General Comments:

- The notation “(mod m)” is used in only one context: to clarify what is meant by a congruence (≡). For instance, I can’t tell whether 12 ≡ 4 is true or not unless you specify the modulus. To that end, whenever you are doing a computation involving congruences or stating that two numbers are congruent, you must specify the modulus by writing (mod m) only once at the end of the computation.

Some authors use “mod m”, usually without parentheses, to denote “remainder modulo m”, but we are not using that notation in this class. For instance, other sources may write something like 12 mod 5 = 2, but that is gibberish to us.

As above, I sometimes write out the phrase “modulo m”. This does not have the same function as writing “(mod m)”! I use the phrase “modulo m” to mean “when divided by m”. Thus for instance I say “find the remainder of 12 modulo 5” instead of writing “find the remainder of 12 when it is divided by 5”. It makes no sense to write something like “12 modulo 5 ≡ 2”. Instead I would write 12 ≡ 2 (mod 5) or “2 is the remainder of 12 modulo 5”, depending on what I want to emphasize.

- Please clearly state any statements you are proving as claims! Label your proof with “Proof”!

- Some of you are getting sloppy in your proof writing. What did proofs do to you that caused them to lose your respect? Make them nice, clear, and concise! Make your computations neat and concise too, as in my solutions below.

Exercise 4.3.15

(a) Find the remainder of $3 \cdot 4 \cdot 5 + 11$ modulo 6.

Solution:

$$3 \cdot 4 \cdot 5 + 11 = 12 \cdot 5 + 11 \equiv 11 \equiv 5 \pmod{6}.$$
• The notation “(mod 6)” is used exactly once, to clarify what all the congruence symbols \((\equiv)\) in the computation mean.
• Write an equals sign (=) when two quantities are equal, rather than just congruent \((\equiv)\). Of course, equality implies congruence for any modulus.

(b) Find the remainder of \(-2^3 \cdot 11 - 71\) modulo 7.

Solution:

\[-2^3 \cdot 11 - 71 \equiv -1 \cdot 4 - 1 = -5 \equiv 2 \pmod{7}.\]

(c) Find the remainder of \(5^{999} + 16\) modulo 4.

Solution:

\[5^{999} + 16 \equiv 1^{999} = 1 \pmod{4}.\]

(d) Find the remainder of \(3^{2200}\) modulo 8.

Solution:

\[3^{2200} = (3^2)^{2200} \equiv 1^{2200} = 1 \pmod{8}.\]

**Exercise 4.3.16**

**Claim** (a). Let \(n \in \mathbb{Z}\). Then \(n^2 \equiv 0 \pmod{4}\) or \(n^2 \equiv 1 \pmod{4}\).

**Proof #1.** If \(n\) is even, then there is \(k \in \mathbb{Z}\) such that \(n = 2k\). Then \(n^2 = 4k^2 \equiv 0 \pmod{4}\). If \(n\) is odd, then there is \(j \in \mathbb{Z}\) such that \(n = 2j + 1\). Then \(n^2 = 4j^2 + 4j + 1 \equiv 1 \pmod{4}\). \(\square\)

**Proof #2.** Since \(n\) is congruent to its remainder modulo 4, it suffices to prove \(n^2 \equiv 0 \pmod{4}\) for \(n = 0, 1, 2, 3\). We compute:

\[
\begin{align*}
0^2 &= 0; & 1^2 &= 1; & 2^2 &= 4 \equiv 0 \pmod{4}; & 3^2 &= 9 \equiv 1 \pmod{4}.
\end{align*}
\]

\(\square\)

**Claim** (b). Let \(n \in \mathbb{Z}\). If \(n\) is odd, then \(n^2 \equiv 1 \pmod{8}\).

**Proof #1.** Since \(n\) is odd, there is \(k \in \mathbb{Z}\) such that \(n = 2k + 1\). Then \(n^2 = 4k(k + 1) + 1\). Since \(k\) and \(k + 1\) are consecutive integers, one of the two must be even, so \(k(k + 1)\) is even, namely \(k(k + 1) = 2j\) for some \(j \in \mathbb{Z}\). Thus

\[n^2 = 4k(k + 1) + 1 = 4(2j) + 1 = 8j + 1 \equiv 1 \pmod{8}.\]

\(\square\)

