Theorem. (The Division Algorithm) Let \( a, b \) be integers with \( b \neq 0 \). Then there exist unique integers \( q \) and \( r \) such that \( a = bq + r \) and \( 0 \leq r < |b| \).

Theorem. Let \( a \) and \( b \) be integers, not both 0, and let \( d \) be their greatest common divisor. Then there exist, not necessarily unique, integers \( a \) and \( b \) such that \( d = au + bv \). Furthermore, \( d \) is the smallest positive integer that can be written in the form \( au + bv \).

Theorem. Let \( p \) be an integer such that \( p \neq 0, \pm 1 \). Then \( p \) is prime if and only if for each \( i, j \) such that \( p_i \parallel bc \), then \( p_i \parallel b \) or \( p_i \parallel c \).

Theorem. (The Fundamental Theorem of Arithmetic) Every integer, except 0, \( \pm 1 \) is a product of primes. This prime factorization is unique in the following sense: If \( \prod p^k_i \parallel n \) and \( \prod q^j_i \parallel n \), then \( k_i = j_i \) for all \( i \). Then \( S \) is a subring of \( R \).

Theorem. Let \( S \) be a nonempty subset of a ring \( R \) such that

1. \( S \) is closed under subtraction;
2. \( S \) is closed under multiplication.

Then \( S \) is a subring of \( R \).
I. Review homework problems.

II. Review quizzes.

III. Be able to prove short and straightforward theorems (e.g. see Problem 11 below).

Some practice problems for review

1. Let $a, b$ be integers and let $k = ab + 1$. Prove that $\gcd(k, a) = \gcd(k, b) = 1$.

2. Let $a, b$ be integers. Prove that $\gcd(a, b) = \gcd(a, b + at)$ for every $t \in \mathbb{Z}$.

3. Prove that $\sqrt{77}$ is irrational.

4. If $a \equiv 2 \pmod{4}$, prove that there are no integers $c$ and $d$ such that $a = c^2 - d^2$.

5. Prove or disprove: If $a$ and $b$ are integers with $[a] = [b + 2]$ in $\mathbb{Z}_6$, then $a - b$ is not a prime.

6. Solve the equation $x^2 + 3x + 2 = 0$ in $\mathbb{Z}_p$, where $p \geq 3$ is a prime.

7. Solve the equations in $\mathbb{Z}_{12}$:
   (a) $3x = 9$
   (b) $5x = 7$
   (c) $4x = 6$.

8. Let $d$ be an integer that is not a perfect square. Show that $\mathbb{Q}(\sqrt{d}) = a + b\sqrt{d} \mid a, b \in \mathbb{Q}$ is a subfield of $\mathbb{C}$.

9. Define new addition and new multiplication on $\mathbb{Z}$ by $a \oplus b = a + b - 1$ and $a \odot b = ab - (a + b) + 2$. Prove that with these new operations $\mathbb{Z}$ is an integral domain.

10. The addition and multiplication table for a three element commutative ring with an identity are given below. Use the ring laws to complete the tables.

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>c</td>
<td>b</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>c</td>
<td>a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
</tbody>
</table>

Solve the given equation $c + x = a^2$ for $x$ in the given ring.

11. Be able to prove any of the statements in the following

   **Theorem.** For any elements $a$ and $b$ of a ring $R$,
   (a) $a \cdot 0_R = 0_r = 0_R \cdot a$.
   (b) $a(-b) = -(ab) = (-a)b$.
   (c) $-(-a) = a$.
   (d) $-(a + b) = (-a) + (-b)$.
   (e) $(-a)(-b) = ab$.

12. Can a ring have more than one zero element? How about more than one identity element?