COMS10014 Solutions 5: Proofs

1. Laws of Logical Reasoning

1. a. This argument is valid. If P is "great" and Q is "misunderstood", then this argument is $P \wedge (P \to Q) \vdash Q$. This is an instance of modus ponens. You could also check with a truth table that (replacing $\vdash$ with $\to$) it is a tautology.

   Note: what happened to 'Helen'? If you felt uneasy about P referring once to the general concept of greatness and once to the greatness of a specific Helen, well done for spotting this. We will make this point more precise when we look at predicate logic.

b. This is not valid. If P is "Frank goes running regularly" and Q is "Frank completes the race", then the argument is $\big((\neg P \to \neg Q) \wedge \neg Q\ \big) \to \neg P$ and this is not a tautology: it is not true for the assignment P=true, Q=false.

c. Valid. This is a disjunctive syllogism.

d. Valid. This is an example of $\wedge$ elimination.

e. Invalid. If R: "it rains" and C: "I go by car" then $(R \to C) \wedge C$ does not imply R, as it is false in the case R=false, C=true. This mistake is common enough that it gets its own name: it is called the *fallacy of affirming the conclusion*.

f. Valid. This is another modus ponens.

You can see that in general, "valid?" means "tautology?" and you could solve the validity part of all these questions with a truth table. But, since you know the laws of logical reasoning as presented in the lecture notes are sound, whenever you can spot that a logical argument is an instance of one of these laws, you can declare it valid without making a truth table. This often saves time (for example in an exam).

2. Yes, you get help with unloading the car. If P: "it is snowing", Q:"we go skiing", R: "it is cold", S: "we stay in" and T: "we help unloading the car", we have

1. $\neg P$
2. $Q \to P$
3. $\neg Q \to (R \to S)$
4. $S \to T$
5. R

The structure of the proof, as a tree:

$$\dfrac{\dfrac{R \qquad \dfrac{\dfrac{\neg P \quad Q \to P}{\neg Q}\,\text{m.t.} \quad \neg Q \to (R \to S)}{R \to S}\,\text{m.p.}}{S}\,\text{m.p.} \qquad S \to T}{T}\,\text{m.p.}$$

(m.p. = modus ponens, m.t. = modus tollens)

2. Spot the Mistake

If you replace Q with '$n < 5$', then the claim becomes $n \geq 2 \rightarrow n < 5$, which is obviously false in general, and yet the 'counter-example' $n = 4$ still satisfies $n \geq 2$ and $n < 5$. So something must be wrong with this line of argument (even if the original claim about primes is true).

P and Q have a free variable n, so the original claim $P \vDash Q$ means '$P \rightarrow Q$ holds for every possible (integer) n'. (The truth table involved would have one row for each integer value, which would make it an infinite table, but we can still reason about such a table even if we cannot write it down.) In other words, the claim is that $P \rightarrow Q$ is a tautology.

The negation of '$P \rightarrow Q$ is a tautology' is not '$P \rightarrow Q$ is a contradiction', but '$P \rightarrow Q$ is a contradiction, or a contingency'. The distinction only vanishes if there are no free variables. The negation of '$P \rightarrow Q$ is true for all n' is thus not '$P \rightarrow Q$ is false for all n' but '$P \rightarrow Q$ is false for at least one n'.

The argument shows that '$P \rightarrow Q$ is false for all n' is false, because it is true for at least one n namely $n = 4$. But that just means that $P \rightarrow Q$ is not a contradiction and therefore it is either a contingency or a tautology. That is not enough to show that $P \rightarrow Q$ is definitely a tautology.

3. Proofs

1. If a, b are both odd then we can write $a = 2k + 1$ and $b = 2m + 1$ (*note: we need two different variables here!*). Then $ab = 2(2km + k + m) + 1$ which is odd. If a is even, then $a = 2k$ for some k and so $ab = 2(kb)$ which is even, whatever b is so this covers two cases at once, and if b is even then $b = 2k$ and so $ab = 2(ak)$ which is even again.

2. The three proofs:

   a. Let n be even, then $n = 2k$ for some k and therefore $n^2 = (2k)^2 = 2(2k^2)$ which is also even (specifically, $n^2 = 2k'$ for $k' = 2k^2$).

   b. The contrapositive of "n even $\rightarrow$ n^2 even" is "n^2 odd $\rightarrow$ n odd", so assume that $n^2 = 2k + 1$. *Do not attempt to take a square root here!* Instead, rewrite this as $n^2 - 1 = 2k$ and therefore $(n + 1)(n - 1) = 2k$. From Part 1., this means at least one of $n - 1$ and $n + 1$ is even. If $n - 1 = 2m$ then $n = 2m + 1$ which is odd, and if $n + 1$ is even then $n + 1 = 2m$ so $n = 2m - 1 = 2(m - 1) + 1$ which is odd. In both cases, n is odd.

   c. Suppose that n is even, but n^2 is odd. Then $n = 2k$ and so $n^2 = 2(2k^2)$ which is a contradiction to the fact that n^2 cannot be both odd and even.

