Modular arithmetic

For every positive integer \( m \), the \textit{integers modulo} \( m \) are:

\[ \mathbb{Z}_m : 0, 1, \ldots, m - 1. \]

with arithmetic operations of addition \( +_m \) and multiplication \( \cdot_m \) defined as follows

\[
\begin{align*}
  k +_m l &= \lfloor k + l \rfloor_m = \text{rem}(k + l, m), \\
  k \cdot_m l &= \lfloor k \cdot l \rfloor_m = \text{rem}(k \cdot l, m)
\end{align*}
\]

for all \( 0 \leq k, l < m \).
Example 49  The addition and multiplication tables for $\mathbb{Z}_4$ are:

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\quad
\begin{array}{c|cccc}
\cdot & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 2 & 0 & 2 & 0 \\
3 & 3 & 0 & 3 & 2 \\
\end{array}
\]

Note that the addition table has a cyclic pattern, while there is no obvious pattern in the multiplication table.
From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

<table>
<thead>
<tr>
<th></th>
<th>additive inverse</th>
<th></th>
<th>multiplicative inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Interestingly, we have a non-trivial multiplicative inverse; namely, 3.
Example 50  *The addition and multiplication tables for \( \mathbb{Z}_5 \) are:*

<table>
<thead>
<tr>
<th></th>
<th>( \mathbb{Z}_5 ) Addition</th>
<th>( \mathbb{Z}_5 ) Multiplication</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 1 2 3 4</td>
<td>0 0 0 0 0</td>
</tr>
<tr>
<td>1</td>
<td>1 2 3 4 0</td>
<td>1 0 1 2 3</td>
</tr>
<tr>
<td>2</td>
<td>2 3 4 0 1</td>
<td>2 0 2 4 1</td>
</tr>
<tr>
<td>3</td>
<td>3 4 0 1 2</td>
<td>3 0 3 1 4</td>
</tr>
<tr>
<td>4</td>
<td>4 0 1 2 3</td>
<td>4 0 4 3 2</td>
</tr>
</tbody>
</table>

Again, the addition table has a cyclic pattern, while this time the multiplication table restricted to non-zero elements has a permutation pattern.
From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

<table>
<thead>
<tr>
<th>additive inverse</th>
<th>multiplicative inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Surprisingly, every non-zero element has a multiplicative inverse.
Proposition 51  For all natural numbers \( m > 1 \), the modular-arithmetic structure

\[(\mathbb{Z}_m, 0, +_m, 1, \cdot_m)\]

is a commutative ring.

NB  Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses.
Important mathematical jargon: Sets

Very roughly, sets are the mathematicians’ data structures. Informally, we will consider a set as a (well-defined, unordered) collection of mathematical objects, called the elements (or members) of the set.
Set membership

The symbol ‘∈’ known as the set membership predicate is central to the theory of sets, and its purpose is to build statements of the form

\[ x \in A \]

that are true whenever it is the case that the object \( x \) is an element of the set \( A \), and false otherwise.
## Defining sets

<table>
<thead>
<tr>
<th>The set</th>
<th>of even primes of booleans</th>
<th>is</th>
<th>{-2, -1, 0, 1, 2, 3}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>([-2 .. 3])</td>
<td></td>
<td>{true, false}</td>
</tr>
</tbody>
</table>
Set comprehension

The basic idea behind set comprehension is to define a set by means of a property that precisely characterises all the elements of the set.

Notations:

\[ \{ x \in A \mid P(x) \} , \{ x \in A : P(x) \} \]

\[ a \in \{ x \in A \mid P(x) \} \iff (a \in A \land P(a)) \]
Greatest common divisor

Given a natural number $n$, the set of its divisors is defined by set comprehension as follows

$$D(n) = \{ d \in \mathbb{N} : d \mid n \}.$$  the set of divisors of $n$

Example 53

1. $D(0) = \mathbb{N}$

2. $D(1224) = \{ 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 68, 72, 102, 136, 153, 204, 306, 408, 612, 1224 \}$

Remark  Sets of divisors are hard to compute. However, the computation of the greatest divisor is straightforward. : )
Going a step further, what about the common divisors of pairs of natural numbers? That is, the set

$$\text{CD}(m, n) = \{ d \in \mathbb{N} : d \mid m \land d \mid n \}$$

for $m, n \in \mathbb{N}$.

