MATH6222 Week 7

xarskii

2017-04-20

1 Modular Arithmetic

This is Chapter 7 in textbook.

Problem: Find the last digit of $971^{216} + 523^{121}$

Observation:

- The last digit of $a \times b$ only depends on last digit of a and the last digit of b.
  (So the last digit of 971^{216} is still 1)
  ($3^{121} = 3^{120} \cdot 3 = (3^4)^{30} \cdot 3 = (81)^{30} \cdot 3$. The last digit must be $1 \times 3 = 3$.)
- The last digit of $a + b$ only depends on the last digit of a and b.

Therefore the last digit of the sum is 4.

Definition: Fix a natural number n, called the modulus. We say $a, b \in \mathbb{Z}$ are **congruent modular** n if $n|(a-b)$. Equivalently, we can write, $a = b + kn$ for some $k \in \mathbb{Z}$. We write this as $a \equiv b \mod n$.

Example:

$$\text{mod } 3 : \ldots\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\ldots$$

$\{a \in \mathbb{Z} : a \equiv 0 \mod 3\}$ is the set of all multiples of 3, i.e. $3k$
$\{a \in \mathbb{Z} : a \equiv 1 \mod 3\}$ is the set of all integers of the form $3k + 1$
$\{a \in \mathbb{Z} : a \equiv 2 \mod 3\}$ is the set of all integers of the form $3k + 2$

$a \equiv b \mod 10 \iff a$ and b have same last digit.
Having the same last digit is the same as saying that a and b differ by a multiple of 10?

But, $\{a \in \mathbb{Z} : a \equiv 3 \mod 10\} = \{\dots, -17, -7, 3, 13, 23, \dots\}$ So the previous statement is almost true.

Given $a \in \mathbb{Z}$, the congruence class of a modulo n is

$$\bar{a} = \{x \in \mathbb{Z} : a \equiv x \mod n\}$$

For $\mod 3$,
$\bar{0} = \{\dots, -6, -3, 0, 3, 6, \dots\}$
$\bar{1} = \{\dots, -5, -2, 1, 4, 7, \dots\}$
$\bar{2} = \{\dots, -4, -1, 2, 5, 8, \dots\}$
Actually, $Z = \bar{0} \cup \bar{1} \cup \bar{2}$.

Proposition: Working $\mod n$, there are exactly n distinct congruence classes. And every integer lies in exactly one of these classes.

For $\mod 2, \bar{0}$ is the set of even numbers, $\bar{1}$ is the set of odd numbers. Two congruence classes.
Also, $\bar{0} = \bar{2}$. Same set.

Proof: Observe that $\bar{0}, \bar{1}, \dots, \overline{n-1}$ are clearly distinct congruence classes.
Reason: If $0 \leq i < j \leq n-1$, then $i - j$ can't be divisible by n. (too close to each other)
Every other integer lies in exactly one of these congruence classes ($\mod n$).
Why? Given any integer a, division algorithm tells you that $\exists\, !k, r \in \mathbb{Z}$ such that $a = kn + r$ where $0 \leq r \leq n-1$. And this is the same as $a \equiv r \mod n$. (Note: ! means "unique")

Key Lemma of Modular Arithmetic: If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then

1. $a + b \equiv a' + b' \mod n$
2. $ab \equiv a'b' \mod n$

$\mod 10$: last digit of sum or product only depends on last digits of summands.
$\mod 2$: (oddness/eveness) the parity of sum/product only depends on the parity of inputs.

Proof: $a = a' + kn$ for some $k \in \mathbb{Z}$. $b = b' + ln$ for some $l \in \mathbb{Z}$.

Then $a + b = a' + kn + b' + ln = a' + b' + (k + l)n$. This by definition means $a + b \equiv a' + b' \mod n$.

If we multiple a, b,

$ab = (a' + kn)(b' + ln) = a'b' + n(kb' + la' + kln) \equiv a'b' \mod n$.

We are done.

2 Friday's Lecture

Last time:

$a \equiv b \mod n \iff a = b + kn$ for some $k \in \mathbb{Z}$.

$\overline{a} = \{x \in \mathbb{Z} : x = a \mod n\}$

$\overline{0} = \{kn : k \in \mathbb{Z}\}$

$\overline{1} = \{kn + 1 : k \in \mathbb{Z}\}$

$\overline{2} = \{kn + 2 : k \in \mathbb{Z}\}$

$\overline{n-1} = \{kn + (n-1) : k \in \mathbb{Z}\}$

Every integer is in exactly one of these congruence classes.

For any integer m, $\exists$ unique k, r such that $m = kn + r, 0 \leq r \leq n - 1$.

1. Shallow: we can be clever about "reducing an integer mod n".
2. Deep: addition/multiplication is well-defined on congruence classes, which **means finding the remainder often division by n, or which of these congruence classes it's in.**

Example: Find last digit of $971^{216} + 513^{121}$. I'm asking to reduce this number $\mod 10$.

$971 \equiv 1 \mod 10$

$971^{216} \equiv 1^{216} \mod 10 \equiv 1 \mod 10$

$$\begin{aligned}
523^{121} &\equiv 3^{121} \mod 10 \\
&\equiv (3^4)^{30} \cdot 3 \mod 10 \\
&\equiv 81^{30} \cdot 3 \mod 10 \\
&\equiv 1^{30} \cdot 3 \mod 10 \\
&\equiv 3 \mod 10
\end{aligned}$$

$971^{216} + 523^{121} \equiv 1 + 3 \mod 10 \equiv 4 \mod 10$

Example: Suppose it's 3 o'clock. What time will show on a 12-hour clock after 47^{101} hours.

Reduce $3 + 47^{101} \mod 12$.

$47^{101} \equiv 11^{101} \mod 12$

$11 \equiv -1 \mod 12$ or $11^2 \equiv 121 \equiv 1 \mod 12$
$11^{101} \equiv (-1)^{101} \mod 12 \equiv -1 \mod 12$

Example: $9, 18, \ldots$ the sum of the digits of the multiple of 9 is itself a multiple of 9.

$$\begin{aligned} a_n, a_{n-1}, \ldots, a_1, a_0 &= a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0 \\ &\equiv a_n \times 1^n + a_{n-1} \times n^{n-1} + \cdots + a_1 \times 1 + a_0 \mod 9 \end{aligned}$$

$z_n :=$ set of congruence classes $\mod n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

$\overline{a} + \overline{b} = \overline{a+b}$
$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

$z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$
$\overline{0} = \{3, 6, 9, \ldots\}$
$\overline{1} = \{4, 7, 10, \ldots\}$
$\overline{2} = \{5, 8, 11, \ldots\}$
$\overline{1} + \overline{2} = \overline{0}$

$z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$