WINTER 2012, MATH 312, ASSIGNMENT 1

1) For any real $r \in \mathbb{R}$, let

$[r]$ denote the integer part of r, where $[r] \leq r$ (even for r negative); and let

$\{r\}$ denote the "fractional/decimal" part of r, i.e. $\{r\} = r - [r]$. Note that $\{r\} \in [0, 1)$.

For $j \in \mathbb{Z}$, $0 \leqslant j \leqslant n+1$, consider the $n+2$ numbers $\{j\alpha\}$, which all lie in the interval $0 \leqslant \{j\alpha\} < 1$.

Partition this interval into $n+1$ subintervals

$$\frac{k-1}{n+1} \leqslant x < \frac{k}{n+1} \quad \text{for } k = 1, 2, \ldots, n, n+1.$$

As there are $n+2$ numbers and only $n+1$ intervals, by the Pigeonhole Principle, some interval contains at least 2 of the numbers.

Thus, there exist $r, s \in \mathbb{Z}$ such that

$$0 \leqslant r < s \leqslant n+1 \quad \text{and} \quad \left|\{r\alpha\} - \{s\alpha\}\right| \leqslant \frac{1}{n+1}.$$

6 marks

Now let $a = s - r$ and $b = [s\alpha] - [r\alpha]$. Since $r, s \in \mathbb{Z}$ and $0 \leq r < s \leqslant n+1$, we have $1 \leqslant a \leqslant n$.

Also,
$$|a\alpha - b| = \left|(s-r)\alpha - ([s\alpha] - [r\alpha])\right|$$
$$= \left|\{s\alpha\} - \{r\alpha\}\right| \leqslant \frac{1}{n+1}.$$

So a & b meet our requirements.

4 marks

[Total: 10 marks]

2) Let S be a countable set, i.e. there exists a bijection

$$
\begin{aligned}
f : \mathbb{N} &\longrightarrow S \\
1 &\longmapsto f(1) \\
2 &\longmapsto f(2) \\
&\vdots \\
n &\longmapsto f(n). \\
&\vdots
\end{aligned}
$$

Let E be an infinite subset of S.

Let n_1 be the smallest positive integer s.t. $f(n_1) \in E$

[Such an n_1 exists because the set $\{n \in \mathbb{N} \mid f(n) \in E\}$ is non-empty and bounded below].

Let n_2 be the smallest positive integer greater than n_1 s.t. $f(n_2) \in E$.

$\vdots$

Let n_{k+1} be the smallest positive integer greater than n_k s.t. $f(n_{k+1}) \in E$

$\vdots$

[Such a process will continue indefinitely because E is infinite].

Now consider the function

$$
\begin{aligned}
g : \mathbb{N} &\longrightarrow E \\
1 &\longmapsto f(n_1) \\
2 &\longmapsto f(n_2) \\
&\vdots \\
k &\longmapsto f(n_k) \\
&\vdots
\end{aligned}
$$

5 marks

2) (continued)

<u>Showing that g is injective</u>

Suppose $f(n_j) = f(n_k) \in E$ for $j, k \in \mathbb{N}$.

Then $n_j = n_k$ since f is injective

Then $j = k$ because the n_i's were chosen in a strictly increasing manner.

<u>Showing that g is surjective</u>

Let e be an element of E.

As $E \subseteq S$, we see that $e \in S$

As $f: \mathbb{N} \longrightarrow S$ is surjective, e is in the image of f.

In fact, as $e \in E = \{f(n_1), f(n_2), \ldots, f(n_k), \ldots\}$, we see that $e = f(n_x)$ for some $x \in \mathbb{N}$.

But then $g(x) = f(n_x) = e$.

$\Longrightarrow$ As $g: \mathbb{N} \longrightarrow E$ is a bijection, E is a countable set as well. 5 marks

[Total: 10 marks]

3) Let P_n denote the statement

"$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$"

for some given $n \in \mathbb{N}$

"Base" Case : Show P_1 is true.

$$1^2 = 1 = \frac{1}{6}(1)(1+1)(2(1)+1) \quad \checkmark$$

2 marks

"Induction Step" : Showing P_k true implies P_{k+1} true.

Suppose P_k is true for some $k \in \mathbb{N}$, i.e. suppose

$$1^2 + 2^2 + \cdots + k^2 = \frac{1}{6}k(k+1)(2k+1)$$

Then $1^2 + 2^2 + \cdots + k^2 + (k+1)^2$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2$$

$$= \frac{1}{6}(k+1)\left[k(2k+1) + 6(k+1)\right]$$

$$= \frac{1}{6}(k+1)\left[2k^2 + 7k + 6\right]$$

$$= \frac{1}{6}(k+1)(k+2)(2k+3)$$

$$= \frac{1}{6}(k+1)\left[(k+1)+1\right]\left[2(k+1)+1\right]$$

i.e. P_{k+1} is true.

Conclusion

By mathematical induction,

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$$

is true for any $n \in \mathbb{N}$.

8 marks

[Total : 10 marks]

4) $$a^3 - a = a(a^2-1)$$
$$= a(a-1)(a+1)$$
$$= \underbrace{(a-1)\cdot a \cdot (a+1)}_{\text{3 consecutive integers}}$$

For any 3 consecutive integers, exactly one of them is divisible by 3, which makes their product also divisible by 3.

