COMS10014 Worksheet 5: Proofs

1. Laws of Logical Reasoning

1. (★) Are the following arguments valid? If so, which laws of logical reasoning do they use?

a. To be great is to be misunderstood.
Helen is great.
Helen is misunderstood.

b. If Frank does not go running regularly, he will not be able to complete the race.
Frank did not complete the race.
Therefore, he did not go running regularly.

c. The taxi is either red or green. The taxi is not red, therefore the taxi is green.

d. Logic is fun and it is sunny today. Therefore, logic is fun.

e. If it rains, then I go by car. I went by by car yesterday.
Therefore, it rained yesterday.

f. If it rains, then I'll go by car. It rains today, therefore I go by car today.

2. (★★) Consider the following argument:

"It is not snowing this morning. We will go skiing only if it is snowing. If we do not go skiing, then, if it is cold we will stay in. If we are in, then we can help you unload the car when you arrive. It is cold today."

What conclusions can you draw, and in particular, will you get help unloading the car today? Explain the rules of inference that you used to come to your conclusion.

2. Spot the Mistake (★★)

Claim: Every integer $n \geq 2$ has a prime decomposition, that is, we can write it as $n = a \times b \times c \times \ldots$ where all the variables on the right-hand side are prime numbers. (This claim is true.)

The following is not a valid argument – where is the mistake?

Let P be the proposition "$n \geq 2$" and Q the proposition "n has a prime decomposition". The claim is $P \vDash Q$, which means the same thing as that that $P \to Q$ is true. We do a proof by contradiction, showing that $\neg(P \to Q)$ is false. Since $P \to Q \equiv \neg P \vee Q$, then $\neg(P \to Q) \equiv P \wedge \neg Q$ using DeMorgan. Written out, $P \wedge \neg Q$ is "$n \geq 2$ and n does not have a prime decomposition". However, this claim has a counter-example: $n = 4$ satisfies $n = 2$ and n has a prime decomposition 2×2. Therefore, the negated claim is false, so the original claim is true.

3. Proofs

1. (★) Prove, with a direct proof, that if a and b are both odd then $a \times b$ is odd, and in the other three cases (a even, b even, both even) then $a \times b$ is even.
2. Prove that the square of an even integer is an even integer in three different ways:
   a. (★) By direct proof.
   b. (★★) By indirect proof.
   c. (★) By contradiction.
3. Prove that for any integer n, if $n^3 + 5$ is odd, then n is even in three different ways:
   a. (★★) By direct proof.
   b. (★) By indirect proof.
   c. (★) By contradiction.

The (★★) parts require an extra 'trick' along the way. You can use the results from earlier parts in the proofs of the later parts of this exercise.

4. True or False? (★★)

Decide whether the following statements are true or false, and prove this. For the true statements, choose a proof strategy and write down which strategy you used. For the false statements, finding a counter-example is usually the best strategy.

1. The sum of an even integer and an odd integer is an odd integer.
2. If $x + y$ is even, then x and y have the same parity
   (parity is the property of being odd or even).
3. All primes are odd.
4. For all integers n, the term $n^3 - n$ is even.
5. For all *real numbers* a, b, if $a^2 = b^2$ then $a = b$.

5. A Real Proof (★★)

For any *real numbers* m, n, prove that $m^2 = n^2$ if and only if $m = n$ or $m = (-n)$.

Note: there are at least two different ways to prove and "if and only if" statement. This proof works with both the common ways, and you should try them both.

6. Modular Arithmetic (★★)

Euclid's theorem says that for any integer a and any positive integer b, we can find exactly one pair of integers (q, r) such that $a = qb + r$ and $0 \leq r$ and $r < b$. That is, r is an element of $\{0, 1, \dots, b - 1\}$. This r is called the remainder of a modulo b.

We write $x \equiv y \pmod b$ or $x \equiv_b y$ to mean that x and y both have the same remainder modulo b. In the special case $b = 2$, the numbers n with $n \equiv_2 0$ are even, and $n \equiv_2 1$ are odd numbers.

1. Prove that, if $x \equiv y \pmod b$ for any integers x, y and any positive integer b, then we can write $x = bk + y$ for some integer k.
2. Prove that the square of any odd integer has the form $8m + 1$ for some integer m.
3. Let n be an integer that is not divisible by 5. Prove that $n^4 - 1$ is divisible by 5.
4. Prove, without using prime decomposition, that for any integers u, v the product $u \times v$ is a multiple of 3 if and only if u is a multiple of 3 or v is a multiple of 3.
5. For a positive integer n, the set $\mathbb{Z}_n$ is the set of integers from 0 to $n - 1$, that is exactly the set of possible remainders modulo n. On $\mathbb{Z}_n$, we can define addition $+_n$ and multiplication $\times_n$ as follows: add/multiply the two remainders, then take the remainder of the result modulo n.
    a. Create addition/multiplication tables (that is, truth tables) for $+_2$ and $\times_2$ over $\mathbb{Z}_2$.
    b. Which logical operations do these correspond to, if 0 is false and 1 is true?
    c. Create the multiplication table for $\mathbb{Z}_5$. Note: It is nicer to draw this as a 5×5 table with one operand in the rows, and one in the columns, than to create a table with 25 rows.

7. Modular Arithmetic Challenge (★★★)

1. Show that, if p is a prime number and $a \times b \equiv 0 \pmod p$ (for a, b natural numbers) then $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$. You can use that every natural number has a unique prime factorisation.
2. Find an example of natural numbers a, b, n where $a \times b \equiv 0 \pmod n$ but both $a \not\equiv 0 \pmod n$ and $b \not\equiv 0 \pmod n$.