(##1) Prove the basic lemma: If \(a \equiv b \pmod{n}\) and \(c \equiv d \pmod{n}\), then \((a + c) \equiv (b + d) \pmod{n}\).

From the definition of congruence, we have:

\[ a - b = k_1n \quad \text{and} \quad c - d = k_2n. \]

If we combine these two equalities, we have:

\[
\begin{align*}
  a - b + c - d &= k_1n + k_2n \\
  a + c - (b + d) &= (k_1 + k_2)n
\end{align*}
\]

From our definition of congruence mod \(n\), we must have:

\[
(a + c) \equiv (b + d) \pmod{n}.
\]

(##2) Here are all the lemmas that you should know how to prove, but unless we ask you for a specific proof (as above), then you may use them as lemmas in other proofs.

(a) If \(a \equiv b \pmod{n}\), then \(ka \equiv kb \pmod{n}\).

(b) If \(a \equiv b \pmod{n}\) and \(c \equiv d \pmod{n}\), then \(ac \equiv bd \pmod{n}\).

(c) If \(m \in \mathbb{Z}^+\) and \(a \equiv b \pmod{n}\), then \(a^m \equiv b^m \pmod{n}\).

(d) Because \(kn \equiv 0 \pmod{n}\), we can reduce a congruence: If \(a \equiv b \pmod{n}\), then \(a \equiv (b \pm kn) \pmod{n}\).

(##3) In most computing languages (including graphing calculators), there is a \texttt{mod} function.

If \(n \in \mathbb{Z}^+\) and \(n \geq 2\), then the definition is:

\[
\text{mod}(m, n) \quad \text{is the nonnegative remainder when} \quad m \quad \text{is divided by} \quad n.
\]

This is a result from the “Division Algorithm Theorem”.

Essentially, WLOG, if \(m\) is positive and \(n \geq 2\), then division is nothing more than repetitive subtraction.

We say that there exists UNIQUE nonnegative integers \(q\) and \(r\) such that

\[ m = qn + r, \]

where \(q\) is the quotient (the number of times \(n\) can be subtracted from \(m\)) and \(r\) is the nonnegative remainder such that \(0 \leq r \leq (n - 1)\).

PROOF: It should clear that at least one value of \(q\) exists. If \(n\) cannot be subtracted from \(m\) because \(m\) is too small, then we have \(q = 0\).

Once we have chosen a nonnegative \(q\), then we must have

\[ r = m - qn, \]

and we want to show that \(0 \leq r \leq (n - 1)\).
Assume that after subtracting \(n\) a total of \(q\) times, we have a unique remainder based on \(q\). We must have
\[
r < n,
\]
else we could have subtracted \(n\) at least one more time. Thus, we must have
\[
0 \leq r \leq (n - 1) .
\]

Is it possible for us to have two different \(q\)'s? NO.

BWOC, suppose we have two different results from the algorithm: \((q_1, r_1)\) and \((q_2, r_2)\).

WLOG, let’s assume that \(q_1 > q_2\).
\[
q_1 n + r_1 = q_2 n + r_2 \quad (q_1 - q_2) n = r_2 - r_1.
\]

Since \((q_1 - q_2) \geq 1\), the left side is some positive multiple of \(n\).
The right side is a number less than \(n\) minus another number less than \(n\), so it must be less than \(n\). (\(\Rightarrow\Rightarrow\))

Thus, the mod function produces unique nonnegative values of \(q\) and \(r\).

(a) Examples:
\[
\text{mod}(m, 2) = 0 \text{ iff } m \text{ is even, because } m \equiv 0 \text{ (mod 2)} .
\]
\[
\text{mod}(m, 2) = 1 \text{ iff } m \text{ is odd, because } m \equiv 1 \text{ (mod 2)} .
\]

(b) Suppose the base is \(n = 3\).
\[
3 \mid m \text{ iff } \text{mod}(m, 3) = 0 .
\]
\[
3 \nmid m \text{ iff } \text{mod}(m, 3) = 1 \text{ or } 2 .
\]

(c) In general, we have
\[
n \nmid m \text{ iff } \text{mod}(m, n) \in \{1, ..., (n - 1)\} .
\]

(\#4) Sometimes, we need to be a bit more flexible.

