Assignment from S-POP:

Part B(i): Exercises B(i)-1, 3, 4, 6, 7, 8, 10; **Part B(iv):** Exercises B(iv)-1, 4; **Part B(v):** Exercises B(v)-1, 3, 6; **Part B(vii): Exercises B(vii)-1, 2, 3.**

Part B(i):

3. Let a, b, and c be integers. Recall that we say "a divides b," written $a|b$, if there exists an integer q such that $b = aq$. **(a)** Prove that, if $a|b$ and $a|c$, then $a|(b+c)$. **(b)** Prove that, if $a|b$, then $a|nb$ for any integer n.

Solution: (a) Assume $a|b$ and $a|c$. Then $\exists m, n \in \mathbb{Z} : b = am$ and $c = an$. Then $b + c = a(m+n)$, and since $m+n \in \mathbb{Z}$, we conclude that $a|(b+c)$. So $a|b$ and $a|c \Rightarrow a|(b+c)$. □

(b) Assume $a|b$. Then $\exists m \in \mathbb{Z} : b = am$. So, if $n \in \mathbb{Z}$, we have $bn = (am)n = a(mn)$. Since $mn \in \mathbb{Z}$, we conclude that $a|bn$. So $a|b \Rightarrow a|nb$ for any integer n. □

4. Supply a proof by contraposition of Proposition B(i)-1_{E}.

Solution: We wish to show that, if $n-1$ is not an odd number, then n is not an even number. So assume that $n-1$ is not odd. Then $n-1$ is even. (This follows, for example, from the division algorithm, page 4 of S-POP.). So $n-1 = 2k$ for some $k \in \mathbb{Z}$. But then $n = 2k+1$ for some $k \in \mathbb{Z}$, so n is odd, so n is not even. So $n-1$ is not odd $\Rightarrow$ n is not even, or equivalently, by contraposition, n is even $\Rightarrow$ $n-1$ is odd. □

8. Consider the converse to the statement of Exercise B(i)-3(a). Is this converse statement true? If so, prove it. If not, show that it's false by counterexample.

Solution: The converse to the statement $P \Rightarrow Q$ is the statement $Q \Rightarrow P$. So we are asking: Is the statement "if $a|(b+c)$, then $a|b$ and $a|c$" true, for all integers a, b, c? The answer is **no**. Proof by counterexample: $3|(7+5)$ but $3 \nmid 7$ and $3 \nmid 5$.

Part B(iv):

4. Prove that, if $C \in \mathbb{R}$, then

$$\lim_{n\to\infty} Cx_n = C \lim_{n\to\infty} x_n,$$

providing the limit on the right exists.

Solution: Suppose $\lim_{n\to\infty} x_n$ exists: call this limit L. Let $\varepsilon > 0$ and let C be a constant: we wish to show $\exists N \in \mathbb{N}$ such that, if $n \geq N$, then $|Cx_n - CL| < \varepsilon$.

We first consider the case $C = 0$. In this case, we have $|Cx_n - CL| = 0 < \varepsilon$ automatically, and we're done.

Now suppose $C \neq 0$. Since $\lim_{n\to\infty} x_n = L$, there is, by definition of limit, an $N \in \mathbb{N}$ such that, if $n \geq N$, then $|x_n - L| < \varepsilon/|C|$. But then, for such n,

$$|Cx_n - CL| = |C| \cdot |x_n - L| < |C| \cdot (\varepsilon/|C|) = \varepsilon,$$

and we're done. □

Part B(v):

3. Use mathematical induction to prove that, for any positive integer n,

$$\frac{d}{dx}x^n = nx^{n-1}$$

(pretend you didn't already know this, although it's OK to assume it's true for $n = 1$). Hint: for the inductive step, use the product rule.

Solution: Let A_n be the statement "For any positive integer n, $\frac{d}{dx}x^n = nx^{n-1}$." To prove this by induction, we need to prove that A_1 is true, and that $A_k \Rightarrow A_{k+1}$.

First we need to demonstrate A_1: $\frac{d}{dx}x^1 = 1x^{1-1}$. That is, we need to show that $\frac{d}{dx}x = 1$. But we know this to be true from elementary calculus.

