AM 106: Applied Algebra **Salil Vadhan**

Lecture Notes 3

September 11, 2018

1 Modular Arithmetic

- **Def:** For integers $a \geq 0$ and $b > 0$, $a \bmod b$ is the remainder when a is divided by b. That is, if we write $a = bq + r$ for integers q and r with $0 \leq r < b$, then $a \bmod b = r$.
- **Proposition:** For integers $a \geq 0$ and $b > 0$, $a \bmod b$ equals the least-significant ("ones") digit of a when written in base b. That is, if $a = a_n a_{n-1} \cdots a_0 = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0$, where $a_i \in \{0, 1, \ldots, b-1\}$, then $a_0 = a \bmod b$.
  - $3457 \bmod 10 =$
  - $22 \bmod 4 =$
- **Q:** What is the relation between $a \bmod b$ and $(-a) \bmod b$?
- **Example:** US Postal Service (USPS) money order check digit scheme
  - Takes a 10-digit *decimal* number a and appends $a \bmod 9$ for the purpose of detecting errors.
  - So $0897136591 \mapsto 08971365914$.
  - Why not mod 10?
- **Homomorphic Properties of Mod (Gallian Exercise 11):** When doing arithmetic modulo n, can take mods first.
  - $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$.
  - $(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$.
  - This is very useful to speed up computations!
  - Example: USPS check-digit $0897136591 \bmod 9 =$.
- USPS check-digit scheme does not detect even all one-digit errors.
  - Why not?
  - How can we modify it to do so?
- This is the simplest example of an *error-correcting code*. Gallian also discusses detecting swaps of consecutive digits. At the end of the course, we will study codes for detecting and correcting many more errors, e.g 30% of the digits of a large piece of data.

2 Relations

- **Def:** A *relation* on a set S is a set of ordered pairs of elements of S, i.e. $R \subseteq S \times S$. $(a, b) \in R$ often denoted aRb.
- **Properties of Relations:**
  - R is *reflexive* if $(a, a) \in R$ for all $a \in S$.
  - R is *symmetric* if $(a, b) \in R \Rightarrow (b, a) \in R$ for all $a, b \in S$.
  - R is *transitive* if $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$ for all $a, b, c \in S$.
  - R is an *equivalence relation* if R is reflexive, symmetric, and transitive.
- **Examples:**
  - $<$ on $\mathbb{Z}$
  - $\leq$ on $\mathbb{Z}$
  - $=$ on $\mathbb{Z}$
  - "is a (full, biological) sibling of" on people.
- If R is an equivalence relation on S and $a \in S$, then the *equivalence class of* a is the set $[a]_R = \{b \in S : (a, b) \in R\}$.
- **Proposition:** If R is an equivalence relation, then its equivalence classes form a partition of S. That is, every element $a \in S$ is in exactly one equivalence class (namely $[a]$).
  Proof: In book.
- **The Congruence Relation:** For $a, b \in \mathbb{Z}$, we define $a \equiv b \pmod{n}$ if $a \bmod n = b \bmod n$. Equivalently, $n|(b - a)$.
  - The congruence relation modulo n is an equivalence relation on integers, and we'll denote the equivalence class of integer a by

    $$[a]_n = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\} = \{\ldots, a - 2n, a - n, a, a + n, a + 2n, \ldots\} = [a \bmod n]_n.$$

    This is known as the *the congruence class of* a *modulo* n.
  - **Q:** How many distinct congruence classes are there modulo n?
  - **Example:** The congruence classes modulo 3 are:

  - We can do arithmetic on the equivalence classes. That is, we can *define* $[a]_n + [b]_n$ to be $[a + b]_n$, and $[a]_n \cdot [b]_n$ to be $[ab]_n$. These are well-defined (i.e. if $[a]_n = [a']_n$ and $[b]_n = [b']_n$, then $[a + b]_n = [a' + b']_n$) by the Homomorphic Properties of Mod.

3 Algorithms

Algorithms — step-by-step procedures for solving problems — have been a part of algebra since its earliest days. In his *Elements* (c. 300 BC), Euclid described the Euclidean algorithm, which remains to this current day (and we'll see it below). The word *algorithm* is derived from the name of the Persian mathematician al-Khwarizmi (c. 780), who is considered one of the founders of algebra and gave the first general methods for solving linear and quadratic equations.

