MATH 436: Homework II.
Due in class on Friday, Sep 26

1. Let $d \geq 1$ be an integer. Recall that $\mathbb{Z}/d\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, d\bar{-}1\}$ becomes an Abelian group under the addition $+$ inherited from $\mathbb{Z}$ and an Abelian monoid under the multiplication $\cdot$ inherited from $\mathbb{Z}$. Let $(\mathbb{Z}/d\mathbb{Z})^*$ be the group of units in $(\mathbb{Z}/d\mathbb{Z}, \cdot)$.
(a) Show that for $n \in \mathbb{Z}$, $\bar{n}$ is a unit in $\mathbb{Z}/d\mathbb{Z}$ if and only if $gcd(n, d) = 1$. (Comment: We say n and d are relatively prime whenever $gcd(n, d) = 1$.) [Hint: Use the result on gcd's obtained in Homework I].
(b) Recall that a prime number is an integer $p > 1$ such that the only positive integer divisors of p are 1 and p itself. Show that for p a prime, every nonzero residue $\bar{n} \neq \bar{0}$ is a unit. Conclude that $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$.

2. [**Wilson's Theorem**] In general if we have integers x, y such that $\bar{x} = \bar{y}$ in $\mathbb{Z}/n\mathbb{Z}$ we say that x and y are congruent modulo n and write $x \equiv y \bmod n$.
Recall that any nonzero integer can be written UNIQUELY in the form $\pm p_1^{n_1} \ldots p_k^{n_k}$ where the p_j are distinct primes and $n_j \geq 1$. A consequence of this is that if a prime p divides nm then p either divides n or m or both. You may use these facts freely in the Homework, we will prove these as general consequences of more general theorems later on but elementary proofs can also be found in many algebra books.
(a) Let p be a prime and x an integer. Show that $x^2 \equiv 1 \bmod p$ implies that $x \equiv \pm 1 \bmod p$.
(b) If $(A, \star)$ is a finite Abelian group we may define $\prod_{a \in A} a$. Thus if $A = \{a_1, \ldots, a_n\}$ where a_j are distinct then $\prod_{a \in A} a = a_1 \star \cdots \star a_n$. (Note we can only use this notation as the order of the elements is not important since A is Abelian.) Let $I = \{a \in A | a^2 = e\}$, be the set of "involutions" in A.
Show that $\prod_{a \in A} a = \prod_{a \in I} a$ for all finite Abelian groups A.
(c) Apply (b) to $(\mathbb{Z}/p\mathbb{Z})^*$ to prove Wilson's Theorem which states that
$(p-1)! \equiv -1 \bmod p$ for all primes p.

3. [**Fermat's Little Theorem**] (a) Explain briefly using Lagrange's Theorem relating the order of a group and its subgroups why in a finite group G we have $x^{|G|} = e$ for all $x \in G$.
(b) Prove Fermat's Little Theorem:
If p is a prime then $n^{p-1} \equiv 1$ mod p for all integers n which are not divisible by p. Also $n^p \equiv n$ mod p for all integers n.

4. [**Mobius Inversion Theorem**] Let $\mathbb{N}^+ = \{1, 2, 3, \dots\}$ be the set of positive integers. It is a semigroup under $+$ and a monoid under $\cdot$. Let $\mathbb{C}$ be the complex numbers. For positive integers d, n we say d divides n and write $d|n$ when $\frac{n}{d} \in \mathbb{Z}$. We define $A = \{f : \mathbb{N}^+ \to \mathbb{C}\}$ to be the set of "arithmetic functions". We define a convolution $\star$ on A via $(f \star g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$ for all $n \in \mathbb{N}^+$. Here the sum is over all positive integer divisors of n.
(a)Show that $(A, \star)$ is an Abelian monoid with identity δ given by

$$\delta(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ otherwise.} \end{cases}$$

(b) Define $\mathbb{I} \in A$ by $\mathbb{I}(n) = 1$ for all $n \in \mathbb{N}^+$. Define $\tau \in A$ by $\tau(n) =$(number of positive divisors of n) for all $n \in \mathbb{N}^+$. Show that $\tau = \mathbb{I} \star \mathbb{I}$.
(c) Define the Mobius function $\mu \in A$ by considering the prime factorization of a number n, $n = p_1^{n_1} \dots p_k^{n_k}$ where $p_1, \dots, p_k$ are distinct primes. We say that n is squarefree if each $n_j \leq 1$, i.e., no prime occurs more than once in the factorization. In general we let $l(n)$ denote the number of distinct primes occuring in the factorization of n. Then

$$\mu(n) = \begin{cases} (-1)^{l(n)} \text{ if } n \text{ is squarefree,} \\ 0 \text{ otherwise.} \end{cases}$$

