MATH104 Solution Sheet 5

1.

a) Let $m, n \in \mathbb{Z}$. If m is even then mn is even.

Given	**Goal**
$m, n \in \mathbb{Z}$ m is even	mn is even

Recall that an integer m is even if it is divisible by 2, that is if $m = 2k$ for some integer k. So we have

Given	**Goal**
$m, n \in \mathbb{Z}$ $m = 2k$ for some $k \in \mathbb{Z}$	$mn = 2\ell$ for some $\ell \in \mathbb{Z}$

Now we can see how to proceed. *Given* that $m = 2k$ we have $mn = 2kn = 2\ell$, where $\ell = kn$.

Proof. Let $m, n \in \mathbb{Z}$ and suppose that m is even: thus there is an integer k with $m = 2k$. So $mn = (2k)n = 2(kn)$ is divisible by 2, i.e. mn is even as required. ∎

b) Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$ then $a \mid c$.

Given	**Goal**
$a, b, c \in \mathbb{Z}$ $a \mid b$ $b \mid c$	$a \mid c$

Using the definition of 'divides', we can rewrite this as

Given	**Goal**
$a, b, c \in \mathbb{Z}$ $b = ka$ for some $k \in \mathbb{Z}$ $c = \ell b$ for some $\ell \in \mathbb{Z}$	$c = ma$ for some $m \in \mathbb{Z}$

This shows us how to proceed. *Given* that $c = \ell b$ and $b = ka$ we have $c = \ell(ka) = (\ell k)a$, so c is divisible by a.

Proof. Let $a, b, c \in \mathbb{Z}$ and suppose that $a \mid b$ and $b \mid c$. Thus there are integers k and ℓ such that $b = ka$ and $c = \ell b$. It follows that $c = \ell(ka) = (\ell k)a$, so that $a \mid c$ as required. ∎

c) Let $x \in \mathbb{R}$. If $5x \leq x^2$ then $x \leq 0$ or $x \geq 5$.

Given	**Goal**
$x \in \mathbb{R}$ $5x \leq x^2$	$x \leq 0$ or $x \geq 5$

Following the strategy given in lectures, we *negate* $x \leq 0$ and move it into the **Given** column:

Given	**Goal**
$x \in \mathbb{R}$ $5x \leq x^2$ $x > 0$	$x \geq 5$

The strategy is now clear: *Given* than $5x \leq x^2$ and $x > 0$, we can divide both sides of $5x \leq x^2$ by x to give $5 \leq x$.

Proof. Let $x \in \mathbb{R}$ with $5x \leq x^2$. If $x \leq 0$ the goal is achieved. So suppose $x > 0$. Then we can divide both sides of the inequality by x to give $5 \leq x$. Hence *either* $x \leq 0$ *or* $x \geq 5$ as required. ∎

d) Let a and b be positive real numbers. If $a \neq b$ then $(a+2b)^3 > 27ab^2$. The contrapositive is easier to work with:

Given	**Goal**
$a, b \in \mathbb{R}$ $a, b \geq 0$ $(a+2b)^3 \leq 27ab^2$	$a = b$

Proof.

$$\begin{aligned}(a+2b)^3 \leq 27ab^2 &\Rightarrow a^3 + 6a^2b + 12ab^2 + 8b^3 \leq 27ab^2 \\ &\Rightarrow a^3 + 6a^2b - 15ab^2 + 8b^3 \leq 0 \\ &\Rightarrow (a-b)^2(a+8b) \leq 0.\end{aligned}$$

Now we are given $a \geq 0$ $b \geq 0$, And if $a \neq b$ then $a+8b > 0$. It follows that either $a = b$ (as we are trying to prove) or $(a-b)^2 \leq 0$. Since $(a-b)^2 < 0$ is not possible (a, b are real) we must have $(a-b)^2 = 0$, which is the same as $a - b = 0$, that is $a = b$ as required. ∎

e) There do not exist integers m and n with $13m - 39n = 71$.

Given	**Goal**
$m, n \in \mathbb{Z}$	$13m - 39n \neq 71$

For a proof by contradiction, we move the *negation* of the goal in with the givens:

Given	**Goal**
$m, n \in \mathbb{Z}$ $13m - 39n = 71$	Contradiction

The contradiction will come from the fact that $13m - 39n$ is divisible by 13, but 71 is not.

Proof. Assume for a contradiction that m and n are integers with $13m - 39n = 71$. Now $13m - 39n = 13(m - 3n)$ is divisible by 13. Thus 71 is divisible by 13. This is the required contradiction. ∎

f) Let $n \in \mathbb{Z}$. If n^2 is odd then n is odd.
The contrapositive is: If n is not odd then n^2 is not odd, that is:
If n is even then n^2 is even.

