CS 30: Discrete Math in CS (Winter 2019): Lecture 7

Date: 14th January, 2019 (Monday)
Topic: Modular Arithmetic and Modular Exponentiation
Disclaimer: These notes have not gone through scrutiny and in all probability contain errors.
Please discuss in Piazza/email errors to deeparnab@dartmouth.edu

---

1 Definition and Basic Operations

1. **Definition.** Given any integer $n > 0$ and another integer a (not necessarily positive), we know (by Problem 3, PSet 1) that there are unique integers q, r such that $a = qn + r$ with $0 \le r < n$. The number r is denoted as $a \bmod n$.

2. **Examples.** For example, $17 \bmod 3$ is 2. This is because $17 = 3 \times 5 + 2$. Similarly, $13 \bmod 5 = 3$. Slightly more interestingly, $-1 \bmod 3 = 2$. This is because $-1 = 3 \times (-1) + 2$. Similarly, $-7 \bmod 5 = 3$ since $-7 = 5 \times (-2) + 3$. ✍

   Exercise: *What is* $30 \bmod 7$*? What is* $-30 \bmod 7$*?*

3. **Notation.** Given two integers a, b, we will often use the notation
$$a \equiv_n b$$
to denote the condition that $a \bmod n = b \bmod n$.

4. **Operations.** The following operations hold for any two integers a, b.

   (a) $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
   (b) $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$
   (c) $a^b \bmod n = (a \bmod n)^b \bmod n$ if $b > 0$.

   Let us first see these with some examples, and then we will see the simple proofs.

   - *Examples*
     - For the addition instance, consider $(17 + 13) \bmod 7$. On the left hand side, the answer is $30 \bmod 7 = 2$.
       On the right hand side, $17 \bmod 7 = 3$ and $13 \bmod 7 = 6$. Thus, $17 \bmod 7 + 13 \bmod 7 = 9$, and therefore, $(17 \bmod 7 + 13 \bmod 7) \bmod 7 = 9 \bmod 7 = 2$.
     - For the multiplication instance, consider $(7 \times 8) \bmod 5$. On the left hand side, the answer is $56 \bmod 5 = 1$.
       On the right hand side, we see $7 \bmod 5 = 2$ and $8 \bmod 5 = 3$. Thus, $(7 \bmod 5) \cdot (8 \bmod 5) = 6$, and thus, $((7 \bmod 5) \cdot (8 \bmod 5)) \bmod 5 = 6 \bmod 5 = 1$.
     - For the powering instance, let's look at three examples.
       * Consider $6^3 \bmod 5$. On the left hand side, it is $216 \bmod 5 = 1$. On the right hand side, we see $(6 \bmod 5)^3 = 1$ and thus $(1 \bmod 5) = 1$ as well.

  - $*$ Let's also look at $7^3 \bmod 5$. On the left hand side (flex your cubing muscles!), we see it is $343 \bmod 5 = 3$. On the right hand side, we see $(7 \bmod 5)^3 = 2^3 = 8$. And thus, $8 \bmod 5 = 3$.
  - $*$ Finally, let us consider another interesting example with the powering formula. Consider $6^3 \bmod 7$. On the one hand it is $216 \bmod 7 = 6$.
    Using the above formula, we see this would be $(6 \bmod 7)^3 \bmod 7$. Now, $6 \bmod 7$ is 6 which is **also** $-1 \bmod 7$. Thus, $(6 \bmod 7)^3 \bmod 7$ is the same as $(-1 \bmod 7)^3 \bmod 7$. Which is $(-1)^3 \bmod 7$ which is the same as $-1 \bmod 7$ which is 6. This is going to be very useful to remember.