**Proof #2.** Since \(n\) is odd and 8 is even, the remainder of \(n\) modulo 8 is odd. Since \(n\) is congruent to its remainder modulo 8, it suffices to check the claim for \(n = 1, 3, 5, 7\). We compute:

\[
\begin{align*}
1^2 &= 1; & 3^2 &= 9 \equiv 1 \pmod{8}; & 5^2 &= 25 \equiv 1 \pmod{8}; & 7^2 &= (-1)^2 = 1 \pmod{8}.
\end{align*}
\]

\(\square\)
Exercise 4.3.20

(a) Use Fermat’s little theorem (FLT) to find the remainder of $7^{121}$ modulo 13.

Solution: Since 13 is prime and 13 $\nmid$ 7, Fermat’s little theorem implies $7^{12} \equiv 1 \pmod{13}$. Thus

$$7^{121} = (7^{12})^{10} \cdot 7 \equiv 7 \pmod{13}.$$ 

(b) Use FLT to find the remainder of $22^{100}$ modulo 11.

Solution: Since 11 $\mid$ 22, FLT does not apply. But we can still easily compute

$$22^{100} \equiv 0^{100} = 0 \pmod{11}.$$

(c) Use FLT to find the remainder of $24^{39}$ modulo 7.

Solution: First note that $24 \equiv 3 \pmod{7}$. Since 7 is prime and 7 $\nmid$ 3, FLT implies $3^6 \equiv 1 \pmod{7}$. Thus

$$24^{39} \equiv 3^{39} = (3^6)^6 \cdot 3^3 \equiv 1^6 \cdot 27 \equiv 6 \pmod{7}.$$ 

Exercise 4.3.22

Claim (a). Let $a \in \mathbb{Z}_{\geq 1}$ and let $D$ denote the sum of the digits of $a$. Then $5 \mid a$ if and only if $5 \mid D$.

This claim is false! Counterexample: Let $a = 15$, so $D = 6$. Then $5 \mid a$, but $5 \nmid D$.

Claim (b). Let $a \in \mathbb{Z}_{\geq 1}$ and let $D$ denote the sum of the digits of $a$. Then $9 \mid a$ if and only if $9 \mid D$.

Proof. Write $a = a_na_{n-1}\ldots a_0$, where the $a_i$ denote the digits of $a$. Then

$$a = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^n a_n \equiv a_0 + a_1 + \cdots + a_n = D \pmod{9}.$$ 

Since $a \equiv D \pmod{9}$, we see that $a \equiv 0 \pmod{9}$ if and only if $D \equiv 0 \pmod{9}$. \hfill \Box

Exercise 4.3.23

Claim (Criterion for divisibility by 5). Let $a \in \mathbb{Z}_{\geq 1}$ and let $a_0$ denote the one’s digit of $a$. Then $5 \mid a$ if and only if $5 \mid a_0$.

Proof. Write $a = a_na_{n-1}\ldots a_0$, where the $a_i$ denote the digits of $a$. Then

$$a = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^n a_n \equiv a_0 \pmod{5}.$$ 

Since $a \equiv a_0 \pmod{5}$, we see that $a \equiv 0 \pmod{5}$ if and only if $a_0 \equiv 0 \pmod{5}$. \hfill \Box

Claim (Criterion for divisibility by 11). Let $a \in \mathbb{Z}_{\geq 1}$ and let $E$ denote the alternating sum of the digits of $a$. Then $11 \mid a$ if and only if $11 \mid E$.
Proof. Write \( a = a_n a_{n-1} \ldots a_0 \), where the \( a_i \) denote the digits of \( a \). Then

\[
a = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^na_n \\
\equiv a_0 + (-1)a_1 + (-1)^2a_2 + \cdots + (-1)^na_n \\
= a_0 - a_1 + a_2 - \cdots + (-1)^na_n \\
= E \pmod{11}.
\]

Since \( a \equiv E \pmod{11} \), we see that \( a \equiv 0 \pmod{11} \) if and only if \( E \equiv 0 \pmod{11} \).

Comments:

- State your criteria precisely as claims!
- These divisibility criteria are really useful and easy to use! For instance, I can immediately tell that \( 11 \mid 13541 \) and \( 11 \mid 616 \), while \( 11 \nmid 10101 \) and \( 11 \nmid 11111 \).