Assignment #10 Solutions

$\boxed{\text{Page 307, 35.1}}$ *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: $\gcd(54321, 50) = \gcd(50, 21) = \gcd(21, 8) = \gcd(8, 5) = \gcd(5, 3) = \gcd(3, 2) = \gcd(2, 1) = 1$.

$\boxed{\text{Page 307, 35.2}}$ *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:

$$\begin{aligned}
25 &= 1 \times 20 + 5 \\
20 &= 4 \times 5 + 0, \text{ so} \\
5 &= 1 \times 25 - 1 \times 20.
\end{aligned}$$

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

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

$$\begin{aligned}
54321 &= 1086 \times 50 + 21 \\
50 &= 2 \times 21 + 8 \\
21 &= 2 \times 8 + 5 \\
8 &= 1 \times 5 + 3 \\
5 &= 1 \times 3 + 2 \\
3 &= 1 \times 2 + 1, \text{ so} \\
1 &= 3 - 1 \times 2 \\
&= 3 - 1 \times (5 - 1 \times 3) \\
&= 2 \times 3 - 1 \times 5 \\
&= 2 \times (8 - 1 \times 5) - 1 \times 5 \\
&= 2 \times 8 - 3 \times 5 \\
&= 2 \times 8 - 3 \times (21 - 2 \times 8) \\
&= -3 \times 21 + 8 \times 8 \\
&= -3 \times 21 + 8 \times (50 - 2 \times 21) \\
&= 8 \times 50 - 19 \times 21 \\
&= 8 \times 50 - 19 \times (54321 - 1086 \times 50) \\
&= -19 \times 54321 + 20642 \times 50.
\end{aligned}$$

$\boxed{\text{Page 308, 35.10}}$ *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.

$\boxed{\text{Page 308, 35.11}}$ *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 $\gcd(4a^2+1, 2a+1) = \gcd(2a+1, 2) = \gcd(2, 1) = 1$.

$\boxed{\text{Page 308, 35.14}}$ *Suppose $a, b, n \in \mathbb{Z}$ with $n > 0$. Suppose that $ab \equiv 1 (\text{mod } n)$. 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.

$\boxed{\text{Page 308, 35.15}}$ *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 $ab \equiv 1 (\text{mod } n)$.*

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

$\boxed{\text{Page 319, 36.2}}$ *Solve the following equations for x in the $\mathbb{Z}_n$ specified.*

(a) $3 \otimes x = 4$ *in* $\mathbb{Z}_{11}$.

(b) $4 \otimes x \ominus 8 = 9$ *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 $x = 628 \otimes 349 = 518$.

$\boxed{\text{Page 319, 36.8}}$ *Prove Proposition 36.4. Why is this proposition restricted to $n \geq 2$?*

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

(i) $a \oplus b = (a+b) \bmod n = (b+a) \bmod n = b \oplus a$ and $a \otimes b = (ab) \bmod n = (ba) \bmod n = b \otimes a$.

(ii) $a \oplus (b \oplus c) = (a + (b + c)) \bmod n = ((a + b) + c) \bmod n = (a \oplus b) \oplus c$ and $a \otimes (b \otimes c) = (a(bc)) \bmod n = ((ab)c) \bmod n = (a \otimes b) \otimes c$.

(iii) $a \oplus 0 = (a + 0) \bmod n = a \bmod n = a$, $a \otimes 1 = (a \times 1) \bmod n = a \bmod n = a$, and $a \otimes 0 = (a \times 0) \bmod n = 0 \bmod n = 0$.

(iv) $a \otimes (b \oplus c) = (a(b + c)) \bmod n = (ab + ac) \bmod n = a \otimes b \oplus a \otimes c$.

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

$\boxed{\text{Page 320, 36.12}}$ *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) $a \ominus b$ is invertible.

(c) $a \otimes b$ is invertible.

(d) $a \oslash b$ 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 $1 \ominus 1 = 0$ is not invertible.

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

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

$\boxed{\text{Page 320, 36.13}}$ *Let n be an integer with $n \geq 2$. Prove that in $\mathbb{Z}_n$, the element $n - 1$ is its own inverse.*

Note $(n - 1) \otimes (n - 1) = (n - 1)(n - 1) \bmod n = n^2 - 2n + 1 \bmod n = n(n - 2) + 1 \bmod n = 1$.