As hinted in the previous lecture, we too will be interested in algorithmic issues. We will not be satisfied to know that certain algebraic objects or solutions to equations exist, but we will want to know whether there are general and efficient methods for constructing them.

A precise mathematical model for what constitutes an algorithm wasn't given until the 1930's in the work of Church and Turing, who used it to show that certain well-defined mathematical problems have no algorithm whatsoever. These mathematical models were a major inspiration for the design of the first general-purpose computers in the 1940's, and have remained relevant to understanding the power of computers even has technology has changed.

It will be too much of a detour for us to discuss these formal models of algorithms. Instead, we will informally introduce some of the basic terminology for discussing and comparing algorithms and give some examples. If you're interested in reading more about algorithms, a standard textbook is Cormen-Leiserson-Rivest-Stein (see syllabus).

3.1 Defining Algorithms

Example: Grade-School Addition. We illustrate the idea of an algorithm with the simple example of grade-school addition, which takes two n-digit numbers $x = x_{n-1} \cdots x_0$ and $y = y_{n-1} \cdots y_0$ (say in base 10) and computes their sum $z = z_n z_{n-1} \cdots z_0$. As we all know, the algorithm computes the digits z_i of the result from the least significant ($i = 0$) to the most significant ($i = 1$), keeping track of carry digits c_i as it goes.

GradeSchoolAddition($x_{n-1} \cdots x_0, y_{n-1} \cdots y_0$):

- Let $c_0 = 0$.
- For $i = 0$ to $n - 1$, let $c_{i+1} z_i$ be the base 10 representation of $x_i + y_i + c_i$.
- Output $c_n z_{n-1} z_{n-2} \cdots z_0$.

In general, an *algorithm* is an unambiguous, "step-by-step" procedure for transforming "inputs" to "outputs". To understand this definition, we need to specify a few things:

- "inputs and outputs": these are taken to be *strings* (finite sequences of symbols) over some fixed, finite *alphabet* of symbols, e.g. $\{0, 1, 2, \ldots, 9\}$, $\{0, 1\}$, $\{a, b, c, \ldots, z\}$.
- "step": operation on individual symbols, e.g. on individual digits.
- Can be made mathematically precise via any one of many equivalent models (Turing Machine, RAM, ...).

Def: Algorithm A *computes* a function f if for every input string x, the output string, denoted $A(x)$, equals $f(x)$.

- The same set of rules should work for *all* possible inputs (infinitely many).
- **Example:** Grade-school addition computes the function $f(x\#y) = z$, where z is the base-10 representation of the sum of the numbers for which x and y are the base-10 representations, and # is an additional alphabet symbol just used to separate the two summands.
- Representation of input and output not too important. Any reasonable representation can be easily converted into any other, e.g. base 10 vs. binary (=base 2) representation.
- Not all well-defined functions have algorithms! For example, there is no algorithm for finding integer solutions to polynomial equations in many variables, e.g. $10wx^2y - 3xz + 2wz^9 - \cdots = 0$ (aka Diophantine Equations). On PS2, you'll see an algorithm for *linear* Diophantine Equations. Computability Theory (covered in cs121) studies which problems have algorithms and which do not.

3.2 Computational Complexity

Some algorithms are better than others (even if they compute the same function). In particular, we prefer algorithms that take fewer steps.

Examples:

- The running time of grade-school addition scales at most linearly with the length of the input, so we say that it runs in time "order n" (written $O(n)$).
- The running time of grade-school multiplication is $O(n^2)$. However, there are more sophisticated algorithms that are asymptotically faster!
- What about exponentiation $f(x, y) = x^y$? For n-digit numbers, this can take time exponential in n, regardless of what algorithm is used.
- But modular exponentiation $f(x, y) = x^y \bmod z$ can be computed in time $O(n^3)$ for n-digit numbers. (Hint: if $y = y_{n-1}y_{n-2}\cdots y_0$ is the binary representation of y, then $x^y = \prod_{i=0}^{n-1} \left(x^{2^i}\right)^{y_i}$.)