Morgan Saville

Discrete Maths Supervision 1

1.1.1 Take $n = 8$.
$2n + 13 = 16 + 13 = 29$ which is prime
$\therefore$ Statement 1 does not hold $\forall n$

2. Statement 2 is equivalent to the following:
If $x^2 + y = 13$ and $x = 3$ then $y = 4$ $(*)$
Proof of $(*)$:
$x^2 + y \,\big|_{x=3} = 3^2 + y = 9 + y$

Setting this equal to 13, $9 + y = 13$
$\therefore y = 4$
$\therefore (*)$ holds
$\therefore$ Statement 2 holds

3. Let n be even
$\therefore n = 2k$ for some $k \in \mathbb{Z}$ where $j = 2k^2 \in \mathbb{Z}$
$\therefore n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2j$ ~~for some $j \in \mathbb{Z}$~~
$\therefore n^2$ is even

Alternatively, let n be ~~even~~ odd
$\therefore n = 2\alpha + 1$ for some $\alpha \in \mathbb{Z}$
$\therefore n^2 = (2\alpha + 1)^2 = 4\alpha^2 + 4\alpha + 1$
$= 2(2\alpha^2 + 2\alpha) + 1$
$= 2\beta + 1$ for some $\beta \in \mathbb{Z}$
$\therefore n^2$ is odd

$\therefore n^2$ is even iff n is even.

5 $x + z = y - z \iff x + 2z = y$

$\iff 2z = y - x$

$\iff z = \frac{1}{2}(y - x)$

$\therefore$ Statement 5 is equivalent to the following

$\forall x, y \in \mathbb{Z}, \frac{1}{2}(y-x) \in \mathbb{Z}$

$\cancel{(y-x) \in \mathbb{Z}}$

$\Rightarrow y - x$ must be even

$\therefore (x, y) = (0, 1)$ is a counter example

$\therefore$ the statement is false.

4. $x + z = y - z \iff z = \frac{1}{2}(y - x)$

$\therefore$ Statement 4 is equivalent to the following:

$\forall x, y \in \cancel{\mathbb{Z}}\, \mathbb{R}, \frac{1}{2}(y - x) \in \mathbb{R}$

which is evidently true because $2 \in \mathbb{R}$, $1 \in \mathbb{R}$, and ~~the operations~~ $\mathbb{R}$ is closed under subtraction, multiplication and division.

$\therefore$ Statement 4 is true.

6. Let a, b be two rational numbers

$\therefore a = \frac{\alpha}{\beta}, \; b = \frac{\gamma}{\delta}$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$

$$\therefore a + \beta = \frac{\alpha\delta}{\beta\delta} + \frac{\beta\gamma}{\beta\delta}$$

$$= \frac{\alpha\delta + \beta\gamma}{\beta\delta}$$

$$= \frac{p}{q} \quad \text{where } p = \alpha\delta + \beta\gamma \in \mathbb{Z}, \; q = \beta\delta \in \mathbb{Z}$$

$\therefore \alpha + \beta$ is rational. $\Rightarrow$ Statement 6 is true.

7. $\frac{2y}{y+1} = x \iff 2y = x(y+1)$ for $y \neq -1$

$\iff (2-x)y = x$

$\iff y = \frac{x}{2-x}$ for $x \neq 2$

which is a bijective mapping from $x \in \mathbb{R} \setminus \{2\}$ to $y \in \mathbb{R} \setminus \{-1\}$

$\therefore \forall x \in \mathbb{R} \setminus \{2\}\ \exists$ a unique value $y \in \mathbb{R} \setminus \{-1\}$

$\therefore$ Statement 7 is true.

8. Statement 8 is equivalent to the following
$\forall m, n \in \mathbb{Z}$, if m is odd and n is odd then mn is odd
$(*)$

Proof of $(*)$.

Let $m = 2a+1$ for some $a \in \mathbb{Z}$

$n = 2b+1$ for some $b \in \mathbb{Z}$

$$\begin{aligned} mn &= (2a+1)(2b+1) \\ &= 4ab + 2a + 2b + 1 \\ &= 2(2ab + a + b) + 1 \\ &= 2c + 1 \quad \text{where } c = 2ab + a + b \in \mathbb{Z} \end{aligned}$$

$\therefore mn$ is odd

$\therefore (*)$ is true

$\therefore$ Statement 8 is true.

