EECS 203
Review for Midterm 3
Statement of Theorems and Definitions

- **Definition** *A partial ordering on a set A is a reflexive,* **antisymmetric**, *and transitive relation on A.*
- **Definition** *Let $(A, \sqsubseteq)$ be a poset and $S \subseteq A$. An element $m \in S$ is the greatest element of S if $(\forall s \in S)(s \sqsubseteq m)$. An element $m \in S$ is the least element of S if $(\forall s \in S)(m \sqsubseteq s)$.*
- **Definition** *An element $m \in S$ is a maximal element of S if there is no other element $s \in S$ with $m \sqsubseteq s$. An element $m \in S$ is a minimal element of S if there is no other element $s \in S$ with $s \sqsubseteq m$.*
- Given a poset $(A, \sqsubseteq)$ and a subset S of A, we want to look at the elements of A which are "above" and "below" all elements of S.
- **Definition** *We define the set $ub(S)$ of upper bounds of S as $\{x \in A \mid (\forall s \in S)(s \sqsubseteq x)\}$. The set $lb(S)$ of lower bounds of S is $\{x \in A \mid (\forall s \in S)(x \sqsubseteq s)\}$.*
- In the picture, $ub(S)$
- **Definition** *If the subset $ub(S)$ has itself a least element, this is called the least upper bound of S. Furthermore, if the set $lb(S)$ has a greatest element, this is called the greatest lower bound of S.*

- **Definition** *A poset* $(A, \sqsubseteq)$ *is called a lattice if any two element subset* $\{x, y\}$ *of* A *has a least upper bound and a greatest lower bound. These are denoted* $x \sqcup y$ *and* $x \sqcap y$ *respectively.*

- **Theorem (Fundamental Theorem of Arithmetic.)** *Every positive integer* m *has a unique factorization into primes of the form*

$$m = p_1^{j_1} \cdot p_2^{j_2} \ldots$$

where $p_1 = 2, p_2 = 3, \ldots$ *are the prime numbers in order, and* j_i *is the number of times the prime* p_i *divides* m*.*

- This gives rise to a function

$$f(m, i) = \text{ the number of times the prime } p_i \text{ divides } m.$$

- **Proposition**

$$m \mid n \iff (\forall i)(f(m, i) \leq f(n, i)).$$

- From this, it follows that

$$f(lcm(m, n), i) = \max\{f(m, i), f(n, i)\}$$

and

$$f(gcd(m, n), i) = \min\{f(m, i), f(n, i)\}.$$

This proves that the poset $(\mathbb{N}, |)$ is a lattice.

- **Theorem (Division Theorem.)** *Let* n *be a fixed integer* ≥ 2*. For any* $z \in \mathbb{Z}$ *we can find unique integers* q, r *such that*

$$z = qn + r \text{ where } 0 \leq r \leq n - 1.$$

- **Definition** *Two integers x and y are congruent mod n, where $n > 0$, if $x - y$ is a multiple of n.*
- **Theorem** *For any integers x and y, $x \equiv y \pmod{n}$ if and only if $x \bmod n = y \bmod n$.*
- **Proposition** *If $a \equiv b$ and $c \equiv d \pmod{n}$ then (1) $a + c \equiv b + d$ and (2) $ac \equiv bd \pmod{n}$.*
- **Definition** *Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. For $a, b \in \mathbb{Z}_n$ define*

  $$a \oplus_n b = (a + b) \bmod n$$

  and

  $$a \otimes b = ab \bmod n.$$

- **Euclid's algorithm**:

```
function gcd(m:ℕ⁺; n:ℕ);
{
(a, b) := (m, n);
while b != 0 do % gcd(a,b) = gcd(m,n)
(a,b) := (b, a mod b);
gcd(m,n) := a
}
```

- Toward correctness of Euclid:

  Lemma *For any x, y:*

  $$\gcd(x, y) = \gcd(y, x \bmod y).$$

- **Theorem** **(Lamé)**. *For any $k \geq 1$, if Euclid's algorithm takes k trips to compute $\gcd(m, n)$, where $m \geq n$, then $n \geq f_{k+1}$.*

- **Definition** *Consider the congruence*

$$mx \equiv 1 \bmod n.$$

An x that satisfies this congruence is called a multiplicative inverse of m modulo n.

- **Theorem** *For non-negative integers m and n, there are "integer coefficients" s and t such that*

$$\gcd(m, n) = sm + tn.$$

- **Corollary** *When m and n are relatively prime, there is always a solution x to $mx \equiv 1 \pmod{n}$.*

- **Extended Euclid's Algorithm:**

```
procedure egcd(m:ℕ⁺; n:ℕ);
{
if n = 0 return (m,1,0);
else { (d', s', t') := egcd(n, m mod n);
(d, s, t) := (d', t', s' - t'* (m div n));
return (d,s,t);}
}
```

- **Theorem** **(Chinese Remainder Theorem.)** *Given moduli $m_1, \ldots, m_k$ relatively prime in pairs, let M be the product $m_1 \cdot \cdots \cdot m_k$. Then for given*

$a_1, \ldots, a_k$ *there is a unique* x *in* $\mathbb{Z}_M$ *such that*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

- **Theorem** **(Fermat's Little Theorem.)** *Let* p *be a prime number and* a *be a positive integer such that* p *does not divide* a*. Then* $a^{p-1} \equiv 1 \bmod p$*.*
- The RSA encryption and decryption functions are inverses of each other. That is, $d(e(M)) = M$, where

$$e(M) = M^e \bmod pq, \text{ and } d(C) = C^s \bmod pq,$$

where s is an inverse of e modulo $(p-1)(q-1)$.