(3.5 # 44) Show that $\sqrt[3]{5}$ is irrational.

(a) Suppose $\sqrt[3]{5}$ is rational. Then we can write $\sqrt[3]{5} = a/b$ where $(a, b) = 1$ and $b \neq 0$. Then $5 = a^3/b^3$, so $5b^3 = a^3$. Now $5 \mid a^3$, so $5 \mid a$. Then we can write $a = 5k$ for some integer $k$, so $5b^3 = 125k^3$, and hence $5 \mid b^3$, so $5 \mid b$. But this is a contradiction since $(a, b) = 1$. Therefore $\sqrt[3]{5}$ is irrational.

(b) Since $\sqrt[3]{5}$ is not an integer, and it is the root of the polynomial $x^3 - 5$, it is irrational, by Theorem 3.18.

(3.5 # 74) Show that if $p$ is prime and $1 \leq k < p$, then the binomial coefficient $\binom{p}{k}$ is divisible by $p$.

The binomial coefficient
$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{1 \cdot 2 \cdots p}{1 \cdot 2 \cdots k \cdot 1 \cdot 2 \cdots (p-k)}.$$ Since $k < p$, all the factors in the denominator are less than $p$, so they do not cancel the $p$ in the numerator. Therefore, $p$ divides $\binom{p}{k}$.

(3.6 # 16) Show that if $a$ is a positive integer and $a^m + 1$ is an odd prime, then $m = 2^n$ for some positive integer $n$.

Suppose that $a^m + 1$ is an odd prime. If $m = k\ell$ with $\ell > 1$ odd, then we can factor
$$a^m + 1 = (a^k + 1)(a^{k(\ell-1)} - a^{k(\ell-2)} + \cdots - a^{k} + 1).$$ Since $k < m$, $a^{k} + 1 < a^{m} + 1$, and since $a > 0$, $a^{k} + 1 > 1$, so this is a nontrivial factorization, and hence a contradiction. Therefore $m$ must have no odd factors, so it must be of the form $m = 2^n$.

(3.6 # 18) Use the fact that every prime divisor of $F_4 = 2^{2^4} + 1$ is of the form $2^n k + 1$ to verify that $F_4$ is prime.

Any prime factor of $F_4$ must be of the form $64k + 1$, and must be less than or equal to $\lfloor \sqrt[4]{65,337} \rfloor = 256 = 2^8$. Then $64 + 1 = 65$ is not prime, $64 \cdot 2 + 1 = 129$ is not prime, and $64 \cdot 3 + 1 = 193 \nmid F_4$. The next possible factor $64 \cdot 4 + 1 = 2^8 + 1$ is too big, so $F_4$ is prime.
(4.1 # 12) Construct a table for addition modulo 6.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

(4.1 # 14) Construct a table for multiplication modulo 6.

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

(4.1 # 20) Show that if $n$ is an odd positive integer or if $n$ is a positive integer divisible by 4, then

$$1^3 + 2^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.$$  

Is this statement true if $n$ is even but not divisible by 4?

By a problem from the first HW,

$$1^3 + 2^3 + \cdots + (n-1)^3 = \left[\frac{n(n-1)}{2}\right]^2 = \frac{n^2(n-1)^2}{4}.$$  

If $4 \mid n$, then $n = 4k$ for some integer $k$, so

$$\frac{n^2(n-1)^2}{4} = kn(n-1)^2 \equiv 0 \pmod{n}.$$  

If $n$ is odd then $n-1$ is even, so $n-1 = 2m$ for some integer $m$. Then

$$\frac{n^2(n-1)^2}{4} = n^2m^2 \equiv 0 \pmod{n}.$$  

If $n$ is even but not divisible by 4, then $n = 2\ell$ for some odd integer $\ell$, and

$$\frac{n^2(n-1)^2}{4} = \ell^2(n-1)^2 = \ell^2n^2 - 2\ell^2n + \ell^2 \equiv \ell^2 \pmod{n},$$  

and since $\ell$ is odd and $n$ is even, $n \nmid \ell^2$, so $\ell^2 \not\equiv 0 \pmod{n}$.

(4.1 # 22) Show by induction that if $n$ is a positive integer, then $4^n \equiv 1 + 3n \pmod{9}$.

For the base case, $4 \equiv 1+3 \pmod{9}$. For the induction hypothesis, assume that $4^n \equiv 1+3n \pmod{9}$ for some positive integer $n$. Then

$$4^{n+1} = 4 \cdot 4^n \equiv 4(1+3n) \equiv 4 + 12n \equiv 4 + 3n \equiv 1 + 3(n+1) \pmod{9}.$$  

Therefore $4^n \equiv 1 + 3n \pmod{9}$ for all positive integers $n$.  

(4.1 # 26) Show that if \( p \) is prime, then the only solutions of the congruence \( x^2 \equiv x \pmod{p} \) are those integers \( x \) such that \( x \equiv 0 \) or \( 1 \pmod{p} \).

If \( x^2 \equiv x \pmod{p} \), then \( x(x-1) \equiv 0 \pmod{p} \). Thus \( p \mid x(x-1) \), so \( p \mid x \) or \( p \mid x-1 \). Hence the only solutions are \( x \equiv 0 \pmod{p} \) or \( x \equiv 1 \pmod{p} \).