3. The three proofs:

   a. The extra step we need here is to prove that n and n^3 always have the same parity. Case distinction: if n is even, then $n = 2k$ for some k and so $n^3 = 2(4k^2)$. If n is odd, so $n = 2k + 1$ for some k, then $n^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1$ which is $2(4k^3 + 6k^2 + 3k) + 1$ and therefore odd. (The same holds for other powers: n^k for positive integer powers k always has the same parity as n.)
   So, if $n^3 + 5$ is odd, then $n^3 + 5 = 2k + 1$ for some k and so $n^3 = 2k - 4 = 2(k - 2)$ and therefore n^3 is even; but this means that n must be even too.

b. We prove that if n is odd then $n^3 + 5$ is even. Namely, if $n = 2k + 1$ then $n^3 + 5 = (2k + 1)^3 + 5 = 2(4k^3 + 6k^2 + 3k + 3)$ which must be even.

c. Assume that $n^3 + 5$ is odd and n is odd. Then $n = 2k + 1$ and so $n^3 + 5 = (2k + 1)^3 + 5 = 2(4k^3 + 6k^2 + 3k + 3)$ as before, but this contradicts the assumption that $n^3 + 5$ is odd.

4. True or False?

1. True, by direct proof. If a is even then we can write $a = 2k$ for some k, and if b is odd then we can write $b = 2m + 1$ for some m.
   Then $a + b = 2k + 2m + 1 = 2(k + m) + 1$ so the sum is odd.

2. True, by contradiction. Suppose that $x + y$ is even, but the two have different parity – then one must be odd and one must be even. But that is a contradiction to what we just proved in 1.

3. False. 2 is an even prime. (2 is the only even prime, but the statement was about "all" primes, so the statement is false.)

4. True, by case distinction. If n is even then $n = 2k$ for some k and so $n^3 - n = 8k^3 - 2k = 2(4k^3 - k)$ which is even. If n is odd, then $n = 2k + 1$ for some k and $n^3 - n = n(n^2 - 1) = (2k + 1)((2k + 1\,)^2 - 1) = 8k^3 + 12k^2 + 4k = 2(4k^3 + 6k^2 + 2k)$ which is even again.

5. False. If $a = 1$ and $b = (-1)$ then $a^2 = b^2$, for example.

5. A Real Proof

The first way to do a ↔ proof is to prove the ← and → directions separately, so:

Claim: $\underline{m^2 = n^2 \rightarrow (m = n \vee m = (-n))}$. Assume $m^2 = n^2$ and rewrite as $m^2 - n^2 = 0$ which we factor as $(m + n)(m - n) = 0$. Since a product is zero over the reals if and only if a factor is zero, we get $m + n = 0 \vee m - n = 0$ which is $m = (-n) \vee m = n$.

Claim: $\underline{(m = n \vee m = (-n)) \rightarrow m^2 = n^2}$. By case distinction: if $m = n$ then $m^2 = n^2$ and if $m = (-n)$ then $m^2 = n^2$ as well.

The second way to prove a ↔ proof is to do a normal proof, but only use steps that work in both directions (for example, $m = n \rightarrow m^2 = n^2$ only works in one direction!).

$$
\begin{array}{ll}
 & m^2 = n^2 \\
\equiv & m^2 - n^2 = 0 \\
\equiv & (m + n)(m - n) = 0 \\
\equiv & m + n = 0 \vee m - n = 0 \\
\equiv & m = (-n) \vee m = n
\end{array}
$$

All these steps work in both directions, so this is a direct proof. The second-to-last step uses the fact that a product is zero if and only if any of its factors is zero.

6. Modular Arithmetic

1. Pick any integers $x,\ y$. By Euclid's theorem, there are integers q, r, q', r' such that $x = qb + r$ and $y = q'b + r'$ where r, r' are the remainders modulo b. If $x \equiv y \pmod b$ then we also have $r = r'$ so we can write $(x - y) = qb + r - (q'b + r) = b(q - q')$.
   Therefore, $x = b(q' - q) + y$ so $k = q - q'$ satisfies the equation we want.

2. The proof is a case distinction over the remainder modulo 8. Let n be an odd integer, then we can write $n = 8q + r$ using Euclid's theorem with $r \in \{0,1,2,3,4,5,6,7\}$. The cases 0,2,4,6 all give even integers, as for $r = 2s$ we get $n = 2(4q + s)$, so we only have to check the odd remainders. In any case, $(8q + r)^2 = 8(8q^2 + 2qr) + r^2$ so

   - For $n = 8q + 1$, we have $n^2 = 8(8q^2 + 2q) + 1$ which is of the correct form.
   - For $n = 8q + 3$, we have $n^2 = 8(8q^2 + 6q) + 9 = 8(8q^2 + 6q + 1) + 1$.
   - For $n = 8q + 5$, we have $n^2 = 8(8q^2 + 10q) + 25 = 8(8q^2 + 10q + 3) + 1$.
   - For $n = 8q + 7$, we have $n^2 = 8(8q^2 + 14q) + 49 = 8(8q^2 + 14q + 6) + 1$.

