Solutions to Exam II

Problem 1. a) State the definition of a surjective function. How is the inverse function of a function $f : A \longrightarrow B$ defined and when does it exist?

b) Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be a function defined by $f(1) = 1$ and for $n > 1$, $f(n)$ is the smallest prime divisor of n. For example, $f(6) = 2$ and $f(15) = 3$.

What is the domain, codomain, range of f? What is $f^{-1}(\{2\})$? What is $f(\{3, 9, 21, 25\})$? What is $f \circ f$?

c) Let $f : X \longrightarrow Y$ be a function. Prove that $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

Solution: a) A function $f : A \longrightarrow B$ is **surjective** (or **onto**) if for any $b \in B$ there is $a \in A$ such that $f(a) = b$ (so B is equal to the range of f).

We say that the function $g : B \longrightarrow A$ is the **inverse** function of $f : A \longrightarrow B$ if $f \circ g = \mathrm{id}_B$ (i.e. $f(g(b)) = b$ for all $b \in B$) and $g \circ f = \mathrm{id}_A$ (i.e. $g(f(a)) = a$ for all $a \in A$). The inverse of f exists if and only if f is a bijection (i.e. it is both injective and surjective). For $b \in B$, the value $g(b)$ is defined as the unique element $a \in A$ such that $f(a) = b$.

b) Since $f : \mathbb{N} \longrightarrow \mathbb{N}$, the domain of f is $\mathbb{N}$ and the codomain of f is $\mathbb{N}$. By definition, every value of f is either a prime number of 1. Conversely, if p is a prime number then $f(p) = p$ so every prime number is a value of f. This proves that the range of f is the set of all prime numbers and the number 1:

$$\text{range of } f \;=\; \{n \in \mathbb{N} : n = 1 \text{ or } n \text{ is a prime number}\}.$$

The set $f^{-1}(\{2\})$ consists of all natural numbers which are mapped by f onto 2, i.e. all natural numbers whose smallest prime divisor is 2. Since 2 is the smallest prime, this is the same as all the numbers which are divisible by 2. In other words, $f^{-1}(\{2\})$ is the set of all even numbers:

$$f^{-1}(\{2\}) = \{n \in \mathbb{N} : n \text{ is even}\}.$$

Note that $f(3) = 3$, $f(9) = 3$, $f(21) = 3$, and $f(25) = 5$. Thus $f(\{3, 9, 21, 25\}) = \{3, 5\}$.

Finally, note that $f(f(1)) = f(1) = 1$ and if $n > 1$ then $f(n)$ is the smallest prime divisor of n. In particular, $f(n)$ is a prime number and therefore $f(f(n)) = f(n)$. This proves that $f \circ f = f$.

c) Let $x \in f^{-1}(A \cap B)$. This means that $f(x) \in A \cap B$, i.e. $f(x) \in A$ and $f(x) \in B$. Thus $x \in f^{-1}(A)$ and $x \in f^{-1}(B)$, which implies that $x \in f^{-1}(A) \cap f^{-1}(B)$. This proves that $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$.

Conversely, suppose that $x \in f^{-1}(A) \cap f^{-1}(B)$. Then $x \in f^{-1}(A)$ and $x \in f^{-1}(B)$, so $f(x) \in A$ and $f(x) \in B$. Thus $f(x) \in A \cap B$ and therefore $x \in f^{-1}(A \cap B)$. This proves that $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$.

Since we proved that $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$ and $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$, we conclude that $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$

Problem 2. a) State the definition of a relation R on a set A. What does it mean that R is transitive? What does it mean that R is antisymmetric? Define a relation R on the set $A = \{1, 2, 3, 4\}$ which is reflexive, neither symmetric nor antisymmetric.

b) Let us say that two natural numbers m, n are in the relation R if m and n are divisible by exactly the same prime numbers. For example, $(6, 12) \in R$ but $(6, 9) \notin R$. Prove that R is an equivalence

relation on the set $\mathbb{N}$. What is the equivalence class of 4? Find all natural numbers whose equivalence class is finite.

Solution: a) A **relation** R on a set A is a subset R of $A \times A$. Instead of writing $(a, b) \in R$ one often writes aRb and says that a is in relation R with b.
R is **transitive** if for any $a, b, c \in A$ such that aRb and bRc we have aRc.
R is **antisymmetric** if for any $a, b \in A$, if aRb then bRb does not hold. In other words, if $(a, b) \in R$ then $(b, a) \notin R$.

