \( a \odot b \) is invertible.

(a) Counterexample: 1 and \( n - 1 \) are invertible (we know \( n - 1 \) is invertible since consecutive integers are relatively prime, or see the next problem), but \( 1 \oplus (n - 1) = 0 \) is not invertible.

(b) Counterexample: 1 is invertible, but \( 1 \odot 1 = 0 \) is not invertible.

(c) Proof: \( (a \odot b) \odot (b^{-1} \odot a^{-1}) = 1 \), so \( a \odot b \) is invertible (and, in fact, its inverse is \( b^{-1} \odot a^{-1} \)).

(d) Proof: Rewrite \( a \odot b = a \odot b^{-1} \). Since \( a \) and \( b^{-1} \) are both invertible, the result follows from (c).

Let \( n \) be an integer with \( n \geq 2 \). Prove that in \( \mathbb{Z}_n \), the element \( n - 1 \) is its own inverse.

Note \( (n - 1) \odot (n - 1) = (n - 1)(n - 1) \mod n = n^2 - 2n + 1 \mod n = n(n - 2) + 1 \mod n = 1 \).