Discrete Structures
Tutorial Solutions 2023

Ashwin Abraham
Rishabh RP

September 24th, 2023

Contents

Chapter 1

Propositions, Predicates, Numbers

Question 1

Assume the predicate $prime(n)$ is defined, which is true if and only if n is a prime number. Express the following statements in predicate logic:

1. There exist infinitely many prime numbers.
2. There exist arbitrarily long sequences of consecutive numbers such that none of the numbers is a prime number.
3. For all positive numbers n, there exists a prime number p such that $n \leq p \leq 2n$.

Question 2

These are some famous problems involving primes, some of which are still unsolved. Express them using predicate logic. Do NOT attempt to prove them or read the proofs, where available.

1. There exist infinitely many prime numbers p such that $p + 2$ is also a prime. This is also called the twin primes conjecture.
2. Every even number > 2 can be written as a sum of two (not necessarily distinct) prime numbers. This is called the Goldbach conjecture.
3. There exist arbitrarily long arithmetic progressions of prime numbers. This was proved in the early 2000s by Ben Green and Terrence Tao.
4. There exists a constant c such that there are infinitely many pairs of distinct prime numbers that differ by at most c. This was proved by Yitang Zhang in 2013 for c around 70 million. The value has now been reduced considerably.

Question 3

Define the addition and multiplication operations of numbers using the basic assumptions. Prove that they are commutative and associative, and that multiplication distributes over addition.

Question 4

Prove that for any natural number $m > 0$, for every number n, there exist unique natural numbers q and r such that $n = qm + r$ and $m > r \geq 0$. This is called the division property of numbers and is the starting point for many basic results in number theory.

Chapter 2

Greatest Common Divisor

Question 1

Let a, b be positive numbers, and let X be the set of all positive numbers r such that $xa = yb + r$ for some natural numbers x, y. Prove that the set X is exactly the set of all multiples of $\gcd(a, b)$. First, show that the smallest element must be $\gcd(a, b)$, and any other element must be a multiple of the gcd.

Question 2

Let a, b be positive numbers such that $a \mod b \neq 0$. Let $g > 0$ be the smallest number such that $xa \mod b = g$ for some number x. Prove that $g = \gcd(a, b)$. This implies that a has a multiplicative inverse $\mod b$ if and only if $\gcd(a, b) = 1$.

Question 3

Consider the following definition of a function $f(n, m)$. Define $f(0, n) = n$ for all n, $f(n, m) = f(m, n)$ for all n, m, and $f(n, m) = f(n \mod m, m)$. Prove using strong induction that this defines f uniquely, and that for all n, m, $f(n, m) = \gcd(n, m)$. This gives an algorithm for computing $\gcd(n, m)$ called Euclid's algorithm. If n, m are numbers with k bits in their binary representations, find an upper bound on the number of arithmetic operations required to compute the gcd. Modify the algorithm to find x and y such that $xn = ym + \gcd(n, m)$.

Question 4

Another algorithm for finding the gcd is given by a different definition. Again, $\gcd(0, n) = \gcd(n, 0) = n$ for all n, $\gcd(2n, 2m) = 2\gcd(n, m)$, $\gcd(2n, 2m + 1) = \gcd(n, 2m + 1)$, $\gcd(2n + 1, 2m) = \gcd(2n + 1, m)$, and $\gcd(2n + 1, 2m + 1) = \gcd(2m + 1, n - m)$ if $m \leq n$ and $\gcd(2n + 1, m - n)$ otherwise. Prove that this function is well-defined and it gives exactly the gcd of n, m. This needs the fact that every number $n > 0$ is either $2m$ or $2m + 1$ for some $m < n$. This has the advantage that it uses only subtraction and division by 2 and is easier to implement in hardware.

Question 5

Consider an $m \times n$ matrix A with integer entries. Let L be the set of all m-dimensional vectors v such that $v = Ax$ for some n-dimensional vector x with integer entries. The set L is called a lattice. Prove that for any such matrix A, there exists an $m \times m$ matrix B such that L is exactly the set of vectors By, where y can be any integral m-dimensional vector. Note that when A is the 1×2 matrix $[ab]$, B is the 1×1 matrix $[\gcd(a, b)]$. B is called a basis for L. A challenging problem is to find a basis with "smallest" possible entries and a vector in L with the smallest magnitude. This is equivalent to finding gcd if $m = 1$ but is much more difficult for arbitrary m. Try to do it for $m = 2$. The dimension of L is the smallest k such that every vector in L can be written as an integer linear combination of k m-dimensional vectors. The dimension of L can be at most m but may be less than m. Given the matrix A, can you find an efficient algorithm to find the dimension of L?

