Math 212, Lecture 10

Arithmetic in congruence

Last time: Defined congruence:

\[ a \equiv b \pmod{m} \iff m \mid b - a \]

Checkered: (1) Congruence is like equality:

\[ a \equiv a \pmod{m}, \ a \equiv b \pmod{m} \implies b \equiv a \pmod{m}, \]

\[ (a \equiv b \pmod{m} \land b \equiv c \pmod{m}) \implies (a \equiv c \pmod{m}). \]

(2) Arithmetic (+, -, \cdot) respects congruence:

If \( a \equiv a' \pmod{m}, \ b \equiv b' \pmod{m} \) then

\[ a + b \equiv a' + b' \pmod{m}, \]

\[ a \cdot b \equiv a' \cdot b' \pmod{m}. \]

Lemma: \( a \equiv b \pmod{m} \iff b \) is obtained from \( a \) by shifting by a multiple of \( m \).

(record & recall math using "stories")
In practice: Working mod 7.

\[ 1000 \cdot 613 = (1001 - 1) \cdot (613 - 630) \]
\[ = -1 \cdot (-17) = 17 = 3 \mod 7 \]

Recall division thm: Given a, m have q, r s.t. \( a = qm + r \), \( 0 \leq r < m \).

i.e., for each a have \( 0 \leq r < m \) s.t.
\( a \equiv r \mod m \)

Passage from a to r is called "reduction mod m", r is called the "residue" = "remainder".

Modular arithmetic also called "residue calculus."

Different way: \( 1000 = 142 \cdot 7 + 6 \)
613 = 87 \cdot 7 + 4
\Rightarrow \quad 1000 \cdot 613 = (6 + 142 \cdot 7) \cdot (4 + 87 \cdot 7)
\quad = 6 \cdot 4 + 6 \cdot 7 + 4 \cdot 7 + 7 \cdot 7
\quad = 24 \pmod{7}
\quad \equiv 3 \cdot 7 + 3 \equiv 3 \pmod{7}

When directly calculating, reduce first, then do arithmetic.

**Bottom line:** “Modular arithmetic” is an arithmetic system with \( m \) “numbers”, can take to be \( 0, 1, \ldots, m-1 \), rules of arithmetic: do operation in \( \mathbb{Z} \), then reduce mod \( m \).

**Facts:** this works: set usual rules of arithmetic.

**Observe:** let \( 0 \leq a, b < m \)
(both are "reduced residues")
then either \(a = b\) or \(a \neq b\) (m)

**Pf:** if \(0 \leq a, b < m\), then \(|a - b| < |m - 0| = m\)
so \(m\) can't divide \(b - a\) unless \(b - a = 0\)

\[
\begin{array}{cccccc}
\text{0} & \text{a} & \text{b} & \text{m-1} & \text{m} \\
\hline
\end{array}
\]

(more 13, have an arithmetic system
with 13 numbers, can be taken to be

\(0, 1, 2, 3, \ldots, 12\))

can also say:

\[
1000 \cdot 613 = 6(1000 - 1) \cdot (560 + 53)
\]

\[
\equiv -1 \cdot 53 \equiv -53 \equiv -49 - 4
\]

\[
\equiv -4 \equiv 3 \quad (\text{?})
\]
Application of this idea:

**Divisibility tests**

Observation: \( 10 \equiv 1 \pmod{9} \) (true since \( 10 - 1 = 9 \))

(skill: "unwinding definitions":

can answer question "what does this mean?"
)

So \( 10^2 \mid 1 \cdot 1 \equiv 1 \pmod{9} \)

\[ 1000 = 100 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \pmod{9} \]

\[ 10,000 = 1,000 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \pmod{9} \]

So in fact, \( 10^n \equiv 1 \pmod{9} \) for all \( n \geq 0 \).

If true \( n = 0,1 \). If true for \( n \)

then \( 10^{n+1} = 10^n \cdot 10 \equiv 1 \cdot 1 \equiv 1 \pmod{9} \)

\[ \text{laws of \quad induction \quad case \quad hyp \quad of \quad powers.} \]

Conclusion: \( 7 \cdot 8.534 = 7 \cdot 10^4 + 8 \cdot 10^3 + 5 \cdot 10^2 + 3 \cdot 10 + 4 \)
\[ \equiv 7 \cdot 1 + 8 \cdot 1 + 5 \cdot 1 + 3 \cdot 1 + 4 \cdot 1 \\
= 7 + 8 + 5 + 3 + 4 \equiv 27 \quad (9) \\
= 2 \cdot 10 + 7 \equiv 2 \cdot 1 + 7 = 2 + 7 \\
\equiv 9 \equiv 0 \quad (9) \]

**Prop:** Let \( N \) be an integer, let \( S(N) = \text{sum of the (decimal) digits of } N \). Then \( N \equiv S(N) \quad (9) \)

**Pf:** Write decimal expansion as \( N = \sum_{i=0}^{n} a_i \cdot 10^i \), \( a_i = \text{digits} \)

Then \( N \equiv \sum_{i=0}^{n} a_i \cdot 1 = \sum_{i=0}^{n} a_i : S(N) \quad (9) \)

**Helpful:** \( 9 \mid N \iff N \equiv 0 \quad (9) \)

\[ \iff S(N) \equiv 0 \quad (9) \]
Observation: if $3 \mid a - b$

then $3 \mid a - b$ (Lemma 3/9)

so $3 \mid N \cdot S(N)$ so $S(N) \equiv N \pmod{3}$ (3)

so to check if $N$ is divisible by 3 or 9, replace $N$ with $S(N)$

HW: use same idea to develop a test for divisibility by 11.

\[
\text{Observe: } N \cdot M = S(N) \cdot S(M) \quad (9)
\]

\[
S(N \cdot M) = S(N) \cdot S(M) \quad (9)
\]

\[
\text{Observe: } 10 \equiv 0 \pmod{2} \quad (2) \quad (210)
\]

\[
\Rightarrow 10^n \equiv 0 \pmod{2} \quad \text{if } n \geq 1
\]

\[
\Rightarrow \sum_{i=0}^{n} a_i \cdot 10^i = a_0 \cdot 1 + \sum_{i=1}^{n} a_i \cdot 10 \equiv a_0 \pmod{2} \quad (2)
\]
(parity of $N$ is determined by last digit).

Similarly: $10^2 \equiv 0 (4)$ \hspace{1cm} (100 = 4 \cdot 25)

So if $n \geq 2$, $10^n = 10^2 \cdot 10^{n-2} \equiv 0 \cdot 10^{n-2} \equiv 0 (4)$

So $\sum_{i=0}^{n} a_i \cdot 10^i = a_0 + a_1 \cdot 10 + \sum_{i=2}^{n} a_i \cdot 0$

$\equiv a_0 + a_{n+1} \cdot 10$

(to test if $N$ is divisible by 4, look at last 2 digits)

Ex. show that divisibility by 8 is determined by last 3 digits.

Ex. $510$ just like $210$

So to see if $5 | N$ enough to look at last digit.