1.2.1 $0 \mid n \iff n = 0$

$d \mid 0 \iff d \in \mathbb{Z}$

2 $(km) \mid (kn) \iff (kn) = \alpha(km)$ for some $\alpha \in \mathbb{Z}$

$\iff n = \alpha m$ because $k \neq 0$

$\iff m \mid n$

3 Note: $2 \mid 2^n \iff 2^n = 2\alpha$ for some $\alpha \in \mathbb{Z}$

- $2^n = 2 \cdot 2^{n-1} \quad \forall\, n \in \mathbb{N}$
- $2^{n-1} \in \mathbb{Z} \quad \forall\, n \in \mathbb{N}$

$\therefore\ 2^n = 2\alpha$ where $\alpha = 2^{n-1} \in \mathbb{Z} \quad \forall\, n \in \mathbb{N}$

$\iff 2 \mid 2^n$.

4. ~~$30 \mid n \iff n = 30k$ for some $k \in \mathbb{Z}$~~

$2 \mid n \wedge 3 \mid n \wedge 5 \mid n \iff n = 2a = 3b = 5c$ for some $a, b, c \in \mathbb{Z}$

$\iff n = k(2 \cdot 3 \cdot 5)$ for some $k \in \mathbb{Z}$

$\iff n = 30k$

$\iff 30 \mid n$

5. $(k, m, n) = (2, 2, 2)$ is a counterexample

6. $l \mid m \iff m = al$ for some $a \in \mathbb{Z}$

$m \mid n \iff n = bm$ for some $b \in \mathbb{Z}$

$\therefore (l \mid m) \wedge (m \mid n) \implies n = bm$ for some $b \in \mathbb{Z}$

$\implies n = b(al)$ for some $a, b \in \mathbb{Z}$

$\implies n = cl$ where $c = ab \in \mathbb{Z}$

$\implies l \mid n$

7a. $d \mid m \wedge d \mid n \implies m = ad \wedge n = bd$ for some $a, b \in \mathbb{Z}$

$\implies m + n = ad + bd$

$= (a+b)d$

$\implies m + n = cd$ where $c = a + d \in \mathbb{Z}$

$\implies d \mid (m+n)$

b. $d|m \Rightarrow m = ad$ for some $a \in \mathbb{Z}$.
$\Rightarrow km = kad \quad \forall k \in \mathbb{Z}$
$\Rightarrow km = bd$ where $b = ka \in \mathbb{Z}$
$\Rightarrow d \,|\, km$

c. $(d|m) \wedge (d|n) \Rightarrow m = ad \wedge n = bd$ for some $a, b \in \mathbb{Z}$
$\Rightarrow km + ln = kad + lbd$ ~~for some~~ $\forall k, l \in \mathbb{Z}$
$= d(ka + lb)$
$\Rightarrow km + ln = cd$ where $c = ka + lb \in \mathbb{Z}$
$\Rightarrow d \,|\, (km + ln)$

8. $(m|n) \wedge (n|m) \Rightarrow n = am \wedge m = bn$ for some $a, b \in \mathbb{Z}$
$\Rightarrow n = abn$
$\Rightarrow ab = 1$
$\Rightarrow a = b = 1 \vee a = b = -1$

$\therefore (m|n) \wedge (n|m) \Rightarrow (n = -m) \vee (n = m)$

9. $(k, m, n) = (6, 3, 4)$ is a counterexample
$\therefore$ Statement 9 is false

10a. $P^{\#}(l) = \forall k \in \mathbb{N}_0, 0 \leq k \leq l \Rightarrow P(k)$.
~~Take l = k,~~ Assuming $P^{\#}(l)$, take $k = l$
$0 \leq l \leq l \Rightarrow P(l)$
$\therefore P(l)$
$\therefore P^{\#}(l) \Rightarrow P(l)$