We define the relation R by listing all its elements. Since R is supposed to be reflexive, it must contain $(1, 1), (2, 2), (3, 3), (4, 4)$. To make R not symmetric we will add $(1, 2)$ but not $(2, 1)$. To ensure that it is not antisymmetric we add $(3, 4)$ and $(4, 3)$. Thus the relation

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (3, 4), (4, 3)\}$$

has all the required properties.

b) In order to prove that R is an equivalence relation, we need to show that it is reflexive, symmetric and transitive. Clearly every natural number has the same prime divisors as itself, so R is transitive. If mRn then m and n are divisible by the same prime numbers so n and m are divisible by the same prime numbers, i.e. nRm. This shows that R is symmetric. Now if mRn and nRk then m and n are divisible by the same primes and n and k are divisible by the same primes, hence m and k are divisible by the same primes (namely the primes which divide n). Thus mRk. This proves that R is transitive. It follows that R is an equivalence relation.

Note that 2 is the only prime which divides 4. Thus $m \in [4]$, i.e. $mR4$, if and only if 2 is the only prime divisor of m. This happens if and only if m is a power of 2:

$$[4] = \{2, 4, 8, 16, \ldots\} = \{2^k : k \in \mathbb{N}\}.$$

Note that 1 is the only natural number which has no prime divisors, so $[1] = \{1\}$ is finite. Let $n > 1$. Then the numbers n, n^2, $n^3, \ldots$ all have the same prime divisors. Thus $[n]$ contains n, n^2, $n^3, \ldots$, so it is infinite. It follows that 1 is the only natural number whose equivalence class is finite.

Problem 3. a) State Fermat's Little Theorem.

b) Find the remainder when 5^{1603} is divided by 17.

c) In $\mathbb{Z}_{12}$ find the inverse of the class $[5]$. Use it to solve in $\mathbb{Z}_{12}$ the equation $[5] \cdot x + [2] = [9]$.

d) Suppose that $ar \equiv b \pmod{m}$ and $br \equiv a \pmod{m}$. Prove that $a^2 \equiv b^2 \pmod{m}$.

Solution: a) **Fermat's Little Theorem:** *If p is a prime number and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.*
An equivalent statement: *If p is a prime number and a is an integer, then $a^p \equiv a \pmod{p}$.*

b) Since 17 is a prime number and 5 is not divisible by 17, we have $5^{16} \equiv 1 \pmod{17}$ by Fermat's Little Theorem. Thus

$$5^{1603} = (5^{16})^{100} \cdot 5^3 \equiv 1^{100} \cdot 5^3 = 5^3 \pmod{17}.$$

Furthermore,

$$5^3 = 25 \cdot 5 \equiv 8 \cdot 5 = 40 \equiv 6 \pmod{17}.$$

Thus $5^{1603} \equiv 6 \pmod{17}$. Since $0 \leq 6 < 17$, the remainder when 5^{1603} is divided by 17 is equal to 6.

c) Since $5 \cdot 5 = 25 \equiv 1 \pmod{12}$, we see that $[5][5] = [1]$, so $[5]$ is its own inverse.
To solve $[5]x+[2] = [9]$ we add $-[2]$ to both sides and get $[5]x = [9]-[2] = [9-2] = [7]$. Now we multiply both sides by the multiplicative inverse of $[5]$, which is $[5]$, to get $x = [5][5]x = [5][7] = [35] = [11]$ (as $35 \equiv 11 \pmod{12}$). Thus $x = [11]$.

d) By multiplying the congruence $ar \equiv b \pmod{m}$ by b we get $bar \equiv b^2 \pmod{m}$. Similarly, multiplying $br \equiv a \pmod{m}$ by a yields $abr \equiv a^2 \pmod{m}$. Thus $a^2 \equiv b^2 \equiv abr \pmod{m}$.

Problem 4. a) State the division algorithm.

b) Use Euclid's algorithm to compute $\gcd(889, 168)$. Find $x, y \in \mathbb{Z}$ such that $889x + 168y = \gcd(889, 168)$. Be extremely careful with your calculations (and check your answers).

c) State the Fundamental Theorem of Arithmetic and Euclid's Lemma.

d) Let a be an integer. Prove that the numbers $3a + 5$ and $7a + 12$ are relatively prime.

e) Let a, b be relatively prime integers. Prove that $\gcd(a, b^n) = 1$ for every natural number n.

Solution: a) **Division Algorithm.** Let $n \in \mathbb{N}$. For any integer m there exist unique integers k and r such that $m = kn + r$ and $0 \leq r < n$. The number k is the **quotient** and r is called the **remainder** when m is divided by n.

b) Euclid's algorithm yields:

$$889 = 5 \cdot 168 + 49,$$
$$168 = 3 \cdot 49 + 21,$$
$$49 = 2 \cdot 21 + 7,$$
$$21 = 3 \cdot 7 + 0.$$

It follows that $\gcd(889, 168) = 7$. Working backwards,

$$7 = 49 - 2 \cdot 21 = 49 - 2 \cdot (168 - 3 \cdot 49) = 7 \cdot 49 - 2 \cdot 168 = 7 \cdot (889 - 5 \cdot 168) - 2 \cdot 168 = 7 \cdot 889 - 37 \cdot 168.$$

Thus $x = 7$, $y = -37$ work.

