SOLUTION KEY
Produced by: Kyle Dahlin

Problem 0.2. Determine $\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11)$ and $\text{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11)$.

Solution: The greatest common divisor of $2^4 \cdot 3^2 \cdot 5 \cdot 7^2$ and $2 \cdot 3^3 \cdot 7 \cdot 11$ is $2 \cdot 3^2 \cdot 7$. The least common multiple of $2^3 \cdot 3^2 \cdot 5$ and $2 \cdot 3^3 \cdot 7 \cdot 11$ is $2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$. ■

Comment: Since the numbers can be decomposed into their prime factors, for the greatest common divisor we needed only to look at the *lowest* power of each prime factor appearing in both numbers. On the other hand, to find the least common multiple we looked for the *greatest* power of each prime factor appearing in either number.

Problem 0.6. *** Suppose a and b are integers that divide the integer c. If a and b are relatively prime, show that ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

Solution: Suppose that a and b are integers that divide the integer c and that are relatively prime. By the **Corollary** on Page 5, there exist integers s and t such that $as + bt = 1$. Multiplying this equation through by c gives us:

$$acs + bct = c$$

Since a and b divide c, there are integers x and y such that $ax = c$ and $by = c$. Making the appropriate substitutions in the above equation, we obtain:

$$\begin{aligned} a(by)s + b(ax)t &= c \\ ab(ys + xt) &= c \end{aligned}$$

Hence ab divides c.

Example: Let $a = 4$, $b = 6$, and $c = 12$. Then a and b are not relatively prime and divide c, but $ab = 24$ does not divide c. ■

Problem 0.9. *** Let n be a fixed positive integer greater than 1. If $a \bmod n = a'$ and $b \bmod n = b'$ prove that

i. $(a + b) \bmod n = (a' + b') \bmod n$

ii. $(ab) \bmod n = (a'b') \bmod n$

Solution: Since $a \bmod n = a'$ and $b \bmod n = b'$, there exist numbers x and y such that $a = a' + xn$ and $b = b' + yn$. Thus,

$$\begin{aligned} a + b &= a' + xn + b' + yn \\ &= (a' + b') + (x + y)n \end{aligned}$$

So that $(a + b) \bmod n = (a' + b') \bmod n$. Similarly,

$$\begin{aligned} ab &= a'b' + b'xn + a'yn + xyn^2 \\ &= (a'b') + (b'x + a'y + xyn)n \end{aligned}$$

So that $(ab) \bmod n = (a'b') \bmod n$. ■

SOLUTION KEY
Produced by: Kyle Dahlin

Problem 0.12. Show that $5n + 3$ and $7n + 4$ are relatively prime for all n.

Solution: Let n be an integer and let $a = 5n + 3$ and $b = 7n + 4$. Then

$$\begin{aligned} 7a - 5b &= 7(5n + 3) - 5(7n + 4) \\ &= 35n + 21 - 35n - 20 \\ &= 1 \end{aligned}$$

By Theorem 0.2, the greatest common divisor of a and b is the *smallest* positive integer of the form $as + bt$, hence $\gcd(a, b) = 1$. ■

Problem 0.14. Let p, q, and r be primes other than 3. Show that 3 divides $p^2 + q^2 + r^2$.

Solution: We will use the fact that 3 divides $p^2+q^2+r^2$ if and only if $p^2+q^2+r^2 = 0 \bmod 3$. Since none of p, q, or r is equal to 3 and they are each prime, p, q, and r must be congruent to 1 or 2 modulo 3.

According to the result in Problem 0.9, $p^2 + q^2 + r^2 \bmod 3 = p^2 \bmod 3 + q^2 \bmod 3 + r^2 \bmod 3$. We make a table to determine the possible values of $p^2 + q^2 + r^2 \bmod 3$.

$p \bmod 3$	1	1	1	2
$q \bmod 3$	1	1	2	2
$r \bmod 3$	1	2	2	2
$p^2 + q^2 + r^2 \bmod 3$	3 mod 3	6 mod 3	9 mod 3	12 mod 3

Simplifying the bottom row, we see that each entry is equal to 0 modulo 3. Note that there are other possible combinations of values of p, q, and r but that these are symmetric to one of the ones listed above, meaning they may be obtained just by switching the names of p and q or q and r. ■

Problem 0.16. *** Determine $7^{1000} \bmod 6$ and $6^{1001} \bmod 7$.

Solution: We start by evaluating $7^{1000} \bmod 6$. By the result of Problem 0.9, we have that

$$7^{1000} \bmod 6 = \left((7 \bmod 6)^{1000}\right) \bmod 6$$

Since $7 \bmod 6 = 1$, we get $7^{1000} \bmod 6 = 1^{1000} \bmod 6 = 1$.