b. $P(m) =$ m is even
For $n = 4$, $P(n)$ is true
However, $P^{\#}(n) = P^{\#}(4) \Rightarrow \forall\, 0 \leq k \in \mathbb{N}_0 \leq 4, P(k)$
For example, for $k = 3$, $P(k)$ is false, and so $P^{\#}(n)$ is false.
$\therefore P(n) \Rightarrow P^{\#}(n)$ does not hold

c. $P^{\#}(0) = \forall\ 0 \leq k \in \mathbb{N}_0 \leq 0,\ P(k)$

$= \forall\ k \in \{0\},\ P(k)$

$= P(0)$

d. $(P^{\#}(n) \Rightarrow P^{\#}(n+1)) \iff (P^{\#}(n) \Rightarrow \forall\ 0 \leq k \in \mathbb{N}_0 \leq n+1,\ P(k))$

$\iff (P^{\#}(n) \Rightarrow P(n+1) \land \forall\ 0 \leq k \in \mathbb{N}_0 \leq n,\ P(k))$

$\iff (P^{\#}(n) \Rightarrow P(n+1) \land P^{\#}(n))$

$\iff (P^{\#}(n) \Rightarrow P(n+1))$

e. $P^{\#}(m)\ \forall\ m \in \mathbb{N}_0 \implies P^{\#}(m)$ for arbitrarily large m

$\iff \forall\ 0 \leq k \in \mathbb{N}_0 \leq m,\ P(k)$

$\iff \forall\ 0 \leq k \in \mathbb{N}_0,\ P(k)$

$\iff \forall\ k \in \mathbb{N}_0,\ P(k)$

$P(k)\ \forall\ k \in \mathbb{N}_0 \iff \forall\ 0 \leq k \in \mathbb{N}_0 \leq m,\ P(k)$ for arbitrarily large m

$\iff \forall\ 0 \leq k \in \mathbb{N}_0 \leq n+l,\ P(k)$ where $n, l \in \mathbb{N}_0,\ n \leq m,\ l = m-n$ ~~where $n, l \in \mathbb{N}_0$, $n+l=m$~~

$\iff (\forall\ 0 \leq k \in \mathbb{N}_0 \leq n,\ P(k)) \land (\forall\ n+1 \leq k \in \mathbb{N}_0 \leq l,\ P(k))$

$\implies (\forall\ 0 \leq k \in \mathbb{N}_0 \leq n,\ P(k)) \quad \forall\ n \in \mathbb{N}_0$

$\iff P^{\#}(n)\ \forall\ n \in \mathbb{N}_0$

$\therefore P^{\#}(n)\ \forall n \in \mathbb{N}_0 \iff P(n)\ \forall n \in \mathbb{N}_0$

1.3.1a. $t_3 = 6$

$t_4 = 10$

$t_5 = 15$

b. $(n+1)^2 = \sum_{i=0}^{n} (i+1)^2 - \sum_{i=0}^{n} i^2$

$= \sum_{i=0}^{n} (i^2+2i+1) - \sum_{i=0}^{n} i^2$

$= \sum_{i=0}^{n} (2i+1)$

$$\therefore (n+1)^2 = \left(2\sum_{i=0}^{n} i\right) + (n+1)$$

$$\therefore (n+1)^2 - (n+1) = 2\sum_{i=0}^{n} i$$

$$\therefore t_n = \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

c. n is triangular $\iff n = \frac{k(k+1)}{2}$ for some $k \in \mathbb{Z}^+$

$$\iff 8n = 4k(k+1)$$

$$\iff 8n+1 = 4k(k+1)+1$$

$$= 4k^2 + 4k + 1$$

$$= (2k+1)^2$$

$$= j^2 \text{ where } j = 2k+1 \in \mathbb{Z}^+$$

$$\iff 8n+1 \text{ is square}$$

d. Let t_n and t_{n+1} be two consecutive triangular numbers

$$t_n = \frac{n(n+1)}{2}, \quad t_{n+1} = \frac{(n+1)(n+2)}{2}$$

$$t_n + t_{n+1} = \frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2}$$

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

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

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

$$= (n+1)(n+1)$$

$$= (n+1)^2$$

$$= k^2 \text{ where } k = n+1 \in \mathbb{Z}$$

$\therefore t_n + t_{n+1}$ is square.