c) **Fundamental Theorem of Arithmetic.** *Any integer $n > 1$ can be written in a unique up to order way as a product of prime numbers. In other words, n is a product of prime numbers and if $n = p_1 \dots p_s = q_1 \dots q_t$, where $p_1, \dots, p_s, q_1, \dots, q_t$ are primes then $s = t$ and the sequence $q_1, \dots, q_t$ is a permutation of the sequence $p_1, \dots, p_s$.*

Euclid's Lemma. *If p is a prime number and a, b are integers such that $p|ab$, then $p|a$ or $p|b$.*
Note that this can be stated in an equivalent way as follows: *if p is a prime, then $\mathbb{Z}_p$ satisfies the axiom* M4*: if $xy = 0$ the $x = 0$ or $y = 0$.*

d) It suffices to find integers x, y such that $x(7a + 12) + y(3a + 5) = 1$. Note that $3(7a + 12) + (-7)(3a + 5) = 1$. Thus any common divisor of $3a + 5$ and $7a + 12$ must divide 1. It follows that $\gcd(3a + 5, 7a + 12) = 1$.

e) I'st method: Let $a = p_1 \dots p_s$ and $b = q_1 \dots q_t$ be factorizations of a and b into primes. Since a and b are relatively prime, the sets of prime divisors of a and b are disjoint (i.e $p_i \neq q_j$ for all i, j). But the primes which appear in prime factorizations of b and b^n are the same, so a and b^n do not share any primes in their prime factorizations, so they are relatively prime.

II'nd method: We proceed by induction on n. For $n = 1$ the result is given. Suppose that for some $n \in \mathbb{N}$ the results is true for $1, 2, \ldots, n$. Then $\gcd(a, b^n) = 1 = \gcd(a, b)$. There exist integers u, w, s, t such that $ua + wb^n = 1 = sa + tb$. Thus $1 = (ua + wb^n)(sa + tb) = (uas + swb^n + tub)a + (wt)b^{n+1}$. This implies that $\gcd(a, b^{n+1}) = 1$, so the result holds for $n + 1$. By the method of induction, the result holds for all $n \in \mathbb{N}$.

III'rd method: Suppose that $d > 1$ is a common divisor of a and b^n. Then d has a prime divisor p and p is also a common divisor of a and b^n. Since p is a prime and $p|b^n$, we conclude by Euclid's Lemma that $p|b$. This however means that p is a common divisor of a and b, which contradicts the assumption that $\gcd(a, b) = 1$. The contradiction proves that d does not exist, i.e. $\gcd(a, b^n) = 1$.

Problem 5. a) Let $\mathbb{R}$ be an ordered field. Define the least upper bound of a subset A of $\mathbb{R}$. State the completeness axiom.

b) Let $\mathbb{R}$ be an ordered field which satisfies completeness axiom. Prove that the subset $\mathbb{N}$ of $\mathbb{R}$ is not bounded above.

Solution: a) The least upper bound of a set A is the smallest among all upper bounds of A.

Completeness Axiom. Every non-empty bounded above subset of $\mathbb{R}$ has the lest upper bound.

b) The prove is by contradiction. Suppose that $\mathbb{N}$ is bounded above. By completeness axiom, $\mathbb{N}$ has the lest upper bound r. Thus, for every $n \in \mathbb{N}$ we have $n + 1 \leq r$ (since $n + 1 \in \mathbb{N}$). This means that $n \leq r - 1$ for all $n \in \mathbb{N}$. It follows that $r - 1$ is an upper bound for $\mathbb{N}$. But $r - 1 < r$ and r is the least upper bound, a contradiction. This proves that $\mathbb{N}$ is not bounded above.

Problem 6. Let a, b, c be non-zero integers. Consider the set $S = \{xa + yb + zc : x, y, z \in \mathbb{Z}\}$. Prove that S contains a positive integer d which divides each of a, b, c. Conclude that d is the largest common divisor of a, b, and c and that d is the smallest positive element of S.

Solution: Let $e = \gcd(a, b)$. Thus there exist integers u, w such that $e = ua + wb$. Let $d = \gcd(e, c)$. There exist integers s, t such that $d = se + tc$. It follows that $d = s(ua + wb) + tc = (su)a + (sw)b + tc$, so $d \in S$. By definition of d we have $d|e$ and $d|c$. Since $e|a$ and $e|b$ we get that $d|a$, $d|b$, and $d|c$. Thus d is a positive element of S which divides each of a, b, c. If h is a common divisor of a, b, c then $h|(su)a + (sw)b + tc = d$, so $h \leq d$. This proves that d is the greatest common divisor of a, b, c. If m is any element of S then $m = xa + yb + zc$ for some integers x, y, z. It follows that $d|m$ (as d divides a, b, c). Thus, if $m > 0$ then $m \geq d$. In other words, d is the smallest positive element of S.

Exercise. Generalize this to any number of integers (not necessarily three).