CS1231 Part 5 - Number Theory, Continued

Based on lectures by Terence Sim and Aaron Tan
Notes taken by Andrew Tan
AY18/19 Semester 1

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

1 Well Ordering Principle

The **Well Ordering Principle** states that if a non-empty set $S \subseteq \mathbb{Z}$ has a *lower bound*, then S has a least element.

Furthermore, it also states that if a non-empty set $S \subseteq \mathbb{Z}$ has an upper bound, then S has a greatest element.

2 Quotient-Remainder Theorem

Given any integer a and any positive integer b, there exist unique integers q and r such that:

$$a = bq + r \text{ and } 0 \leq r < b$$

The integer q is called the quotient, and the integer r is called the remainder.

The Quotient-Remainder Theorem provides the basis for writing an integer n as a sequence of digits in a base b.

3 Greatest Common Divisor

Let a and b be integers, not both zero. The **greatest common divisor** of a and b, denoted $gcd(a, b)$, is the integer d satisfying:

1. $d \mid a$ and $d \mid b$
2. $\forall c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$ then $c \leq d$

3.1 Euclid's algorithm

Euclid's algorithm is an efficient algorithm that computes the greatest common divisor between two integers.

```
function gcd(a, b):
  while b > 0:
    c = a%b
    (a, b) = (b, c)
  return a
```

3.2 Extended Euclidean Algorithm

Bézout's identity: Let a, b be integers, not both zero, and let $d = gcd(a, b)$. Then there exist integers x, y such that:

$$ax + by = d$$

Basically, the gcd of two integers is some linear combination of those numbers.
With this identity, we can sketch a proof for the Extended Euclidean Algorithm:

1. Trace the execution of Euclid's algorithm on a,b.
2. The last line gives us the gcd d.
3. Work backwards to express d in terms of linear combinations of the quotients and remainders of the previous lines, until we reach the top.

4 Modulo Arithmetic

Let m and n be integers, and let d be a positive integer. We say that m is **congruent** to n **modulo** d, and write:

$$m \equiv n \pmod d$$

if, and only if,

$$d \mid (m - n)$$

4.1 Arithmetic

Given integers a, b, c, d, and n where $n > 1$, and

$$a \equiv c \pmod n \text{ and } b \equiv d \pmod n,$$

then

1. $(a + b) \equiv (c + d) \pmod n$
2. $(a - b) \equiv (c - d) \pmod n$
3. $ab \equiv cd \pmod n$
4. $a^m \equiv c^m \pmod n$, for all positive integers m

We can extend part 3 as such:

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod n$$

Furthermore, if m is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod n$$

4.2 Inverses

For any integers a, n with $n > 1$, if an integer s is such that $as \equiv 1 \pmod n$, then s is called the **multiplicative inverse of a modulo n**. We may write the inverse as a^{-1}.

The commutative law still applies in modulo arithmetic, so $a^{-1-}a \equiv 1 \pmod n$

A Definitions

Definition 4.3.1 (Lower Bound) An integer b is said to be a lower bound for a set $X \subseteq \mathbb{Z}$ if $b \leq x$ for all $x \in X$

Definition 4.5.1 (Greatest Common Divisor) Let a and b be integers, not both zero. The greatest common divisor of a and b, denoted $gcd(a, b)$, is the integer d satisfying:

(i) $d \mid a$ and $d \mid b$

(ii) $\forall c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$ then $c \leq d$.

Definition 4.5.4 (Relatively Prime) Integers a and b are relatively prime (or coprime) if and only if $\gcd(a, b) = 1$

Definition 4.6.1 (Least Common Multiple) For any non-zero integers a, b, their least common multiple, denoted $lcm(a, b)$, is the positive integer m such that:

(i) $a \mid m$ and $b \mid m$

(ii) for all positive integers c, if $a \mid c$ and $b \mid c$, then $m \leq c$

Definition 4.7.1 (Congruence modulo) Let m and n be integers, and d be a positive integer. We say that m is congruent to n modulo d, and write $m \equiv n \pmod{d} \iff d \mid (m - n)$

Definition 4.7.2 (Multiplicative inverse modulo n) For any integers a, n with $n > 1$, if an integer s is such that $as \equiv 1 \pmod{n}$, then s is called the multiplicative inverse of a modulo n. We may write the inverse as a^{-1}.

B Theorems

Theorem 4.3.2 (Well Ordering Principle) If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then S has a least element. Furthermore, if S has an upper bound, then S has a greatest element

Theorem 4.4.1 (Quotient-Remainder Theorem) Given any integer a and any positive integer b, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$

Theorem 4.5.3 (Bézout's identity) Let a, b be integers, not both zero, and let $d = gcd(a, b)$. Then there exist integers x, y such that $ax + by = d$)

Theorem 4.7.3 (Existence of multiplicative inverse) For any integer a, its multiplicative inverse modulo n (where $n > 1$), a^{-1}, exists if, and only if, a and n are coprime.
$\rightarrow$ Corollary 4.7.4 If $n = p$ is a prime number, then all integers a in the range $0 < a < p$ have multiplicative inverses modulo p

Theorem 8.4.1 Epp (Modular Equivalences) Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent:

(a) $n \mid (a - b)$

(b) $a \equiv b \pmod{n}$

(c) $a = b + kn$ for some integer k

(d) a and b have the same (non-negative) remainder when divided by n

(e) $a \bmod n = b \bmod n$

Theorem 8.4.3 Epp (Modulo Arithmetic) Let a, b, c, d, and n be integers with $n > 1$, and suppose:

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}.$$

Then

(a) $(a + b) \equiv (c + d) \pmod{n}$

(b) $(a - b) \equiv (c - d) \pmod{n}$

(c) $ab \equiv cd \pmod{n}$

(d) $a^m \equiv c^m \pmod{n}$, for all positive integers m

→ Corollary 8.4.4 Epp -

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n}$$

In particular, if m is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}$$

Theorem 8.4.9 Epp - For all integers a, b, c, n with $n > 1$ and a and n are coprime, if $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$

C Propositions

Proposition 4.3.3 (Uniqueness of least element) If a set S of integers has a least element, then the least element is unique.

Proposition 4.3.4 (Uniqueness of greatest element) if a set S of integers has a greatest element, then the greatest element is unique.

Proposition 4.5.2 (Existence of gcd) For any integers a, b, not both zero, their gcd exists and is unique.

Proposition 4.5.5 - For any integers a, b, not both zero, if c is a common divisor of a and b, then $c \mid \gcd(a, b)$