e.g. n is triangular $\longrightarrow n = \frac{k(k+1)}{2}$ for some $k \in \mathbb{Z}_0^+$

$$\Longrightarrow 9n+1 = \frac{9k(k+1)+2}{2}$$

$$= \frac{9k^2+9k+2}{2}$$

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

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

$$= \frac{j(j+1)}{2} \quad \text{where } j = 3k+1 \in \mathbb{Z}_0^+$$

$$\Longrightarrow 25n+3 = \frac{25k(k+1)+6}{2}$$

$$= \frac{25k^2+25k+6}{2}$$

$$= \frac{(5k+2)(5k+3)}{2}$$

$$= \frac{l(l+1)}{2} \quad \text{where } l = 5k+2 \in \mathbb{Z}_0^+$$

$$\Longrightarrow 49n+6 = \frac{49k(k+1)+12}{2}$$

$$= \frac{49k^2+49k+12}{2}$$

$$= \frac{(7k+3)(7k+4)}{2} \quad \cancel{\text{where}}$$

$$= \frac{m(m+1)}{2} \quad \text{where } m = 7k+3 \in \mathbb{Z}_0^+$$

$$\Longrightarrow 81n+10 = \frac{81k(k+1)+20}{2}$$

$$= \frac{81k^2+81k+20}{2}$$

$$= \frac{(9k+4)(9k+5)}{2}$$

$$= \frac{p(p+1)}{2} \quad \text{where } p = 9k+4 \in \mathbb{Z}_0^+$$

f. Note that $(2n+1)^2 t_k + t_n$

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

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

$\therefore$ Statement f is equivalent to the following:

$\forall\, n, k \in \mathbb{N}_0,\ \exists\, q \in \mathbb{N}_0$ such that $\frac{q(q+1)}{2} = \frac{k(k+1)(2n+1)^2 + n(n+1)}{2}$

$$\iff q(q+1) = k(k+1)(2n+1)^2 + n(n+1) \quad (*)$$

Proof of $(*)$:

$$k(k+1)(2n+1)^2 + n(n+1) = (k^2+k)(4n^2+4n+1) + (n^2+n)$$
$$= 4k^2n^2 + 4k^2n + k^2 + 4kn^2 + 4kn + k + n^2 + n$$

$$= (2kn+k+n)^2 + (2kn+k+n)$$
$$= (2kn+k+n)(2kn+k+n+1)$$
$$= q(q+1) \quad \text{where } q = 2kn+k+n \in \mathbb{N}_0$$

$\therefore (*)$ is true

$\therefore$ Statement f is true.