- *Proofs*
  - $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
    Proof. Let $a \bmod n$ be r_1 and $b \bmod n$ be r_2. That is, there exist numbers q_1, q_2 such that $a = q_1 n + r_1$ and $b = q_2 n + r_2$, and both $r_1, r_2 < n$. Furthermore, let q_3, r_3 be such that $(r_1 + r_2) = q_3 n + r_3$. Note that q_3 could be 0 or q_3 could be 1 (could it be any larger?) That is, $r_3 = ((a \bmod n) + (b \bmod n)) \bmod n$, that is, the RHS of the above expression.
    Now, $(a+b) = (q_1 + q_2 + q_3)n + r_3$ and thus $(a+b) \bmod n = r_3$. Hence proved. $\square$
  - $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$
    Proof. As before, let $a \bmod n$ be r_1 and $b \bmod n$ be r_2. That is, there exist numbers q_1, q_2 such that $a = q_1 n + r_1$ and $b = q_2 n + r_2$, and both $r_1, r_2 < n$. Furthermore, let q_3, r_3 be such that $r_1 r_2 = q_3 n + r_3$, that is, $r_3 = (r_1 r_2) \bmod n$, that is, the RHS of the above expression. Now,
    $$ab = (q_1 n + r_1) \cdot (q_2 n + r_2) = (q_1 q_2 n + q_1 r_2 + q_2 r_1 + q_3)n + r_3$$
    implying, $ab \bmod n = r_3$. Hence proved. $\square$
  - $a^b \bmod n = (a \bmod n)^b \bmod n$ if $b > 0$.
    Proof. For example, $a^2 \bmod n = (a \cdot a) \bmod n = ((a \bmod n) \cdot (a \bmod n)) \bmod n = (a \bmod n)^2 \bmod n$. $a^3 \bmod n = (a \cdot a^2) \bmod n = \big((a \bmod n) \cdot (a^2 \bmod n)\big) \bmod n = (a \bmod n) \cdot (a \bmod n)^2 \bmod n = (a \bmod n)^3 \bmod n$ $\square$

5. **Ring of Integers.** Note that for any integer a (not necessarily positive), the number $a \bmod n$ is in the set $\{0, 1, 2, \ldots, n-1\}$. This set is often denoted as $\mathbb{Z}_n$.

   For a and b in $\mathbb{Z}_n$ we may use the symbol $+_n$ to denote the operation $a +_n b := (a+b) \bmod n$. Similarly, the symbol $\times_n$ is used to denote the operation $a \times_n b := (a \cdot b) \bmod n$. The above facts about the operations imply for any two numbers in $\mathbb{Z}_n$, $a +_n b$ lies in $\mathbb{Z}_n$ and $a \times_n b$ lies in $\mathbb{Z}_n$. Furthermore, there are two *special* numbers. There is one additive identity, named 0, with the property that $a +_n 0 = a$. There is one multiplicative identity, named 1, with the property that $a \times_n 1 = a$.

   Such sets along with these two operations have a name: they are called *rings*.

2 Modular Exponentiation Algorithm

Suppose we want to figure out what is the remainder when we divide 3^{10} by 7, that is, what is $3^{10} (\bmod 7)$? The hard and often infeasible way would be to compute 3^{10} and then divide by 7 to get the remainder. The above operations allow a much faster way to compute this. Let's first do an example and then give the whole algorithm.

$$
\begin{aligned}
3^{10} \bmod 7 &= (3^2)^5 \bmod 7 && \\
&= 9^5 \bmod 7 && \\
&= (9 \bmod 7)^5 \bmod 7 && \text{Operation (c) above} \\
&= 2^5 \bmod 7 && \text{Progress! From } 3^{10} \text{ we have moved to } 2^5. \\
&= (2 \cdot 2^4) \bmod 7 && \text{Can't halve } 5 \text{ as it is odd.} \\
&= \big((2 \bmod 7) \cdot (2^4 \bmod 7)\big) \bmod 7 && \text{We have again halved the exponent by moving to } 2^2 = 4. \\
&= (2 \cdot (4^2 \bmod 7)) \bmod 7 && \\
&= 4 &&
\end{aligned}
$$

We get 4 when we divide 3^{10} by 7.

The general idea was to keep on reducing the exponent by half by moving to the square, and then replacing the square to a possibly smaller number by taking the $\bmod$ "inside". The full recursive algorithm is shown below.

procedure MODEXP(a, b, n) ▷ Assumes b, n are positive integers.
    ▷ *Returns* $a^b \bmod n$.
    $a \leftarrow a \bmod n$ ▷ We first move a to $a \bmod n$.
    if $b = 1$ **then**:
        return $a \bmod n$.
    if b is even **then**:
        return MODEXP$(a^2 \bmod n, \frac{b}{2}, n)$
    else
        $s =$ MODEXP $(a^2 \bmod n, \frac{b-1}{2}, n)$
        return $(a \cdot s) \bmod n$.

Remark: *The first line ensures $a \in \{0, 1, \ldots, n-1\}$. Note that we compute the mods "brute-force" for $a^2 \bmod n$ and $(a \cdot s) \bmod n$. Both these, that is a^2 and $a \cdot s$, are at most n^2. Thus, to compute $a^b \bmod n$ one only needs to be "divide" numbers as big as n^2 by n.*

Exercise: *Evaluate by hand showing all calculations*

1. $7^{50} (\bmod 15)$.
2. $24^{11} (\bmod 35)$.

Exercise: *Implement the algorithm up in your favorite language.*