3. Let $n = 5q + r$ with $r \in \{0,1,2,3,4\}$ by Euclid. If $r = 0$ then $n = 5q$ is divisible by 5, so there are only four cases to check. In any case,

$$(5k + r)^4 = 625k^4 + 500k^3r + 150k^2r^2 + 20kr^3 + r^4 = 5(125k^4 + 100k^3r + 30k^2r^2 + 4kr^3) + r^4$$

   so we only need to check that $r^4 - 1$ is divisible by 5.

   - If $r = 1$, then $n^4 - 1 = (5k + 1)^4 - 1 = 5(\dots) + 1 - 1$, and this has a factor 5.
   - If $r = 2$, then $n^4 - 1 = (5k + 2)^4 - 1 = 5(\dots) + 16 - 1$ and 15 has a factor 5 too.
   - If $r = 3$, then $n^4 - 1 = (5k + 3)^4 - 1 = 5(\dots) + 81 - 1$ and 80 has a factor 5 too.
   - If $r = 4$, then $n^4 - 1 = (5k + 4)^4 - 1 = 5(\dots) + 256 - 1$ and 255 has a factor 5 too.

4. Using Euclid, write $u = 3q + r$ and $v = 3q' + r'$. Then $u \times v = 3(3qq' + qr' + q'r) + rr'$. We know that $r, r' \in \{0,1,2\}$ so we can make a case distinction:

$r \times r'$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	4

   We see that rr' is zero (in which case $u \times v = 3(\dots)$ is a multiple of 3) if and only if one or both factors are zero, whereas in all other cases, $u \times v = 3(3qq' + qr' + q'r) + z$ where z is itself not a multiple of 3, so neither is $u \times v$. Since division with remainder is unique, in the cases when $z < 3$ then z must be the remainder when dividing $u \times v$ by 3, and so $u \times v$ cannot be a multiple of 3 as it cannot have both remainder 0 and z at the same time. In the last case, $z = 4 = 1 \times 3 + 1$ so $u \times v$ has remainder 1 modulo 3.
   Note: it is not enough to say that $r \times r'$ is zero if and only if one of the factors is zero. The problem is that the product could in principle be a multiple of 3, in which case $u \times v$ would also be a multiple of 3. So we really do need to check all nonzero cases by hand for now.
   The general version of this, for any $b > 0$, is that the remainder of a product is the *remainder of the product of the remainders of the factors*. We have not asked for a proof of this here, as it would require more mathematical theory than we know at the moment.

5. $\mathbb{Z}_2$ is just the set $\{0, 1\}$.

a. The table is:

a	b	$a +_2 b$	$a \times_2 b$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

b. The modulo-2 addition operation is the $\oplus$ (exclusive or), and modulo-2 multiplication is $\wedge$ (and).

c. The multiplication table:

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

This table has the interesting property that, apart from "0 times anything is still 0", every remaining value appears exactly once in every non-zero row and column of the table. This is generally true for $\mathbb{Z}_p$ when p is prime (but not otherwise) and has lots of interesting applications in group theory – for example, it has uses in coding theory (how to send data reliably over a channel that sometimes makes mistakes) and cryptography (how to send data so the bad guys cannot read or change it).

7. Modular Arithmetic Challenge

1. Factor $a = a_1 \times \ldots \times a_n$ where all the a_i are prime, and $b = b_1 \times \ldots \times b_m$ dito. (Note that we used two different variables n, m for the last index, as there is no reason that a, b must both have the same number of prime factors.) Then $a \times b = a_1 \times \ldots \times a_n \times b_1 \times \ldots \times b_m$. Since $a \times b$ has a unique prime factorisation, this must be it.

$a \times b \equiv 0 \pmod{p}$ means that $a \times b = kp$ for some integer k. So, a factor p must appear in the prime decomposition of $a \times b$. The definition of a prime is a number greater than 1 that cannot be written as a product $u \times v$ over the naturals except if one of the factors is p itself (and so the other is 1). Therefore, a factor p must appear as at least one of the a_i or the b_j since that is the prime factorisation of $a \times b$, which is a multiple of p. If $a_i = p$ for some i then a has a factor p itself, so $a = up$ for some integer u, so $a \equiv 0 \pmod{p}$. If none of the a_i is p, then the argument for b (which must now contain the p factor) is the same one.

2. Take for example $a, b = 2$ and $n = 4$. If you followed the above proof's idea closely, you know this can only happen if both a, b contain factors of n, and n being non-prime can split some of its factors into a and others into b.

One application of this fact is that if you have a 'computer integer', say an unsigned 64-bit integer, that is 0 and you know it was calculated by multiplying two such integers a, b then you cannot conclude that one of the factors must have been 0. Indeed, 2×2^{63} will wrap around to 0 in 64-bit arithmetic.