Lecture 5: Finite Fields (PART 2)

PART 2: Modular Arithmetic

Theoretical Underpinnings of Modern Cryptography

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

February 15, 2017
2:27am

Goals:

- To review modular arithmetic
- To present Euclid's GCD algorithms
- To present the prime finite field Z_p
- To show how Euclid's GCD algorithm can be extended to find multiplicative inverses
- **Perl and Python implementations for calculating GCD and multiplicative inverses**

CONTENTS

5.1: MODULAR ARITHMETIC NOTATION

- Given **any** integer a and a **positive** integer n, and given a division of a by n that leaves the remainder between 0 and $n-1$, both inclusive, we define

$$a \; mod \; n$$

to be **the remainder**. Note that the remainder **must** be between 0 and $n-1$, both ends inclusive, even if that means that we must use a negative quotient when dividing a by n.

- We will call two integers a and b to be **congruent modulo** n if

$$a \; mod \; n \quad = \quad b \; mod \; n$$

- Symbolically, we will express such a **congruence** by

$$a \quad \equiv \quad b \pmod{n}$$

- Informally, a congruence may also be displayed as:

$$a \;=\; b \;\; (\text{mod } n)$$

and even

$$a \;=\; b \;\; \text{mod } n$$

as long as it is understood that we are talking about a and b being equal only in the sense that their remainders obtained by subjecting them to modulo n division are exactly the same.

- We say a non-zero integer a is a **divisor** of another integer b provided the remainder is zero when we divide b by a. That is, when $b = ma$ for some integer m.

- When a is a divisor of b, we express this fact by $a \mid b$.

5.1.1: Examples of Congruences

- Here are some congruences modulo 3:

$$\begin{aligned} 7 &\equiv 1 \pmod 3 \\ -8 &\equiv 1 \pmod 3 \\ -2 &\equiv 1 \pmod 3 \\ 7 &\equiv -8 \pmod 3 \\ -2 &\equiv 7 \pmod 3 \end{aligned}$$

- One way of seeing the above congruences (for mod 3 arithmetic):

```
... 0  1  2  0  1  2  0  1  2  0  1  2  0  1  2  0  1  2  0  1  2  0  ...
...- 9 -8 -7 -6 -5 -4 -3 -2 -1  0  1  2  3  4  5  6  7  8  9  10 11 12 ...
```

  where the top line is the output of **modulo 3** arithmetic and the bottom line the set of **all** integers. [The top entry in each column is the modulo 3 value of the bottom entry in the same column. Pause for a moment and think about the fact that whereas $(7 \ mod \ 3) = 1$ on the positive side of the integers, on the negative side we have $(-7 \ mod \ 3) = 2$.]

- As you can see, the **modulo n** arithmetic maps all integers into the set $\{0, 1, 2, 3, ..., n-1\}$.