AM 106/206: Applied Algebra	**Prof. Salil Vadhan**
Lecture Notes 2	
	September 8, 2010

1 Divisibility

- Reading: Gallian Chapter 0.
- **Thm 0.1 ("Division Algorithm"):** For $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique integers q and r with $0 \le r < b$ such that $a = qb + r$.
  Proof:

- **Algorithmic Note:** Despite its name, the theorem statement does not provide an "algorithm." Even though it tells us that q and r exist, it does not tell us how to compute them given a and b. However, in the proof, there is an implicit, but inefficient, algorithm. What is it?
- **Def:** We say that integer b *divides* integer a (written $b|a$) if $a = qb$ for some integer q.
  - **Q:** Which integers divide all integers?
  - **Q:** Which integers are divisible by all integers?
- **Def:** For two integers that are not both zero, their *greatest common divisor* $\gcd(a, b)$ is the largest integer d such that $d|a$ and $d|b$. If $\gcd(a, b) = 1$, we say that a and b are *relatively prime.*
- **Thm 0.2 (GCD is a Linear Combination):** For two integers a, b not both zero, $\gcd(a, b) = as + bt$ for some integers s, t. Moreover, $\gcd(a, b)$ is the smallest positive integer of this form.
  Example: $\gcd(10, 24) =$

  Proof:

- **Algorithmic Note:** Like with the Division Algorithm, the statement Thm 0.2 does not tell us how to compute the integers s and t, but there is an algorithm implicit in the proof.

- **Corollary:** if integers a and b are relatively prime, then there exist integers s and t such that $as + bt = 1$.
  Example: $\gcd(11, 15) =$

2 Primes and Factorization

- **Def:** An integer n is *prime* if $n \notin \{0, \pm 1\}$ and the only divisors of n are ± 1 and $\pm n$.
  - $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11 \ldots$.
  - Unlike Gallian we allow negative numbers to be prime.
- **Euclid's Lemma:** If p is a prime and a, b are integers such that $p|ab$, then $p|a$ or $p|b$.
  Proof:
- **Fundamental Thm of Arithmetic:** Every integer n other than 0 and ± 1 can be written as the product of primes $n = p_1 p_2 \cdots p_r$. Moreover, this factorization is unique up to the order of the p_i's and their signs. That is, if $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ where the p_i's and q_i's are primes, then $r = s$ and there is a permutation $\pi : \{1, \ldots, r\} \to \{1, \ldots, s\}$ such that $p_i = \pm q_{\pi(i)}$ for all i.
  Proof:

3 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.