Again, what does it mean if \(n \equiv 1 \text{ (mod 2)}\)? We know that \(n\) is odd.
However, what does this mean if we use base 4?
The odd remainders in base 4 are 1 and 3.

Consider Problem [4.53].

Let \(n, m \in \mathbb{Z}\). Prove that if \(n \equiv 1 \text{ (mod 2)}\) and \(m \equiv 3 \text{ (mod 4)}\), then \((n^2 + m) \equiv 0 \text{ (mod 4)}\).

Case 1: Suppose \(n \equiv 1 \text{ (mod 4)}\).

By multiplication, we have \(n^2 \equiv 1 \text{ (mod 4)}\), and by addition, we must have
\[
n^2 + m \equiv 1 + 3 \equiv 4 \equiv 0 \text{ (mod 4)} .
\]

Case 2: Suppose \(n \equiv 3 \text{ (mod 4)}\).

By multiplication, we have \(n^2 \equiv 9 \equiv 1 \text{ (mod 4)}\), and by addition, we must have
\[
n^2 + m \equiv 1 + 3 \equiv 4 \equiv 0 \text{ (mod 4)} .
\]
(\#5) Modular arithmetic can substantially shorten our proofs.

[4.4] Let \( x, y \in \mathbb{Z} \). Prove that if \( 3 \nmid x \) and \( 3 \nmid y \), then \( 3 \mid (x^2 - y^2) \).

If \( 3 \nmid x \), then \( x \equiv 1 \) or \( 2 \) (mod \ 3).

By multiplication, we have \( x^2 \equiv 1 \) or \( 4 \) (mod \ 3), but \( 4 \equiv 1 \) (mod \ 3), they are both congruent to \( 1 \) (mod \ 3).

The same is true for \( y^2 \), and thus,

\[
x^2 - y^2 \equiv 1 - 1 \equiv 0 \pmod{3}.
\]

(\#6) Do we have any interesting rules for this one?

[4.15] Let \( a, b \in \mathbb{Z} \). Show that if \( a \equiv 5 \) (mod \ 6) and \( b \equiv 3 \) (mod \ 4),

then \( (4a + 6b) \equiv 6 \) (mod \ 8). Probably not.

We must convert everything to representatives with \( k \)'s in them.

Let \( a = 6k_1 + 5 \) and \( b = 4k_2 + 3 \).

We have the quantity:

\[
4a + 6b = 4(6k_1 + 5) + 6(4k_2 + 3) = 24k_1 + 24k_2 + 38
\]

\[
= 24k_1 + 24k_2 + 32 + 6 = 8(3k_1 + 3k_2 + 4) + 6.
\]

By closure, this is \( 8k + 6 \), and we have \( (4a + 6b) \equiv 6 \pmod{8} \).

(\#7) Does this help us with “if and only if” proofs? Sometimes.

[4.8] Prove that \( 2 \mid (n^4 - 3) \) iff \( 4 \mid (n^2 + 3) \).

There are more cases on the right side, so we should do everything in (mod \ 4).

<table>
<thead>
<tr>
<th>(mod 4)</th>
<th>(n^2 + 3) (mod 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>4 \equiv 0</td>
</tr>
<tr>
<td>2</td>
<td>7 \equiv 3</td>
</tr>
<tr>
<td>3</td>
<td>12 \equiv 0</td>
</tr>
</tbody>
</table>

By cases, we see that \( 4 \mid (n^2 + 3) \) iff \( n \) is odd.

Not that this is biconditional, because if \( n \) is even \( \iff 4 \nmid (n^2 + 3) \).

We also have \( n \) is odd \( \iff (n^4 - 3) \) is even, because \( (odd)^4 \) is odd and \( (odd - odd) \) is even.

I leave it to you to verify the biconditional.

Thus, we have \( 4 \mid (n^2 + 3) \) iff \( n \) is odd \( \iff 2 \mid (n^4 - 3) \).