Let $A = ((\exists x . P(x)) \Rightarrow Q)$

$B = (\forall x . (P(x) \Rightarrow Q))$

Case 0: $\exists x . P(x)$

Take x' such that $P(x')$ is true

$A \Rightarrow Q$

$B : P(x') \Rightarrow$

$\therefore B \Rightarrow Q$

Case 1 $\nexists x . P(x)$

$A \not\Rightarrow Q$

$B \not\Rightarrow Q$

these cases are exhaustive

$\therefore A \iff B$

2.1.1.a. $i = 0m + i \Rightarrow lm+i = km+i$ where $l, k = 0 \in \mathbb{Z}$

$\Rightarrow i \equiv i \pmod{m}$

b. $i \equiv j \pmod{m}$

$\iff lm+i = km+j$ for some $l, k \in \mathbb{Z}$

$\iff km+j = lm+i$

$\iff j \equiv i \pmod{m}$

c. $i \equiv j \pmod{m} \wedge j \equiv k \pmod{m}$

$\iff lm+i = rm+j \wedge pm+j = qm+k$ for some $l, r, p, q \in \mathbb{Z}$

$\iff lm+i = rm+(qm+k-pm)$

$= rm+qm-pm+k$

$= (r+q-p)m+k$

$= sm+k$ where $s = r+q-p \in \mathbb{Z}$

$\iff i \equiv k \pmod{m}$

2 a. $i \equiv j \pmod m \wedge k \equiv l \pmod m$

$\Rightarrow am+i = bm+j \wedge cm+k = dm+l$ for some $a,b,c,d \in \mathbb{Z}$

$\Rightarrow am+i+cm+k = bm+j+dm+l$

$\Rightarrow (a+c)m+(i+k) = (b+d)m+(j+l)$

$\Rightarrow em+(i+k) = fm+(j+l)$ where $e = a+c \in \mathbb{Z}$

$f = b+d \in \mathbb{Z}$

$\Rightarrow i+k \equiv j+l \pmod m$

b. $i \equiv j \pmod m \wedge k \equiv l \pmod m$

$\Rightarrow am+i = bm+j \wedge cm+k = dm+l$ for some $a,b,c,d \in \mathbb{Z}$

$\Rightarrow (am+i)(cm+k) = (bm+j)(dm+l)$

$\Rightarrow acm^2 + im + km + ik = bdm^2 + jm + lm + jl$

$\Rightarrow (acm+i+k)m + ik = (bdm+j+l)m + jl$

$\Rightarrow em + ik = fm + jl$ where $e = acm+i+k \in \mathbb{Z}$

$f = bdm+j+l \in \mathbb{Z}$

$\Rightarrow ik \equiv jl \pmod m$

c. $i \equiv j \pmod m$

$\Rightarrow am+i = bm+j$ for some $a,b \in \mathbb{Z}$

$\Rightarrow (am+i)^n = (bm+j)^n \quad \forall n \in \mathbb{N}_0$

$\Rightarrow \sum_{k=0}^{n} \binom{n}{k} (am)^k i^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (bm)^k j^{n-k}$

$\Rightarrow i^n + \sum_{k=1}^{n} \binom{n}{k} (am)^k i^{n-k} = j^n + \sum_{k=1}^{n} \binom{n}{k} (bm)^k j^{n-k}$

$\Rightarrow i^n + am \sum_{k=1}^{n} \binom{n}{k} (am)^{k-1} i^{n-k} = j^n + bm \sum_{k=1}^{n} \binom{n}{k} (bm)^{k-1} j^{n-k}$

$\Rightarrow cm + i^n = dm + j^n$ where $c = a\sum_{k=1}^{n} \binom{n}{k} (am)^{k-1} i^{n-k} \in \mathbb{Z}$

$d = b\sum_{k=1}^{n} \binom{n}{k} (bm)^{k-1} j^{n-k} \in \mathbb{Z}$

$\Rightarrow i^n \equiv j^n \pmod m$

3. Note that $^{(*)}$ $rem(a,b) = rem(c,b) \iff a \equiv c \pmod{b}$

a. $km + l = l$

$\therefore \operatorname{dm}(km+l) = jm + l$ where $d, j = 0 \in \mathbb{Z}$

$\therefore km + l \equiv l \pmod{m}$

$\therefore rem(km+l, m) = rem(l, m)$ by $(*)$

b. $k = am + rem(k,m)$ for some $a \in \mathbb{Z}$

$\therefore k \equiv rem(k,m) \pmod{m}$

$\therefore k + l \equiv rem(k,m) + l \pmod{m}$

$\therefore rem(k+l, m) = rem(rem(k,m)+l, m)$ by $(*)$

c. $l = am + rem(l,m)$ for some $a \in \mathbb{Z}$

$\therefore l \equiv rem(l,m) \pmod{m}$

$\therefore kl \equiv k\, rem(l,m) \pmod{m}$

$\therefore rem(kl, m) = rem(k\, rem(l,m), m)$ by $(*)$

4. a. $(i+j)+k \equiv i+(j+k) \pmod{m}$

$\iff am + ((i+j)+k) = bm + (i+(j+k))$ for some $a, b \in \mathbb{Z}$

$\iff am + (i+j+k) = bm + (i+j+k)$

which is evidently true, for example, $a = b$

$(ij)k \equiv i(kj) \pmod{m}$

$\iff am + ((ij)k) = bm + (i(jk))$ for some $a, b \in \mathbb{Z}$

$\iff am + ijk = bm + ijk$

$\therefore$ which is evidently true, for example, $a = b$

b. $i + j \equiv 0 \pmod{m}$

$\iff am + (i+j) = bm + 0$ for some $a, b \in \mathbb{Z}$

$\iff am + i = bm + (-j)$

$\iff i \equiv -j \pmod{m}$