Given	**Goal**
$n \in \mathbb{Z}$ n is even	n^2 is even

Proof. Let n be even, $n = 2k$ say. Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ which is even. ∎

g) Let $n \in \mathbb{Z}$. If n is even then $3n + 1$ is odd.

Given	**Goal**
$n \in \mathbb{Z}$ n is even	$3n + 1$ is odd

For a proof by contradiction we move the negation of the goal in with the givens:

Given	**Goal**
$n \in \mathbb{Z}$ n is even $3n + 1$ is even	Contradiction

Using the definition of 'even', this becomes:

Given	**Goal**
$n \in \mathbb{Z}$ $n = 2k$ for some integer k $3n + 1 = 2\ell$ for some integer ℓ	Contradiction

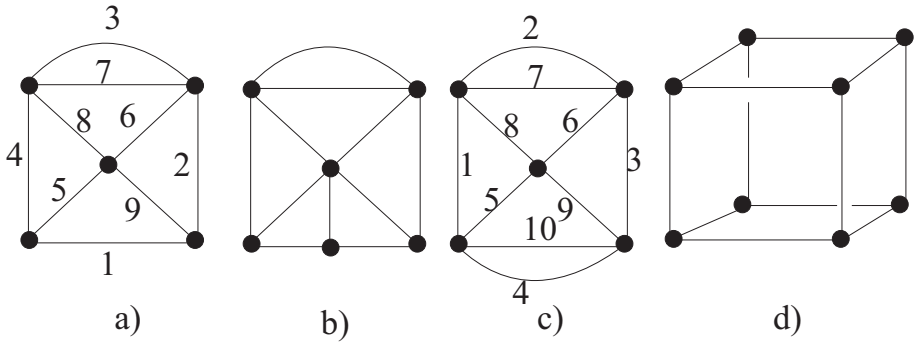
Proof. Let $n \in \mathbb{Z}$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Assume for a contradiction that $3n + 1$ is also even, so $3n + 1 = 2\ell$ for some $\ell \in \mathbb{Z}$. Then $1 = (3n + 1) - 3n = 2\ell - 6k = 2(\ell - 3k)$, which is impossible since 2 does not divide 1 (or you can say '1 is odd'). This is the required contradiction. ∎

2. Euler's argument generalizes to the following:

Theorem 1 *If a network has more than two vertices from which an odd number of edges emanate, then no tour is possible.*

Proof. Suppose for a contradiction that such a tour is possible. Pick a vertex with an odd number of edges which is neither the start nor the end of the tour. Then the tour leaves this vertex as many times as it enters it: since it enters and leaves along different edges, there must be an even number of edges at the vertex. This is the required contradiction. ∎

In order to show that a tour is *possible*, we just have to describe how we'd do it. To make this easier, some networks are shown below with numbered edges.



a) A tour is possible. Starting at the bottom left vertex, follow the edges in numbered order. (Notice that there are two vertices with an odd number of edges: any tour must start at one of these and end at the other.)

b) No tour is possible. Four of the six vertices have an odd number of edges emanating from them.

c) A tour is possible. Starting at the bottom left vertex, follow the edges in numbered order.

d) No tour is possible. The eight vertices all have an odd number (3) of edges emanating from them.

If a tour is required to begin and end at the same vertex, then we have to enter and leave *every* vertex the same number of times. Hence a tour can only be possible if *every* vertex has an even number of edges emanating from it. Thus no tour is possible for a), b), or d). However, a tour is possible for c): the one described above starts and ends at the same vertex (the bottom left vertex).

3*. Let $f(n) = n^3 - 2n^2 + 5n + 19$. Then $f(19) = 19^3 - 2 \times 19^2 + 5 \times 19 + 19$ is certainly divisible by 19 and is bigger than 19, and so cannot be prime.

Let $f(n) = 5n^4 - 2n^2 + 4n$. Then $f(2) = 5 \times 2^4 - 2 \times 2^2 + 4 \times 2$ is divisible by 2 and is bigger than 2, so cannot be prime. We could equally well have used any other value of $n > 1$.

