Lecture 26

Leading Question: Is 98654320480 divisible by 120?

Instructor's Comments: Note that $120 = 5!$

Divisibility Rules

A positive integer n is divisible by

A) 2^k if and only if the last k digits are divisible by 2^k where $k \in \mathbb{N}$.

B) 3 (or 9) if and only if the sum of the digits is divisible by 3 (or 9).

C) 5^k if and only if the last k digits are divisible by 5^k where $k \in \mathbb{N}$.

D) 7 (or 11 or 13) if and only if the alternating sum of triples of digits is divisible by 7 (or 11 or 13).

Example: $n = 123456333$. Look at $333 - 456 + 123 = 0$ Since $7 \mid 0$ (and 11 and 13), we see that $7 \mid n$ (and 11 and 13).

We prove that 9 divides a number n if and only if the sum of the digits is divisible by 9.

Proof: Let $n \in \mathbb{N}$. Write

$$n = d_0 + 10d_1 + 10^2 d_2 + ... + 10^k d_k$$

where $d_i \in \{0, 1, 2, ..., 9\}$. (For example, $213 = 3 + 10(1) + 100(2)$). Thus,

$$\begin{aligned} 9 \mid n \Leftrightarrow n &\equiv 0 \pmod 9 \\ \Leftrightarrow 0 &\equiv d_0 + 10d_1 + ... + 10^k d_k \pmod 9 \\ \Leftrightarrow 0 &\equiv d_0 + d_1 + ... + d_k \pmod 9 && \text{By (PC)} \\ \Leftrightarrow 9 &\mid (d_0 + d_1 + ... + d_k) \end{aligned}$$

Hence $9 \mid n$ if and only if 9 divides the sum of the digits of n. ■

Instructor's Comments: Note this is the first time I used an iff bidirectional proof. If this is your first time too you should make a note. This is the 10-15 minute mark. Note that if you're running low on time you needn't write out all the divisibility rules (or even mention them!)

Let's look at some examples of division of congruences. Can I divide integers with congruences?

(i) $3 \equiv 24 \pmod 7$

(ii) $1 \equiv 8 \pmod 7$

(iii) $3 \equiv 27 \pmod 6$

(iv) $1 \not\equiv 9 \pmod 6$

The above examples suggests that if you're dividing by a number that is coprime to the modulus, then you can divide. This is true in general.

Proposition: (Congruences and Division (CD)). Let $a, b, c \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Proof: By assumption, $n \mid (ac - bc)$ so $n \mid c(a - b)$. Since $\gcd(c, n) = 1$, by Coprimeness and Divisibility, $n \mid (a - b)$. Hence $a \equiv b \pmod{n}$.

Instructor's Comments: This is the 20-25 minute mark. introduce the next proposition as something they know but helps organize thoughts.

Proposition: (Congruent iff Same Remainder - CISR) Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder after division by n.

Instructor's Comments: Delay the proof until after they get a chance to use it.

What is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4?

Solution: Notice that

$$6 = 4(1) + 2 \qquad 77 = 19(4) + 1 \qquad 999 = 249(4) + 3$$

Hence, by Congruent if and only if Same Remainder, we have $77 \equiv 1 \pmod 4$ and $999 \equiv 3 \pmod 4$. Thus, by Properties of Congruences,

$$\begin{aligned}
77^{100}(999) - 6^{83} &\equiv (1)^{100}(3) - 2^{83} \pmod 4 \\
&\equiv 3 - 2^2 \cdot 2^{81} \pmod 4 \\
&\equiv 3 - 4 \cdot 2^{81} \pmod 4 \\
&\equiv 3 - 0(2^{81}) \pmod 4 \\
&\equiv 3 \pmod 4
\end{aligned}$$

Once again by Congruent If and only If Same Remainder, 3 is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4. ■

Restating,

Proposition: (Congruent iff Same Remainder - CISR) Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder after division by n.

Proof: By the Division Algorithm, write $a = nq_a + r_a$ and $b = nq_b + r_b$ where $0 \leq r_a, r_b < n$. Subtracting gives

$$a - b = n(q_a - q_b) + r_a - r_b$$

To prove $\Rightarrow$, first assume that $a \equiv b \pmod{n}$, that is $n \mid a - b$. Since $n \mid n(q_a - q_b)$, we have by Divisibility of Integer Combinations that $n \mid (a - b) + n(q_a - q_b)(-1)$ and thus, $n \mid r_a - r_b$. By our restriction on the remainders, we see that the difference is bounded by

$$-n + 1 \leq r_a - r_b \leq n - 1$$

However, only 0 is divisible by n in this range! Since $n \mid (r_a - r_b)$, we must have that $r_a - r_b = 0$. Hence $r_a = r_b$.

$\Leftarrow$ Assume that $r_a = r_b$. Since

$$a - b = n(q_a - q_b) + r_a - r_b = n(q_a - q_b)$$

we see that $n \mid (a - b)$ and hence $a \equiv b \pmod{n}$. ■

Instructor's Comments: This is likely the 50 minute mark. If it isn't get students to work or think about the following problem which you'll take up in the next class.

Question: What is the last digit of $5^{32}3^{10} + 9^{22}$?