**Example 54**

$$\text{CD}(1224, 660) = \{1, 2, 3, 4, 6, 12\}$$

Since $\text{CD}(n, n) = \text{D}(n)$, the computation of common divisors is as hard as that of divisors. But, what about the computation of the greatest common divisor?
Lemma 56 (Key Lemma) Let $m$ and $m'$ be natural numbers and let $n$ be a positive integer such that $m \equiv m' \pmod{n}$. Then,

$$CD(m, n) = CD(m', n).$$

**Proof:**

Assume $m \equiv m' \pmod{n}$.

If $d \in CD(m, n)$, then $d \in CD(m', n)$ for all $d$.

$(\Rightarrow)$ Assume $d \in CD(m, n) \iff d \mid m$ and $d \mid n$.

If $d \in CD(m', n)$, then $d \mid m'$ and $d \mid n$.

If $d \mid m'$ and $d \mid n$, then $d \mid (m' - m)$.

If $d \mid (m' - m)$, then $d \mid m'$ and $d \mid n$.

If $d \mid n$, then $d \mid m$.

Hence, $d \in CD(m, n)$.

Therefore, $CD(m, n) = CD(m', n)$.
Lemma

\[ d \mid a \land d \mid b \implies d \mid p \cdot a + q \cdot b \ \forall p, q. \]

\[ \exists \text{ integer linear combination}. \]

\[
\begin{align*}
CD(m, n) &= CD\left(\frac{\text{rem}(m, n)}{\text{rem}(m, n)} \equiv m \pmod{n}\right) \\
&= CD(m - n, n) \quad m - n \equiv m \ (m > n) \\
CD(Rn, n) &= D(n)
\end{align*}
\]
Lemma 58  For all positive integers $m$ and $n,$

\[ CD(m, n) = \begin{cases} \text{greatest} \ D(n) = n, & \text{if } n \mid m \\ \text{greatest} \ CD(n, \text{rem}(m, n)), & \text{otherwise} \end{cases} \]
Lemma 58  For all positive integers $m$ and $n$,

$$\text{CD}(m, n) = \begin{cases} D(n), & \text{if } n \mid m \\ \text{CD}(n, \text{rem}(m, n)), & \text{otherwise} \end{cases}$$

Since a positive integer $n$ is the greatest divisor in $D(n)$, the lemma suggests a recursive procedure:

$$\text{gcd}(m, n) = \begin{cases} n, & \text{if } n \mid m \\ \text{gcd}(n, \text{rem}(m, n)), & \text{otherwise} \end{cases}$$

for computing the greatest common divisor, of two positive integers $m$ and $n$. This is

Euclid’s Algorithm
fun gcd( m , n )
  = let
    val ( q , r ) = divalg( m , n )
  in
    if r = 0 then n
    else gcd( n , r )
  end
Example 59 \((\gcd(13, 34) = 1)\)

\[
\gcd(13, 34) = \gcd(34, 13) \\
= \gcd(13, 8) \\
= \gcd(8, 5) \\
= \gcd(5, 3) \\
= \gcd(3, 2) \\
= \gcd(2, 1) \\
= 1
\]
Theorem 60 Euclid’s Algorithm $\text{gcd}$ terminates on all pairs of positive integers and, for such $m$ and $n$, $\text{gcd}(m, n)$ is the greatest common divisor of $m$ and $n$ in the sense that the following two properties hold:

(i) both $\text{gcd}(m, n) | m$ and $\text{gcd}(m, n) | n$, and 

(ii) for all positive integers $d$ such that $d | m$ and $d | n$ it necessarily follows that $d | \text{gcd}(m, n)$.

Proof: Partial correctness: Because

$$\text{gcd}(m, n) = D(\text{gcd}(m, n))$$

by design of the algorithm.
\[ \text{gcd}(m, n) \]

\[ m = q \cdot n + r \]
\[ q > 0 , 0 < r < n \]
\[ 0 < m < n \]

\[ n \mid m \]

\[ \text{gcd}(n, r) \]

\[ r \mid n \]
\[ n = q' \cdot r + r' \]
\[ q' > 0 , 0 < r' < r \]

\[ \text{gcd}(r, r') \]

\[ \text{gcd}(n, m) \]

\[ \frac{r'}{2} < \frac{n}{2} \]

\[ 2r' < r + r' \leq q' \cdot r + r' = n \]
Idea:

Running Time and Fibonacci:

Calculate \( \gcd(F_{n+1}, F_n) \)
and look at its running time.
Fractions in lowest terms

fun lowterms( m , n )
  = let
     val gcdval = gcd( m , n )
   in
     ( m div gcdval , n div gcdval )
   end