We proceed similarly in evaluating $6^{1001} \bmod 7$. In this case, since $6^2 \bmod 7 = 1 \bmod 7$, we find that

$$\begin{aligned} 6^{1001} \bmod 7 &= 6(6^2)^{500} \bmod 7 \\ &= (6 \bmod 7)((6^2)^{500} \bmod 7) \\ &= (6 \bmod 7)(1 \bmod 7) \\ &= 6 \bmod 7 \end{aligned}$$

■

SOLUTION KEY
Produced by: Kyle Dahlin

Problem 0.27. For every positive integer n, prove that a set with exactly n elements has exactly 2^n subsets (counting the empty set and the entire set).

Solution: We proceed by applying the First Principle of Mathematical Induction. Let A be a set with $n = 1$ elements. Then the only subsets of A are the empty set, $\emptyset$, and the entire set, A. Hence there are $2 = 2^n$ subsets of A.

Now suppose that the statement is true for the integer n. We wish to show that it is also true for the integer $n + 1$. Let A be a set with $n + 1$ elements. Let x be some element of A and define the set $B = A \setminus \{x\}$, that is, the set obtained by removing x from A. Then B has exactly n elements and so must have 2^n subsets.

Any subset of A has the form C or $C \cup \{x\}$, where C is a subset of B. Since there are 2^n such subsets of B, then A must have $2^n + 2^n = 2(2^n) = 2^{n+1}$ subsets. Hence, by the First Principle of Mathematical Induction, the statement is true. ■

Comment: In some texts, the step described in the first paragraph above is called the **Base Case** and the next step is called the **Induction Step**.

Problem 0.28. Prove that $2^n 3^{2n} - 1$ is always divisible by 17.

Solution: We proceed by applying the First Principle of Mathematical Induction. Let $a_n = 2^n 3^{2n} - 1$. Then $a_1 = 2 \cdot 3^2 - 1 = 17$ is divisible by 17.

Now suppose that a_n is divisible by 17. We will show that a_{n+1} must also be divisible by 17.

$$\begin{aligned} a_{n+1} &= 2^{n+1} 3^{2(n+1)} - 1 \\ &= 2 \cdot 3^2 \cdot 2^n 3^{2n} - 1 \\ &= 18 \cdot 2^n 3^{2n} - 1 \\ &= 18\left(2^n 3^{2n} - 1\right) - 1 + 18 \\ &= 18a_n + 17 \end{aligned}$$

Hence, a_{n+1} is divisible by 17 since a_n is. ■

Problem 0.32. What is the largest bet that cannot be made with chips worth \$7.00 and \$9.00? Verify that your answer is correct with both forms of induction.

Solution: The book works through a very similar question in **Example 12**. I will follow their process closely.

We rephrase the question into the following: what is the largest positive integer, c, that *cannot* be written in the form $a \cdot 7 + b \cdot 9$?

Let's start by writing out integers of the given form to see if we can guess what the answer might be: 7, 9, 14, 16, 18, 21, 23, 25, 27, 28, 30, 32, 34, 35, 36, 37, 39, 41, 42, 43, 44, 45, 46, 48, 49, 50, 51, 52, 53, 54, 55, 56 ...

It looks like the answer might be 47. It remains to prove that this is the *largest* integer not of the form $a \cdot 7 + b \cdot 9$.

Using the First Principle of Mathematical Induction:

SOLUTION KEY
Produced by: Kyle Dahlin

Let S be the set of all integers greater than or equal to 48 of the form $a \cdot 7 + b \cdot 9$, where a and b are non-negative. Then $48 \in S$, so that S is non-empty. Suppose now that some integer $n \in S$ with $n = a \cdot 7 + b \cdot 9$. We must now show that $n + 1 \in S$. Since $n \geq 48$, we cannot have that both $a < 5$ and $b < 3$. If $a \geq 5$, then

$$\begin{aligned} n + 1 &= a \cdot 7 + b \cdot 9 + (-5 \cdot 7 + 4 \cdot 9) \\ &= (a - 5) \cdot 7 + (b + 4) \cdot 9 \end{aligned}$$

so that $n + 1 \in S$. Otherwise, if $b \geq 3$, then

$$\begin{aligned} n + 1 &= a \cdot 7 + b \cdot 9 + (4 \cdot 7 - 3 \cdot 9) \\ &= (a + 4) \cdot 7 + (b - 3) \cdot 9 \end{aligned}$$

and again, $n + 1 \in S$.

Using the Second Principle of Mathematical Induction:

To prove the statement, note that each of the integers 48, 49, 50, 51, 52, 53, and 54 is in S. Now assume that for some integer $n > 54$, S contains all integers k with $48 \leq k < n$. We must show that $n \in S$. Since $n - 7 \in S$, there are nonnegative integers a and b such that $n - 7 = a \cdot 7 + b \cdot 9$. But then $n = (a + 1) \cdot 7 + b \cdot 9$. Thus n is in S. ■

Comment: I drew a large table in my notes in order to create the list of numbers of the form $a \cdot 7 + b \cdot 9$.

Notice how much more difficult it was to use the First Principle of Mathematical Induction, in this case. It's tempting to always use that version but sometimes the Second Principle is much easier to apply.