Math 347, Part III Review and Practice Problems

Review all homework problems.

Chapter 6, Divisibility

- Use Euclidean algorithm to find the gcd(a, b), and find all integer solutions for the Diophantine equation, $ax + by = \gcd(a, b)$.

- Property on relatively prime numbers. Positive integers a and b are relatively prime, i.e. $gcd(a, b) = 1$ if and only if there exist integers m and n such that
$$ma + nb = 1.$$
Or equivalently, a and b have distinct prime factorizations.

  Theorem: Suppose that a and b are relatively prime. Then $a|m$ and $b|m$ imply $ab|m$.

  Theorem: Suppose that a and b are relatively prime. If $a|bq$, then $a|q$.

- Given positive integers a and b, then we have an integer solution for Diophantine equation
$$ma + nb = c$$
if and only if c is a multiple of $d = gcd(a, b)$.

  Find the integer solutions, or nonnegative integer solutions of such equations.
Example: Find all integer solutions, or positive integer solutions of
$$12n + 15m = 24.$$
(Remark: Reduce to the case $4n + 5m = 8$).

- Prime Factorization Theorem: $n = p_1^{l_1} \cdots p_k^{l_k}$. Applications

Chapter 7, Modular Arithmetic

- Congruence: $x \equiv y \bmod n$ if $x - y = kn$ for some $k \in \mathbb{Z}$. We let
$$\bar{x} = \{y \in \mathbb{Z}; y \equiv x \bmod n\} = \{y = x + kn, k \in \mathbb{Z}_n\}$$
denote the set of all integers congruence to x. Then $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ has
  - •a natural addition $\bar{x} + \bar{y} = \overline{x+y}$, and
  - a natural multiplication $\bar{x} \cdot \bar{y} = \overline{xy}$.
  - This can be used to help finding the remainders:

  Example: Find the remainder of 4^{100} mod 7 and find the remainder of 5^{100} mod 7.

  Let n be a positive integer. Then for $\bar{a} \neq \bar{0}$ in $\mathbb{Z}_n$, consdier the map $f_{\bar{a}}(\overline{x}) = \overline{ax}$ on $\mathbb{Z}_n$.

- **Theorem:** Let $\bar{a} \neq \bar{0}$ in $\mathbb{Z}_n$. The map $f_{\bar{a}}(\overline{x}) = \overline{ax}$ is a bijection on Z_n if and only if a and n are relatively prime.

  In particular, if $n = p$ is a prime number, then for any $\bar{a} \neq \bar{0}$ in Z_p, the map $f_a(\bar{x}) = \overline{ax}$ is a bijection on Z_p.
  Find the functional digraph of f_3 and f_5 on Z_{11}.
  Find the order and the inverse of $\bar{3}$ and $\bar{5}$ in Z_{11}.

- **Fermat's Little Theorem:** Let p be a prime number and $\bar{a} \neq \bar{0}$. Then $\bar{a}^{p-1} = \bar{1}$.

- **Theorem:** For general $n \in \mathbb{N}$, the congruence equation $\bar{a} \cdot \bar{x} = \bar{b}$ has a solution if and only if $d = \gcd(a, n)|b$.

- **Chinese Remainder Problems:** Let $n_1, n_2, \cdots, n_r$ be a selection of pairwise relatively prime positive integers and let $N = n_1 \cdots n_r$. Then the integer solutions of the congruence systems
$$x \equiv a_1 \mod n_1, \ \cdots, x \equiv a_r \mod n_r$$
are given by
$$x = a_1 N_1 y_1 + \cdots a_r N_r y_r + kN \quad (\text{with } k \in \mathbb{Z}),$$
where $N_i = N/n_i$, and y_i are the inverse of N_i mod n_i.

- **Remark:** For any positive integer n, $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring, which contains n-elements.
  If $n = p$ is a prime number, then for any $\bar{a} \neq \bar{0}$, there exists a unique $\bar{x} \in \mathbb{Z}_p$ such that $\bar{a} \cdot \bar{x} = \bar{1}$. Therefore, $(\mathbb{Z}_n, +, \cdot)$ is a commutative field and for any $\bar{b} \in \mathbb{Z}_p$, there exists a **unique solution**
$$\bar{a} \cdot \bar{x} = \bar{b}.$$