Answer to 2.5-12: We have $2x \equiv 7 \pmod{17}$. Since 2 and 17 are relatively prime, 2 is guaranteed to have a unique inverse, mod 17 (Theorem 3, p. 140, Rosen). Write 1 as a linear combination of 2 and 17: $1 = -8 \cdot 2 + 17$. So -8 is the inverse of 2 (mod 17). So let's multiply the linear congruence by -8:

$$-8 \cdot 2x \equiv -8 \cdot 7 \pmod{17} \quad \Rightarrow \quad x \equiv -56 \equiv 12 \pmod{17}$$

This shows that *if* x is a solution of $2x \equiv 7 \pmod{17}$, then it must obey $x \equiv 12 \pmod{17}$. But this does not prove that *all* x satisfying $x \equiv 12 \pmod{17}$ are solutions to the original linear congruence. To do this, we substitute $x \equiv 12 \pmod{17}$ into the linear congruence and check if it results in a true statment:

$$2 \cdot x \equiv 2 \cdot 12 = 24 \equiv 7 \pmod{17}$$

It's true. So now we know that $2x \equiv 7 \pmod{17}$ if and only if $x \equiv 12 \pmod{17}$. □

Answer to 2.5-26: Refer to p. 142, Rosen, for the meaning of the various symbols. We have:

$$\begin{aligned} a &\equiv a_1 \bmod 4 \\ a &\equiv a_2 \bmod 7 \end{aligned}$$

In part (d), $a_1 = 2$ and $a_2 = 1$; and in part (h), $a_1 = 3$ and $a_2 = 5$. We'll plug these values in later. For now, let's find the y, M, and m values. First, $m = 4 \cdot 7 = 28$. Also, $M_1 = m/4 = 7$ and $M_2 = m/7 = 4$. Now we must find the inverses. You can show that the inverse of M_1 is 3 (mod 4) and the inverse of M_2 is 2 (mod 7). So $y_1 = 3$ and $y_2 = 2$. We can now use the formula $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 \pmod{28}$. For part (d) we get $x = 22$, and for part (h) we get $x = 19$.

And indeed these are the right answers, since 22 is 2 (mod 4) and 1 (mod 7); and 19 is 3 (mod 4) and 5 (mod 7). □

Answer to 2.5-36: The procedure is demonstrated in Example 10, p. 147, Rosen. The numerical equivalent of ATTACK is 001919000210 (A=00, T=19, C=02, K=10). Separate the number into blocks of four digits: 0019 1900 0210. Now encrypt each block using (see p. 146, Rosen): $C = M^e \bmod n = M^{13} \bmod 2537$

$$\begin{aligned} 0019^{13} \bmod 2537 &= 19^{2^0+2^2+2^3} \bmod 2537 \\ &= (19 \cdot 19^4 \cdot 19^8) \bmod 2537 \\ &= ((19 \bmod 2537) \cdot (19^4 \bmod 2537) \cdot (19^8 \bmod 2537)) \bmod 2537 \end{aligned}$$

Now let's do a few useful computations on the side:

$$\begin{aligned} 19 \textbf{ mod } 2537 &= 19 \textbf{ mod } 2537 = 19 \\ 19^2 \textbf{ mod } 2537 &= 19^2 \textbf{ mod } 2537 = 361 \\ 19^4 \textbf{ mod } 2537 &= 361^2 \textbf{ mod } 2537 = 934 \\ 19^8 \textbf{ mod } 2537 &= 934^2 \textbf{ mod } 2537 = 2165 \end{aligned}$$

Using these numbers, we can compute:

$$19^{13} \textbf{ mod } 2537 = (19 \cdot 934 \cdot 2165) \textbf{ mod } 2537 = 2299$$

So the encryption of 0019 is 2299. Repeating this procedure for 1900 and 0210, we compute the total encryption: ATTACK = 0019 1900 0210 $\rightarrow$ 2299 1317 2117. □

Answer to 2.6-2a:

$$\begin{aligned} \mathbf{A}+\mathbf{B} &= \begin{bmatrix} 1 & 0 & 4 \\ -1 & 2 & 2 \\ 0 & -2 & -3 \end{bmatrix} + \begin{bmatrix} -1 & 3 & 5 \\ 2 & 2 & -3 \\ 2 & -3 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 3 & 9 \\ 1 & 4 & -1 \\ 2 & -5 & -3 \end{bmatrix} \end{aligned}$$

□

Answer to 2.6-4b:

$$\begin{aligned} \mathbf{A} \cdot \mathbf{B} &= \begin{bmatrix} 1 & -3 & 0 \\ 1 & 2 & 2 \\ 2 & 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 & 2 & 3 \\ -1 & 0 & 3 & -1 \\ -3 & -2 & 0 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 4 & -1 & -7 & 6 \\ -7 & -5 & 8 & 5 \\ 4 & 0 & 7 & 3 \end{bmatrix} \end{aligned}$$