Now assume that A_k is true, meaning $\frac{d}{dx}x^k = kx^{k-1}$. Then, by A_1 and the product rule,

$$\begin{aligned}
\frac{d}{dx}x^{k+1} &= \frac{d}{dx}(x^k \cdot x) \\
&= x^k \cdot \frac{d}{dx}x + x \cdot \frac{d}{dx}x^k \\
&= x^k \cdot 1 + x \cdot (kx^{k-1}) \\
&= x^k + kx^k = (k+1)x^k,
\end{aligned}$$

so A_{k+1} follows. So we have proved by induction that A_n holds for all $n \in \mathbb{N}$, and we are done. □

6. Let A_n be the statement

$$1 + 2 + 3 + \cdots + n = \frac{(2n+1)^2}{8}.$$

Prove that if A_k is true for any positive integer k, then so is A_{k+1}. Is A_n true for all positive integers n? Explain your answer.

Solution: Assume A_k: $1+2+3+\cdots+n = (2k+1)^2/8$. Then

$$\begin{aligned} 1+2+3+\cdots+k+1 &= (1+2+3+\cdots+k)+k+1 \\ &= \frac{(2k+1)^2}{8}+k+1 \\ &= \frac{(2k+1)^2}{8}+\frac{8(k+1)}{8} \\ &= \frac{(2k+1)^2+8(k+1)}{8} \\ &= \frac{4k^2+12k+9}{8} = \frac{(2(k+1)+1)^2}{8}, \end{aligned}$$

so A_{k+1} follows.

But note that the statement A_n is not true for *any* positive integer n, since we know that $1+2+3+\cdots+n = n(n+1)/2$ (see Proposition B(v)-1_{E}), and

$$\frac{n(n+1)}{2} - \frac{(2n+1)^2}{8} = \frac{4n(n+1-(2n+1)^2}{8} = \frac{1}{8} = 0.$$

The point is that the inductive step $A_k \Rightarrow A_{k+1}$ is not always enough; you need the base step A_1 as well. And in this case A_1 fails, since $1 \neq (2\cdot 1+1)^2/8 = 9/8$.

Part B(vii):

1. Use proof by contradiction to show that there are no integers a and b with $6a+21b=1$.

Solution: Suppose there were such integers a and b. Note that $3|6$ and $3|21$. By Exercise B(i)-1, parts (a) and (b), then, we have $3|(6a+21b)$, which by assumption equals 1, so $3|1$. This contradicts the fact that $3 \nmid 1$. So there are no integers a and b with $6a+21b=1$. □

3. Prove that there are infinitely many positive prime numbers of the form $4\ell+3$ (for ℓ an integer).

Solution: Assume it is not the case that there are infinitely many prime numbers of the form $4\ell+3$: that is, assume there are finitely many, say K, prime numbers of the form $4\ell+3$. Denote these primes by $p_1, p_2, \ldots, p_K$.

Put $M = 4p_1p_2\cdots p_K - 1$, and note that

$$M = 4(p_1p_2\cdots p_K - 1) + 3,$$

so M is of the form $4\ell+3$. Because of this, M *must have a prime divisor of the form* $4\ell+3$. Why? Because every positive integer, and therefore every prime, is of the form 4ℓ, $4\ell+1$, $4\ell+2$, or $4\ell+3$. Since M is odd, it can't be divisible by any integer of the form 4ℓ or $4\ell+2$, because such numbers are even. So all prime divisors of M are of the form $4\ell+1$ or $4\ell+3$. But if all prime divisors of M were of the form $4\ell+1$, then by Exercise

B(v)-5, M would be too. Since M is not of this form, some prime divisor of M must be of the form $4\ell + 3$, as claimed.

Let p be any prime divisor of M such that p is of the form $4\ell + 3$. Then p must equal one of the primes $p_1, p_2, \ldots, p_K$, since these are the only primes of this form. Since p is one of these primes, it certainly divides the product of all these primes, so p certainly divides $N = 4p_1p_2 \cdots p_K$. But any integer dividing two integers divides their difference, so p divides $M - N$.

On the other hand, by definition of $M - N$, we have $M - N = -1$. But -1 is not divisible by any prime, so p cannot divide $M - N$.

So $p|(M-N)$ and $p\not|(M-N)$. Contradiction. So there are infinitely many prime numbers of the form $4\ell + 3$. $\square$