[Note: this is true even if $a \leqslant 0$]

[Alternatively,

$$a^3 - a = (a-1)\cdot a \cdot (a+1)$$
$$\equiv 0 \cdot 1 \cdot 2 \pmod 3$$
$$\equiv 0 \pmod 3$$]

Total: [5 marks]

5) Let P_n denote the statement "$5 \mid n^5 - n$" for some given $n \in \mathbb{N}$

"Base" Case: Show P_1 is true. $5 \mid 1^5 - 1 = 0$ (as $0 = 5(0)$) ✓	2 marks
"Induction Step": Showing P_k true implies P_{k+1} true Suppose P_k is true for some $k \in \mathbb{N}$, i.e. suppose $5 \mid k^5 - k$, i.e. $k^5 - k = 5a$ for some $a \in \mathbb{Z}$. Then, $(k+1)^5 - (k+1) = [k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1] - [k+1]$ $= (k^5 - k) + (5k^4 + 10k^3 + 10k^2 + 5k + 1 - 1)$ $= 5a + 5(k^4 + 2k^3 + 2k^2 + k)$ $= 5(a + k^4 + 2k^3 + 2k^2 + k)$ So $5 \mid (k+1)^5 - (k+1)$ and P_{k+1} is true. Conclusion By mathematical induction, $5 \mid n^5 - n$ for all $n \in \mathbb{N}$.	8 marks
	[Total: 10 marks]

6) Existence of $\gcd(a,b)$

For $a, b \in \mathbb{Z}$ not both zero, the common divisors of a & b are a subset of the finite set of integers,

$$\{-\max\{|a|,|b|\}, -\max\{|a|,|b|\}+1, \ldots, -1, 0, 1, 2, \ldots, \max\{|a|,|b|\}\}.$$

Thus, the set of common divisors of a and b is itself a finite, ordered set and must thus have a greatest element, the gcd.

Note that the set of common divisors of a and b is non-empty because it always contains the number 1. (and actually -1 too).

Show that $\gcd(a,b) = m_0 a + n_0 b$ for $m_0, n_0 \in \mathbb{Z}$.

Let $S = \{ma + nb \mid m, n \in \mathbb{Z} \text{ and } ma + nb > 0\}$

$S \neq \emptyset$: $\left.\begin{array}{l}\text{if } m \text{ has the sign of } a \\ \text{and } n \text{ has the sign of } b\end{array}\right\}$ then $ma + nb > 0$

[Note, here, it's important that a, b not both 0]

S is bounded below by the number 0.

Thus, S has a <u>least element</u> (since we're working over the integers). Call it $S_0 = m_0 a + n_0 b$.

We seek to prove that

$$m_0 a + n_0 b = S_0 = \gcd(a,b)$$

6) (continued)

Firstly,

$$\left.\begin{array}{l} \gcd(a,b) \mid a \\ \gcd(a,b) \mid b \end{array}\right\} \Rightarrow \gcd(a,b) \mid m_0 a + n_0 b = s_0 \quad \dots (1)$$

Conversely, we seek to prove $s_0 \mid a$ & $s_0 \mid b$

[for then s_0 would be a common divisor of a & b, which means $s_0 \mid \gcd(a,b)$]

By the Division Algorithm, there exist $q, r \in \mathbb{Z}$

s.t. $a = q s_0 + r$ where $0 \leq r < s_0$

$$= q(m_0 a + n_0 b) + r$$

$$\Rightarrow (1 - q m_0) a - (q n_0) b = r$$

Case 1 $r = 0 \Rightarrow a = q s_0 + 0 \Rightarrow s_0 \mid a$.

Case 2 $r > 0 \Rightarrow$ Since r can be written as a linear combination of a & b, $r \in S$.

But $r < s_0$, so this contradicts the minimality of s_0 in S. $\times\!\!\times$ ← Contradiction

Thus, must have $s_0 \mid a$. And similarly $s_0 \mid b$.

So, $s_0 \mid \gcd(a,b) \quad \dots (2)$

(1) & (2) show that

$$\gcd(a,b) = s_0 = m_0 a + n_0 b.$$

6 marks

[Total: 10 marks]

7)

n	n^2	$(n+1)^2$	smallest prime b/w n^2 & $(n+1)^2$	
1	1	4	2	1 mark
2	4	9	5	1
3	9	16	11	1
4	16	25	17	1
5	25	36	29	1
6	36	49	37	1
7	49	64	53	1
8	64	81	67	1
9	81	100	83	1
10	100	121	101	1

[Total: 10 marks]

8) <u>Dirichlet's Theorem on Primes in Arithmetic Progressions</u>

Let a & b be relatively prime positive integers.
Then the arithmetic progression $an+b$, $n=1,2,3,\ldots$ contains infinitely many primes.

Let $a = 10$, $b = 1$.

Note that $\gcd(a,b) = \gcd(10,1) = 1$
so a & b are relatively prime positive integers. 3 marks

Then by Dirichlet's Theorem, the arithmetic progression $11, 21, 31, 41, 51, \ldots$ contains infinitely many primes.

i.e. there are infinitely many primes whose decimal expansion ends with 1. 2 marks

[Total: 5 marks]