These examples suggest a proof that integer polynomials can't always take prime values. Let $f(n) = a_r n^r + a_{r-1} n^{r-1} + \cdots + a_1 n + a_0$ be an integer polynomial. If the constant term a_0 is zero, then

$$f(2) = a_r 2^r + a_{r-1} 2^{r-1} + \cdots + 2a_1$$

is divisible by 2. If a_0 is non-zero, then

$$f(a_0) = a_r a_0^r + a_{r-1} a_0^{r-1} + \cdots + a_1 a_0 + a_0$$

is divisible by a_0. However, there are some other issues to consider:

a) Consider first the case where $a_0 \neq 0$. It's certainly true that $a_0 \mid f(a_0)$, but this doesn't necessarily mean that $f(a_0)$ is not prime – it's possible that a_0 is prime, and $f(a_0) = a_0$. (On the other hand, if $f(a_0) = 0$ or $f(a_0) < 0$, then $f(a_0)$ is *not* prime by our definition.) To get around this problem, notice that for every integer $k \geq 1$

$$f(ka_0) = a_r k^r a_0^r + a_{r-1} k^{r-1} a_0^{r-1} + \cdots + a_1 k a_0 + a_0$$

is also divisible by a_0. If there's a value of k for which $f(ka_0) \neq a_0$, then $f(ka_0)$ is not prime. However, there must be such a value, since $f(n)$ is a polynomial of degree r, and hence we can only have $f(n) = a_0$ for at most r values of n. Well, that's true *provided* $f(n)$ isn't a *constant* polynomial. If $f(n) = a_0$ is constant, and a_0 is prime, then $f(n)$ is prime for all values of n, and no amount of clever argument will change this. We'll thus have to exclude constant polynomials from our theorem.

A similar point applies when $a_0 = 0$. In this case, $f(2)$ is divisible by 2, but it may be equal to 2: however, $f(2k)$ is also divisible by 2, and can only be equal to 2 for at most r different values of k. So there's some value of k for which $f(2k)$ is not prime.

b) A more serious problem arises when $a_0 = \pm 1$. In this case, while it's true that $f(ka_0)$ is divisible by a_0 for all integers k, this doesn't tell us that some $f(ka_0)$ is not prime, since being divisible by ± 1 doesn't mean that a number isn't prime. We'll also exclude this case from our theorem.

We therefore arrive at:

Theorem 1 *Let $f(n)$ be a non-constant integer polynomial with constant term a_0. If $a_0 \neq 1$ and $a_0 \neq -1$, then there is an integer $n \geq 1$ such that $f(n)$ is not prime.*

Proof. Let

$$f(n) = a_r n^r + a_{r-1} n^{r-1} + \cdots + a_1 n + a_0$$

be a non-constant integer polynomial, and suppose that $a_0 \neq \pm 1$.

If $a_0 = 0$ then for each integer $k \geq 1$ we have

$$f(2k) = a_r 2^r k^r + a_{r-1} 2^{r-1} k^{r-1} + \cdots + 2a_1 k,$$

which is clearly divisible by 2. However, $f(2k)$ can only be equal to 2 for at most r different values of k (since $f(n)$ is non-constant), and hence there is some k for which $f(2k) \neq 2$, and is therefore not prime as required.

If $a_0 \neq 0$ then let $M = |a_0|$. Since $a_0 \neq \pm 1$ we have $M \geq 2$. Then for each integer $k \geq 1$ we have

$$f(Mk) = a_r M^r k^r + a_{r-1} M^{r-1} k^{r-1} + \cdots + a_1 Mk \pm M,$$

which is clearly divisible by M. However, $f(Mk)$ can only be equal to M for at most r different valuse of k, and hence there is some k for which $f(Mk) \neq M$, and is therefore not prime as required. ∎

In fact, the theorem is also true if $a_0 = \pm 1$, but this is harder to prove. Here's an indication (for interest only...) of how it could be done. We start with the example $f(n) = n^2 + n + 1$. The trick is to work out the polynomial with $n + 1$ in place of n:

$$F(n) = f(n+1) = (n+1)^2 + (n+1) + 1 = n^2 + 3n + 3.$$

This has constant term 3, so we know from our earlier work that it's not prime for some value $n = 3k$, where $k \geq 1$ is an integer. In this particular example, $F(3) = 21$ is not prime. However, $F(3) = f(4)$, so $f(4)$ is not prime.

In the general case, we notice that for each integer $i \geq 1$, $F(n) = f(n + i)$ has constant term $f(i)$. (If you're not sure why this is true, try it on a few examples.) So provided we can find some i for which $f(i) \neq \pm 1$, then by our theorem the corresponding $F(n) = f(n + i)$ is not prime for some choice N of n, and hence $f(N + i)$ is not prime. However $f(i)$ can only be $+1$ for at most r values of i, and it can only be -1 for at most r values of i. So integers $i \geq 1$ with $f(i) \neq \pm 1$ do exist.