(4.2 # 2) Find all solutions to the following linear congruences.

(b) \( 6x \equiv 3 \pmod{9} \).

Since \( (6, 9) = 3 \), there are 3 incongruent solutions. It’s easy to see that \( x \equiv 2 \pmod{9} \) is one solution. Then since \( 9/3 = 3 \), the other solutions are \( x \equiv 2 + 3 \equiv 5 \pmod{9} \) and \( x \equiv 2 + 6 \equiv 8 \pmod{9} \).

(c) \( 17x \equiv 14 \pmod{21} \)

Since \( (17, 21) = 1 \), there is a unique solution modulo 21. Using the Euclidean Algorithm we find that \( 17(5) - 21(4) = 1 \), so multiplying by 14, we have \( 17(70) - 21(56) = 14 \). Therefore the unique solution is \( x \equiv 70 \equiv 7 \pmod{21} \).

(d) \( 15x \equiv 9 \pmod{25} \).

Since \( (15, 25) = 5 \) and \( 5 \nmid 9 \), there are no solutions.

(4.2 # 10) Determine which integers \( a \), where \( 1 \leq a \leq 14 \), have an inverse modulo 14, and find the inverse of each of these integers modulo 14.

The numbers \( a \) with an inverse modulo 14 are those for which \( (a, 14) = 1 \): 1, 3, 5, 9, 11, and 13. The inverse of each of these integers modulo 14 is also in that list, since if \( ab \equiv 1 \pmod{m} \), then both \( a \) and \( b \) have an inverse modulo \( m \). So we see that \( \overline{1} = 1, \overline{3} = 5, \overline{5} = 3, \overline{9} = 11, \overline{11} = 9, \) and \( \overline{13} = 13 \).

(4.2 # 18) Show that if \( p \) is an odd prime and \( a \) is a positive integer not divisible by \( p \), then the congruence \( x^2 \equiv a \pmod{p} \) has either no solution or exactly two incongruent solutions.

If the congruence has no solutions, we are done, so suppose that it has at least one solution \( c \). Then \( c^2 \equiv a \pmod{p} \), so also \( (-c)^2 \equiv a \pmod{p} \). If \( c \equiv -c \pmod{p} \), then \( 2c \equiv 0 \pmod{p} \). Since \( p \) is odd, this implies that \( p \mid c \). But then \( a \equiv c^2 \equiv 0 \pmod{p} \). This is a contradiction since \( p \nmid a \). Therefore \( c \) and \( -c \) are incongruent solutions. Now suppose \( b \) is another solution. Then \( b^2 \equiv c^2 \pmod{p} \), so \( (b + c)(b - c) \equiv b^2 - c^2 \equiv 0 \pmod{p} \). Then either \( p \mid (b + c) \) or \( p \mid (b - c) \), so \( b \equiv \pm c \pmod{p} \). Therefore there are exactly two incongruent solutions modulo \( p \).

(4.3 # 12) If eggs are removed from a basket 2, 3, 4, 5, and 6 at a time, there remain, respectively, 1, 2, 3, 4, and 5 eggs. But if the eggs are removed 7 at a time, no eggs remain. What is the least number of eggs that could have been in the basket?
We need to find the least positive integer solution to the system of congruences
\[ \begin{align*}
    x &\equiv 1 \pmod{2} \\
    x &\equiv 2 \pmod{3} \\
    x &\equiv 3 \pmod{4} \\
    x &\equiv 4 \pmod{5} \\
    x &\equiv 5 \pmod{6} \\
    x &\equiv 0 \pmod{7}.
\end{align*} \]

Since the moduli are not pairwise coprime, we can’t use the Chinese Remainder Theorem. However, we notice from the first and fourth congruences that \( x \) must end in a 9, and from the last congruence, it must be a multiple of 7. Since \( 49 \not\equiv 2 \pmod{3} \), we try the next number satisfying these properties, which is 119. It is easy to check that 119 satisfies every congruence.

(3.3 \# 14(b)) Use induction to show that if \( a_1, a_2, \ldots, a_n \) are integers, and \( b \) is another integer such that \((a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1\), then \((a_1a_2 \cdots a_n, b) = 1\).

The base case is trivial. Suppose the statement is true for \( n \). Now suppose that \((a_1, b) = (a_2, b) = \cdots = (a_n, b) = (a_{n+1}, b) = 1\). By the induction hypothesis, \((a_1a_2 \cdots a_n, b) = 1\), so there are integers \( s \) and \( t \) such that
\[ a_1a_2 \cdots a_n s + bt = 1. \]
Multiplying through by \( a_{n+1} \), we have
\[ a_1a_2 \cdots a_n a_{n+1} s + a_{n+1} bt = a_{n+1}. \]
Also, since \((a_{n+1}, b) = 1\), we have integers \( e \) and \( f \) such that \( a_{n+1} e + bf = 1\). Substituting for \( a_{n+1} \), we have
\[ (a_1a_2 \cdots a_n a_{n+1} s + a_{n+1} bt)e + bf = 1. \]
Rewriting, we have
\[ (a_1a_2 \cdots a_n a_{n+1} (se) + b(a_{n+1} te + f) = 1, \]
so \((a_1a_2 \cdots a_n a_{n+1}, b) = 1\). Therefore, the statement is true for all positive integers \( n \).