

Discrete Mathematics — Tutorial Sheet 02 — Mathematical Proofs

BSc (H) in App Comp, Ent Sys, Comp Foren, and the IoT

Direct Proof

Question 1

Prove that the sum of two odd numbers is even.

Question 2

Prove that the product of two odd numbers is odd.

Question 3

Prove the claim “The square of an even natural number is even”.

Question 4

If A and B are real positive numbers, then prove that

$$\underbrace{\frac{A+B}{2}}_{\text{arithmetic mean}} \geq \underbrace{\sqrt{AB}}_{\text{geometric mean}}$$

Hint: Use fact that $(a-b)^2 = a^2 - 2ab + b^2 \geq 0$.

Question 5

Prove the Pythagorean theorem.

Question 6

Prove that $x = y$ if and only if $xy = \frac{(x+y)^2}{4}$. Note, you will need to prove in two “directions” here: the “if” and the “only if” part.

Proof by Cases

Question 7

Prove that for any integer n , the number $(n^3 - n)$ is even.

Question 8

Prove that every prime number greater than 3 is either one more or one less than a multiple of 6.

Hint. Prove the contrapositive by cases.

Question 9

Let a, b, c, d be integers. If $a > c$ and $b > c$, then $\max(a, b) - c$ is always positive.

Proof by Contradiction

Question 10

Prove that a triangle cannot have more than one right angle.

- (a) Prove that the $\sqrt{2}$ is irrational.¹
- (b) Prove that $\log_2(3)$ is irrational.
- (c) Let n be an integer. If $3n + 2$ is odd, then prove that n is odd.
- (d) Prove that there are an infinite number of primes.²
- (e) Prove that there are no integers x and y such that $x^2 = 4y + 2$.
- (f) The Pigeonhole Principle: If more than n pigeons fly into n pigeon holes, then at least one pigeon hole will contain at least two pigeons. Prove this.

Other Proofs

Question 11

Prove that x^n can be computed using only $\log_2(n)$ multiplications when n is a power of 2.

This is a special case of the Montgomery algorithm for computing large integer power quickly — a big deal in cryptography!

- (a) Prove that the sum of the first n positive integers equals $n(n + 1)/2$

¹“irrational”= “not rational”. A **rational** number is a number that can be expressed as quotient of two integers p and q which don’t have a common factor.

²A **prime** is an integer greater than one with exactly two divisors.