□

Answer to 2.6-18: To show that two matrices are inverses, show that their product is the identity:

$$\begin{bmatrix} 2 & 3 & -1 \\ 1 & 2 & 1 \\ -1 & -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 7 & -8 & 5 \\ -4 & 5 & -3 \\ 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

□

Answer to 2.6-24b: There are two ways to perform the multiplication:

(i) First multiply $\mathbf{A}_1$ by $\mathbf{A}_2$, then multiply the result by $\mathbf{A}_3$

(ii) First multiply $\mathbf{A}_2$ by $\mathbf{A}_3$, then multiply the result by $\mathbf{A}_1$

The number of operations performed when multiplying two matrices of sizes $p \times q$ and $q \times r$ is pqr (count them). So the cost of the two ways are:

(i) $\mathbf{A}_1 \cdot \mathbf{A}_2$ costs 2500 operations. Then $(\mathbf{A}_1 \cdot \mathbf{A}_2) \cdot \mathbf{A}_3$ costs 500 operations. The total is 3000 operations.

(ii) $\mathbf{A}_2 \cdot \mathbf{A}_3$ costs 250 operations. Then $\mathbf{A}_1 \cdot (\mathbf{A}_2 \cdot \mathbf{A}_3)$ costs 50 operations. The total is 300 operations.

We therefore see that (ii) is ten times faster. □

Answer to 2.6-30: Remember that the Boolean product of two matrices is almost the same as the matrix product you learned in your linear algebra class: the only difference is that addition is replaced by logical OR ($\vee$) and multiplication is replaced by logical AND ($\wedge$). So:

$$\begin{aligned}
\mathbf{A} \odot \mathbf{B} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) \vee (0 \wedge 1) \vee (1 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) \\ (0 \wedge 1) \vee (1 \wedge 0) \vee (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) \\ (1 \wedge 0) \vee (1 \wedge 1) \vee (1 \wedge 1) \vee (1 \wedge 0) & (1 \wedge 0) \vee (1 \wedge 1) \vee (1 \wedge 1) \vee (1 \wedge 0) \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}
\end{aligned}$$

□

Answer to 3.1-2:

b) Let p = "It is hotter than 100 degrees today," and let q = "The polution is dangerous." Then the argument is:

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

A look at Table 1, p. 169, Rosen, shows that this is an instance of a **disjunctive syllogism**.

e) Let p = "I work all night on this homework," q = "I can answer all the exercises," and r = "I understand the material." Then the argument is:

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$

A look at Table 1, p. 169, Rosen, shows that this is an instance of a **hypothetical syllogism**.

□

Answer to 3.1-12: The error occured in the statement "Hence, n does not equal $3l$ for some integer l." This statement does not follow from the previous one, and, in fact, baldly states the conclusion. □

Answer to 3.1-18:

Indirect proof Suppose n is odd. Then $n = 2k + 1$ for some integer k. Then we have:

$$\begin{aligned} 3n + 2 &= 3(2k + 1) + 2 \\ &= 2(3k + 2) + 1 \end{aligned}$$

That is, $3n + 2$ equals twice an integer plus one: it is odd. This proves "If n is odd, then $3n + 2$ is odd." It therefore also proves the contrapositive: "If $3n + 2$ is even, then n is even."

Proof by contradiction Suppose $3n + 2$ is even, and suppose (for contradiction) that n is not even. Then, by definition, $3n + 2 = 2k$ and $n = 2i + 1$ for some integers k and i. Substituting, we get

$$\begin{aligned} & 3(2i + 1) = 2k \\ \Rightarrow\ & 6i + 3 = 2k \\ \Rightarrow\ & 3 = 2(k - 3i) \end{aligned}$$

Since k and i are integers, the last equation says that 3 is even, which is nonsense (a contradiction). Hence, if $3n + 2$ is indeed even, then n must be even.

□

Answer to 3.1-54: Suppose we have four integers p, $p + 2$, $p + 4$, $p + 6$. Then not all of them can be prime, for the following reasons. We cannot have $p = 0$ **mod** 3, otherwise p would be divisible by 3 (which is fine only if p is 3 itself). So two cases remain:

Case 1: $p = 1$ **mod** 3. Then $p + 2 = 0$ **mod** 3, which means $p + 2$ is not prime.

Case 2: $p = 2$ **mod** 3. Then $p + 4 = 0$ **mod** 3, which means $p + 4$ is not prime.

So the statement given in problem 3.1-54 is false for $n = 4$. In fact, using the above reasoning, you can show that $\langle 3, 5, 7 \rangle$ is the only sequence of consecutive primes satisfying the statement for $n = 3$.

□