Chapter 3

Modular Arithmetic

Question 1

Let m, n be positive integers such that $\gcd(m, n) = 1$. Prove that for all $a \in Z_m$ and $b \in Z_n$, there exists a unique number $x \in Z_{mn}$ such that $x = a \mod m$ and $x = b \mod n$. This is known as the Chinese Remainder Theorem. Suppose now that $\gcd(m, n) = d$ for some number d. Find a necessary and sufficient condition on a and b for such a number x to exist. If it exists, how many distinct such numbers exist in Z_{mn}?

Question 2

A number a such that $1 \leq a < n$ is called a quadratic residue modulo n if the congruence $x^2 = a \mod n$ has a solution. If n is a prime number, how many quadratic residues are there modulo n? If $n = pq$ is a product of two distinct odd prime numbers, how many quadratic residues are there modulo n?

Question 3

Let n be a prime number, and $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{d-1}x^{d-1} + x^d$ be a polynomial of degree d with coefficients $a_i \in Z_n$ for $0 \leq i < d$. An element $a \in Z_n$ is called a root of the polynomial if $P(a) = 0 \mod n$. Prove that a polynomial of degree $d \geq 1$ has at most d roots in Z_n. For all primes n, prove that there exists a polynomial of degree 2 that has no roots in Z_n. Such a polynomial is called irreducible modulo n. Try to explicitly construct such a polynomial for any general prime n. Try to generalize to polynomials of degree d for $d \geq 2$.

Question 4

Let n be a prime number, and a a number not divisible by n. The order of a modulo n is the smallest positive number k such that $a^k = 1 \mod n$. Prove that the order of a divides $n-1$. The number a is said to be a primitive root modulo n if its order is $n-1$. Prove that for all primes n, there exists a primitive root modulo n. Prove that n is prime if and only if there exists a number $a \in Z_n$ such that $a^{n-1} = 1 \mod n$ and $a^{(n-1)/p} \neq 1 \mod n$ for any prime p that divides $n-1$. Hint: Try to find for each divisor d of $n-1$, the number of elements in Z_n of order d.

Question 5

Prove Wilson's theorem that $(n-1)! + 1 = 0 \mod n$ if and only if n is prime. While this gives a necessary and sufficient condition for a number n to be prime, Fermat's little theorem only gives a necessary condition which is not sufficient. There exist composite numbers n such that for all a, $\gcd(a, n) = 1$ implies $a^{n-1} = 1 \mod n$. Such numbers are called Carmichael numbers. Prove that a number n is a Carmichael number if and only if n is a product of distinct primes and for every prime p that divides n, $p-1$ divides $n-1$. The smallest composite Carmichael number is $561 = 3 \times 11 \times 17$, and it is known that there are infinitely many of them. Find small values of a for which 561 is declared to be composite by the Miller-Rabin test.

Chapter 4

Sets, Relations, Functions

Question 1

Prove that if A is any finite set, then any function f from A to A is 1-1 if and only if it is onto. Use induction on the number of elements in A. Give examples of a 1-1 function from A to A that is not onto, and also an onto function from A to A that is not 1-1, for some set A. Prove that every set is either finite or there exists a 1-1 function f from N to A.

Question 2

Prove that the set of all finite subsets of N has the same cardinality as N. Find an explicit bijection between these sets. In other words, given a finite subset of natural numbers, show how to compute a natural number from it, so that the original set can be recovered uniquely from the computed number. Do the same for all finite sequences of natural numbers. Note that there is no fixed bound on the size of the finite subset or the length of the finite sequence. All that is known is that it is some natural number.

Question 3

Let $A_1, A_2, \ldots$ be an infinite sequence of sets such that the intersection of any finite number of sets in the sequence is not empty. Is it true that there exists an element x such that $x \in A_i$ for all i? If so, prove it; else, give an example for which it is false. Suppose $a_1, a_2, \ldots$ is an infinite sequence of numbers such that the gcd of any finite subsequence of numbers in the sequence is greater than 1. Prove that there exists a

prime p such that p divides a_i for all i.

Question 4

Let R be a relation from a set A to itself. Let R_k be defined inductively by $R^0 = I$ and $R^k = R \cdot R^{k-1}$. Suppose there exists a number $k > 0$ such that R_k is the identity relation. Prove that R must be a bijection. Prove that if R is a bijection and A is finite, there exists a $k > 0$ such that $R^k = I$. Give an example to show that this may not be true if A is infinite. For a finite set A with n elements, what is the smallest number k such that for every bijection R from A to A, $R^k = I$? Prove your answer.

Question 5

Let R_1, R_2, R_3 be relations on a set A. Prove or disprove the following statements:

(i) $(R_1 \cdot R_2)^{-1} = R_2^{-1} \cdot R_1^{-1}$.

(ii) $(R_1 \cup R_2) \cdot R_3 = (R_1 \cdot R_3) \cup (R_2 \cdot R_3)$.

(iii) $(R_1 \cap R_2) \cdot R_3 = (R_1 \cdot R_3) \cap (R_2 \cdot R_3)$.

(iv) $R_1 \cdot R_2$ is a function if and only if both R_1 and R_2 are functions.