Show that $\mathbb{I} \star \mu = \delta$.
(d) Use your previous results to prove the Mobius Inversion Theorem:

$$F(n) = \sum_{d|n} f(d) \text{ for all } n \in \mathbb{N}^+$$

if and only if

$$f(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d) \text{ for all } n \in \mathbb{N}^+.$$

5. [**Primitive nth roots of unity**] In the complex numbers $\mathbb{C}$, for $n \geq 1$, define U_n to be the set of nth roots of unity, i.e., $U_n = \{z \in \mathbb{C} | z^n = 1\} = \{e^{\frac{2\pi ik}{n}} | 1 \leq k \leq n\}$. Among these are the subset of primitive nth roots of unity P_n, i.e, $P_n = \{z \in \mathbb{C} | z^n = 1, z^k \neq 1 \text{ for } 1 \leq k < n\}$.
(a) Show that U_n is partitioned into the sets $\{P_d | d \in \mathbb{N}^+ \text{ such that } d|n\}$ and conclude that $|P(n)| = \sum_{d|n} \mu(\frac{n}{d}) d$.
(b) Note U_n is a group under complex multiplication. Define $\theta : (\mathbb{Z}, +) \to$

$(U_n, \cdot)$ via $\theta(k) = e^{\frac{2\pi ik}{n}}$ for all $k \in \mathbb{Z}$. Show that θ is an epimorphism with kernel $n\mathbb{Z}$ and hence conclude that $(\mathbb{Z}/n\mathbb{Z}, +) \cong (U_n, \cdot)$.
(c) Let $\hat{\theta} : \mathbb{Z}/n\mathbb{Z} \to U_n$ be the isomorphism induced by the map θ in (b). Show that $\hat{\theta}^{-1}(P_n) = \{\bar{k} | gcd(k, n) = 1\}$ and conclude that $|P_n| = \phi(n)$ where ϕ is Euler's phi function. Thus $\phi(n) = \sum_{d|n} \mu(\frac{n}{d})d$.

6. **[Grothendieck groups]** Let $(M, +)$ be an Abelian monoid with identity element denoted by 0. Let $S(M)$ be the set of formal differences of elements in M, thus $S(M) = \{m \ominus n | m, n \in M\}$. Basically $S(M) = M \times M$ but we write elements as $m \ominus n$ rather than (m, n) for reasons which will become clear later. [Comment: Throughout this exercise, it might be helpful to view $\ominus$ as subtraction and $\oplus$ as addition. The notation is used here only to make things more formally correct. Note there is no concept of subtraction in the monoid M itself.]
(a) Define a relation $\approx$ on $S(M)$ by $a \ominus b \approx c \ominus d$ if and only if $a + d = c + b$ in M. Show that $\approx$ is reflexive and symmetric but is not an equivalence relation. Show that $\approx$ would be an equivalence relation on $S(M)$ if M has the cancellation property for monoids.
(b) Define a relation $\sim$ on $S(M)$ by $a \ominus b \sim c \ominus d$ if and only if $a + d + m = c + b + m$ in M for some $m \in M$. Show that this is an equivalence relation for any Abelian monoid M. We write $G(M) = S(M)/\sim$ for the set of equivalence classes. We will denote the equivalence class of $a \ominus b$ by $[a \ominus b]$.
(c) Define $\oplus$ on $G(M)$ by $[x_1 \ominus x_2] \oplus [y_1 \ominus y_2] = [(x_1 + y_1) \ominus (x_2 + y_2)]$. Show that $\oplus$ is a well-defined binary operation on $G(M)$ and that it makes $G(M)$ into an Abelian group with identity element $[0 \ominus 0]$. $G(M)$ is called the Grothendieck group of M.
(d) Define $\theta : M \to G(M)$ by $\theta(m) = [m \ominus 0]$. Show that $\theta : (M, +) \to (G(M), \oplus)$ is a homomorphism of monoids. Show that given $m_1, m_2 \in M$ we have $\theta(m_1) = \theta(m_2)$ if and only if there is $m \in M$ such that $m_1 + m = m_2 + m$. We say in this case that the elements m_1 and m_2 are "stably equal" in M, thus two elements in M go to the same element in $G(M)$ if and only if they are stably equal in M.
(e) Show that an Abelian monoid M has the cancellation property if and only if it embeds as a submonoid of some Abelian group, i.e. there is an isomorphism between M and some submonoid of an Abelian group.
(f) Show that the Grothendieck group $G(\mathbb{N})$ for the additive monoid of natural numbers $(\mathbb{N}, +)$, is isomorphic to the group $(\mathbb{Z}, +)$.