CS330 Activities for Lecture 26*

11.1: Modular Arithmetic

- In programming languages, \( x \mod n \) typically yields the remainder of \( x \) after dividing by \( n \).
- **Definition:** In math, \( x \) is congruent to \( y \) modulo \( ("mod") \) \( n \) if they yield the same remainder after dividing by \( n \).
  - Equivalently \( x \) and \( y \) are congruent modulo \( n \) if \( (x - y) \) is a multiple of \( n \).
  - **Notation:** \( x \equiv y \) (mod \( n \)) for congruence, \( n \mid e \) for "\( n \) divides \( e \)". I.e., for some \( k \), we have \( (n-e) = k*n \).
- Note \( x \) and \( y \) don’t have to be nonnegative (but \( n \) is almost always positive).
  - **Examples:** \( 5 \equiv 12 \) (mod 7); \( 5 \equiv -2 \) (mod 7).
- **Addition** and multiplication mod \( n \) are just regular integer addition and multiplication, but restricted to the remainders mod \( n \). **Examples:** \( 5 \times 7 = 35 \equiv 1 \) mod 2; \( 15 \times 6 = 60 \equiv 0 \) mod 10.
- The ring \( \mathbb{Z}_n \) consists of the integers mod \( n \) (= \( \{0, 1, \ldots, n-1\} \)) under addition and multiplication mod \( n \).
  - In math, a ring is a collection of objects and two operations where there are objects that behave like 0 and 1 and the two operations follow rules like \( 0 + x = x, 1 \times x = x, (x+y)z = xz + yz \).
  - All sorts of things that don’t look like numbers still behave like rings. For example, \( n \times n \) matrices of numbers form a ring. (Technically, a non-commutative ring, since matrix multiplication isn’t commutative.) \( \mathbb{Z}_n \) is a commutative ring where congruence serves as equality.
- **Intermediate results:** if \( x \equiv u \) and \( y \equiv w \) (mod \( n \)), then \( x+y \equiv u+w \) (mod \( n \)) and \( x*y \equiv u*w \) (mod \( n \)).
  - These properties are pretty straightforward to prove.
    - If \( x \equiv u \) and \( y \equiv w \) (mod \( n \)), then \( (x-u) = a*n \) and \( (y-w) = b*n \) for some \( a \) and \( b \).
    - For addition, \( (x+y) - (u+w) = (x-u) + (y-w) = a*n + b*n = (a+b)*n \), so \( x+y \equiv u+w \) (mod \( n \)).
    - Multiplication is similar.
- **Subtraction:** \( a - b \equiv c \) (mod \( n \)) if \( a \equiv c + b \) (mod \( n \)). E.g., \( 25 - 17 \equiv 2 \) mod 3 because \( 25 \equiv 1 \) mod 3 and \( 19 \equiv 2+17 \) (mod 3)
  - This also works for negative numbers: \( -1 \equiv 12 \) (mod 13) because \( 13 - 1 = 12 \) (mod 13).
- **Division:** Not all rings support division: We’d like \( a/b \equiv c \) (mod \( n \)) if \( a \equiv b*c \) (mod \( n \)), but this doesn’t always work.
  - E.g., \( 0/2 \) has two values modulo 6: We have \( 0/2 \equiv 0 \) (mod 6) because \( 0 \equiv 2*0 \) (mod 6), but \( 0/2 \) also \( \equiv 3 \) (mod 6) because \( 0 \equiv 2*3 \) (mod 6). On the other hand, \( 3/2 \) is undefined because for \( 3/2 \equiv b \) (mod 6), we need \( 3 \equiv 2*b \) (mod 6), which holds for no \( b \) in the range 0 through 5.
  - If \( n \) is a prime number, then \( \mathbb{Z}_n \) supports a division operation.

**Questions**

1. Without a calculator, calculate \( 8^9 + 12 \) (mod 8). [Hint: Simplify \( 8^8 \) mod 8 before doing the addition.]

2. Without a calculator, calculate \( 2^9 \) (mod 9). [Hint: \( 33 = 32 + 1 \)]

---

* Some material from MATH230 Dr. Robert Ellis IIT-AMAT, zyBooks Disc. Math., and Disc. Math. and its Appl., Rosen (7th Ed.) is included under the academic/nonprofit Fair Use exception of US Copyright Law. This document must NOT be distributed beyond participants in IIT’s CS330.
3. For the ring of $n \times n$ matrices of reals under matrix addition and multiplication, what matrix behaves like zero? What matrix behaves like one?

4. Boolean logic is based on what ring?

5. Write out the addition and multiplication tables modulo 7: One table has $a \in \mathbb{Z}_7$ as row headers, $b \in \mathbb{Z}_7$ as column headers, and each entry contains $a + b \mod 7$. The other table has $a \ast b \mod 7$.

6. (This one will require some work.) Fill out a division table for $a / b \mod 7$ as follows: For row $a$, column $b$, go to the multiplication table mod 7, check the column for $b$ and find the row number containing $a$. That row number is what goes in the entry for $a / b$. 
Some applications for modular arithmetic

Hash tables
- Say we have a set of keys $K$ of size $N$ that we can use as indexes into an array. If $N$ is small, then there’s no problem: Just use an array of length $N$. But if $N$ is large and we’re only using a small number of keys (say $\leq n$), then an array of length $N$ wastes space.
- A hash function maps key values from $K$ into indexes for a hash table, which is an array of length $n$. (So $0 \leq h(k) < n$.) A good hash function has results that look fairly random because that tends to spread the results more evenly across the range.
- A common kind of hash function uses modular arithmetic: For some constant $c$, $h(k) = c*k \mod n$.

Pseudo-random number generators
- A lot of applications rely on access to a set of random numbers. Truly random numbers turn out to be hard to get, plus for debugging it can be nice to run your program multiple times with the same sequence of “random” numbers.
- A pseudo-random number generator is a function that, when called many times, deterministically produces the same sequence of values and the values pass some set of statistical tests for randomness.
- One kind of pseudo-random number generator $X$ takes as parameters the value of $X(0)$ and constants $a$ and $c$ and $m$, with $X(n+1) = a* X(n) + c \mod m$. This produces numbers in the range 0 through $m-1$. (Of course, picking $a$ and $c$ is nontrivial.)

Questions
7. Let $h(k) = 5*k \mod 13$ be hash function. (A toy function, for illustration.) What values do you get for $h(100)$ through $h(105)$? How good of a job does $h$ do at spreading numbers across the range 0 – 12?

8. Repeat the previous question on $h(k) = 25*k \mod 100$. 