Math 445 Number Theory

Introduction/Review of concepts from abstract algebra

An integer \( p \) is prime if whenever \( p = ab \) with \( a, b \in \mathbb{Z} \), either \( a = \pm n \) or \( b = \pm n \).

[For sanity’s sake, we will take the position that primes should also be \( \geq 2 \).]

**Fundamental Theorem of Arithmetic:** Every integer \( n \geq 2 \) can be expressed as a product of primes: \( n = p_1 \cdots p_k \).

If we insist that the primes are written in increasing order, \( p_1 \leq \ldots \leq p_k \), then this representation is unique.

**The Division Algorithm:** For any integers \( n \geq 0 \) and \( m > 0 \), there are unique integers \( q \) and \( r \) with \( n = mq + r \) and \( 0 \leq r \leq m - 1 \).

[Note: this is also true for any integers \( n, m \) with \( m \neq 0 \), although you need to replace “\( m - 1 \)” with “\( |m - 1| \)” .]

The basic idea: keep repeatedly subtracting \( m \) from \( n \) until what’s left is less than \( m \).

Notation: \( b|a = “b \text{ divides } a” \) = “\( b \) is a divisor of \( a” \) = “\( a \) is a multiple of \( b” \), means \( a = bk \) for some integer \( k \).

If \( b|a \) and \( a \neq 0 \), then \( |b| \leq |a| \).

If \( a|b \) and \( b|c \), then \( a|c \)

If \( a|c \) and \( b|d \), then \( ab|cd \)

If \( p \) is prime and \( p|ab \), then either \( p|a \) or \( p|b \)

Notation: \( (a, b) = \gcd(a, b) \) = greatest common divisor of \( a \) and \( b \)

Different, equivalent, formulations for \( d = (a, b) \):

(1) \( d|a \) and \( d|b \), and if \( c|a \) and \( c|b \), then \( c \leq d \).

(2) \( d \) is the smallest positive number that can be written as \( d = ax + by \) with \( a, b \in \mathbb{Z} \).

(3) \( d|a \) and \( d|b \), and if \( c|a \) and \( c|b \), then \( c|d \).

(4) \( d \) is the only divisor of \( a \) and \( b \) that can be expressed as \( d = ax + by \) with \( a, b \in \mathbb{Z} \).

If \( c|a \) and \( c|b \), then \( c|(a, b) \)

If \( c|ab \) and \( (c, a) = 1 \), then \( c|b \)

If \( a|c \) and \( b|c \), and \( (a, b) = 1 \), then \( ab|c \)

If \( a = bq + r \), then \( (a, b) = (b, r) \)

**Euclidean Algorithm:** This last fact gives us a way to compute \( (a, b) \), using the division algorithm:

Starting with \( a > b \), compute \( a = bq_1 + r_1 \), so \( (a, b) = (b, r_1) \). Then compute \( b = r_1q_2 + r_2 \), and repeat: \( r_{i-1} = r_1q_{i+1} + r_{i+1} \). Continue until \( r_{n+1} = 0 \), then \( (a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_n, r_{n+1}) = (r_n, 0) = r_n \).

Since \( b > r_1 > r_2 > r_3 > \ldots \), this process must end, by well-orderedness.

We can reverse these calculations to recover \( (a, b) = ax + by \), by rewriting each equation in our algorithm as \( r_{i+1} = r_i - r_iq_{i+1} \) and then repeatedly substituting the higher equations into the lowest one, in turn, working up through the list of equations.
**Congruence modulo** $n$: Notation: $a \equiv b \pmod{n}$ (also written $a \equiv b \pmod{n}$) means $n|(b-a)$

Equivalently: the division algorithm will give the same remainder for $a$ and $b$ when you divide by $n$.

Congruence mod $n$ is an equivalence relation.

The congruence class of $a \pmod{n}$ is the collection of all integers congruent mod $n$ to $a$:

$[a]_n = \{ b \in \mathbb{Z} : a \equiv b \pmod{n} \} = \{ b \in \mathbb{Z} : n|(b-a) \}.$

**Fermat’s Little Theorem.** If $p$ is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$

Because: $(a\cdot 1)(a\cdot 2)(a\cdot 3)\cdots(a\cdot (p-1)) \equiv 1\cdot 2\cdot 3\cdots (p-1) \pmod{p}$, and $(1\cdot 2\cdot 3\cdots (p-1), p) = 1$.

Same idea, looking at the $a$’s between 1 and $n-1$ that are relatively prime to $n$ (and letting $\phi(n)$ be the number of them), gives

If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}.$

If the prime factorization of $n$ is $p_1^{a_1} \cdots p_k^{a_k}$, then $\phi(n) = [p_1^{a_1}(p_1 - 1)]\cdots[p_k^{a_k}(p_k - 1)].$

The integers $\mathbb{Z}$, the integers mod $n \mathbb{Z}_n$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$ are all rings.

A homomorphism is a function $\varphi : R \to S$ from a ring $R$ to a ring $S$ satisfying:

for any $r, r' \in R$, $\varphi(r+r') = \varphi(r)+\varphi(r')$ and $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r').$

The basic idea is that it is a function that “behaves well” with respect to addition and multiplication.

An isomorphism is a homomorphism that is both one-to-one and onto. If there is an isomorphism from $R$ to $S$, we say that $R$ and $S$ are isomorphic, and write $R \cong S$.

Example: if $(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. The isomorphism is given by

$\varphi([x]_{mn}) = ([x]_m, [x]_n)$

The main ingredients in the proof:

If $\varphi : R \to S$ and $\psi : R \to T$ are ring homomorphisms, then the function $\omega : R \to S \times T$ given by $\omega(r) = (\varphi(r), \psi(r))$ is also a homomorphism.

If $m|n$, then the function $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $\varphi([x]_n) = [x]_m$ is a homomorphism.

Together, these give that the function we want above is a homomorphism. The fact that $(m, n) = 1$ implies that $\varphi$ is one-to-one; then the Pigeonhole Principle implies that it is also onto!

The above isomorphism and induction imply that if $n_1, \ldots n_k$ are pairwise relatively prime (i.e., if $i \neq j$ then $(n_i, n_j) = 1$), then

$\mathbb{Z}_{n_1 \cdots n_k} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. This implies:

**The Chinese Remainder Theorem:** If $n_1, \ldots n_k$ are pairwise relatively prime, then for any $a_1, \ldots a_k \in \mathbb{N}$ the system of equations

$x \equiv a_i \pmod{n_i}$, $i = 1, \ldots k$

has a solution, and any two solutions are congruent modulo $n_1 \cdots n_k$.

A solution can be found by (inductively) replacing a pair of equations $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$, with a single equation $x \equiv c \pmod{mn}$, by solving the equation $a + nk = x = b + mj$ for $k$ and $j$, using the Euclidean Algorithm.