University of Windsor
Department of Mathematics and Statistics
Mathematical Foundations MATH 1020
Practice Questions for Midterm Test 2

---

1. Prove $\forall x, y, z \in \mathbb{Z}$, if x divides y and y divides z, then x divides z.

Proof.
Let $x, y, z \in \mathbb{Z}$.
Assume x divides y and y divides z.
Let $a, b \in \mathbb{Z}$ with $y = ax$ and $z = by$.
Let $c = ab$.
$z = by = b(ax) = cx$.
Therefore, $\exists c \in \mathbb{Z}$, $z = cx$. i.e., x divides z.
Therefore, if x divides y and y divides z, then x divides z.
QED $\square$

2. Prove $\forall x, y \in \mathbb{Z}$, if xy is even and y is odd, then $x + y$ is odd.

Proof.
Let $x, y \in \mathbb{Z}$.
Assume xy is even and y is odd.
Let $a, b \in \mathbb{Z}$ with $xy = 2a$ and $y = 2b + 1$.
Let $c = a - bx + b$.
$2a = xy = x(2b + 1) = 2bx + x$, and so $x = 2a - 2bx$.
Then $x + y = 2a - 2bx + 2b + 1 = 2(a - bx + b) + 1 = 2c + 1$.
Therefore, $\exists c \in \mathbb{Z}$, $x + y = 2c + 1$. i.e., $x + y$ is odd.
Therefore, if xy is even and y is odd, then $x + y$ is odd.
QED $\square$

3. Prove $\forall x, y \in \mathbb{Z}$, if $x + y$ is odd, then $x - y$ is odd.

Proof.
Let $x, y \in \mathbb{Z}$. Assume $x + y$ is odd.
Let $a \in \mathbb{Z}$ with $x + y = 2a + 1$.
Let $b = a - y$.
$x - y = x + y - 2y = 2a + 1 - 2y = 2(a - y) + 1 = 2b + 1$.
Therefore, $x - y$ is odd.
Therefore, if $x + y$ is odd, then $x - y$ is odd.
QED $\square$

4. Prove $\forall x, y \in \mathbb{Z}$, if 3 divides xy and 3 divides $y - 1$, then 3 divides x.

Proof.
Let $x, y \in \mathbb{Z}$.
Assume 3 divides xy and 3 divides $y - 1$.
Let $a, b \in \mathbb{Z}$ with $xy = 3a$ and $y - 1 = 3b$.
Let $c = a - xb$.
$x = xy - xy + x = xy - x(y - 1) = 3a - x(3b) = 3(a - xb) = 3c$.
Therefore, $\exists c \in \mathbb{Z}$, $x = 3c$. i.e., 3 divides x.
Therefore, if 3 divides xy and 3 divides $y - 1$, then 3 divides x.
QED $\square$

5. Prove $\forall x \in \mathbb{Z}$, if 2 divides x and 5 divides x, then 10 divides x.

Proof.
Let $x \in \mathbb{Z}$.
Assume 2 divides x and 5 divides x.
Let $a, b \in \mathbb{Z}$ with $x = 2a$ and $x = 5b$.
Let $c = a - 2b$.
$x = 5x - 4x = 5(2a) - 4(5b) = 10a - 20b = 10(a - 2b) = 10c$.
Therefore, $\exists c \in \mathbb{Z}$, $x = 10c$. i.e., 10 divides x.
Therefore, if 2 divides x and 5 divides x, then 10 divides x.
QED $\square$

6. Prove $\forall a, x, y \in \mathbb{Z}$, if a divides $x + y$ and a divides $2x + y$, then a divides x and a divides y.

Proof.
Let $a, x, y \in \mathbb{Z}$.
Assume a divides $x + y$ and a divides $2x + y$.
Let $s, t \in \mathbb{Z}$ with $x + y = as$ and $2x + y = at$.
Let $u = t - s$ and let $v = 2s - t$.
Then $x = 2x + y - (x + y) = at - as = a(t - s) = au$.
And, $y = 2x + 2y - (2x + y) = 2as - at = a(2s - t) = av$.
Therefore, a divides x and a divides y.
Therefore, if a divides $x + y$ and a divides $2x + y$, then a divides x and a divides y.
QED $\square$

7. Using a proof by contradiction and the well-ordering property, prove $\forall x \in \mathbb{Z}$, if x is odd, then $\forall n \in \mathbb{N}$, x^n is odd.

Proof.
Let $x \in \mathbb{Z}$.
Assume x is odd and $\exists n \in \mathbb{N}$, x^n is not odd.
Let $n \in \mathbb{N}$ be smallest with x^n not odd.
Since x^1 is odd but x^n is not odd, we have $n \neq 1$. This means $n - 1 \in \mathbb{N}$.
Since n is smallest in $\mathbb{N}$ with x^n not odd and $n - 1 \in \mathbb{N}$, we have that x^{n-1} is odd.
Since now x is odd and x^{n-1} is odd, let $a, b \in \mathbb{Z}$ with $x = 2a + 1$ and $x^{n-1} = 2b + 1$.
Let $c = bx + a$.
$x^n = x(x^{n-1}) = x(2b + 1) = 2bx + x = 2bx + 2a + 1 = 2c + 1$.
Therefore, x^n is odd, which is a contradiction, since x^n is not odd.
Therefore, if x is odd, then $\forall n \in \mathbb{N}$, x^n is odd.
QED $\square$

8. Using a proof by contradiction and the well-ordering property, prove $\forall x \in \mathbb{R}$, if $2 < x$, then $\forall n \in \mathbb{N}$, $2^n < x^n$.

Proof.
Let $x \in \mathbb{R}$.
Assume $2 < x$ and $\exists n \in \mathbb{N}$ with $x^n \leq 2^n$.
Let $n \in \mathbb{N}$ be smallest with $x^n \leq 2^n$.
Since $2^1 < x^1$ but $x^n \leq 2^n$, we have $n \neq 1$. This means $n - 1 \in \mathbb{N}$.
Note that since $2 < x$, we have $0 < x$, and so $x^n(x^{-1}) \leq 2^n(x^{-1})$. Then $x^{n-1} \leq 2^n x^{-1}$.
Also, since $2 < x$, we have $x^{-1} < 2^{-1}$, and so $(2^n)x^{-1} < (2^n)2^{-1}$. Then $2^n x^{-1} < 2^{n-1}$.
Since $x^{n-1} \leq 2^n x^{-1}$ and $2^n x^{-1} < 2^{n-1}$, we have $x^{n-1} \leq 2^{n-1}$.
This contradicts n be the smallest natural number with this property.
Therefore, if $2 < x$, then $\forall n \in \mathbb{N}$, $2^n < x^n$.
QED □

9. Prove $\forall x \in \mathbb{R}$, if $0 \leq x < 1$, then $\exists n \in \mathbb{N}$, $\frac{n-1}{n} \leq x < \frac{n}{n+1}$.

Proof.
Let $x \in \mathbb{R}$.
Assume $0 < x < 1$.
Since $x < 1$, we have $0 < 1 - x$.
By the Archimedean property, $\exists n \in \mathbb{N}$, $x < (1 - x)n$.
Let $n \in \mathbb{N}$ be smallest with $x < (1 - x)n$.
Then $x < n - nx$, and so $x + nx < n$. i.e., $x(n + 1) < n$, giving us $x < \frac{n}{n+1}$.
Case 1: $n = 1$.
Since $0 \leq x$, we have $n - 1 \leq x$, and so $\frac{n-1}{n} \leq x$.
Case 2: $1 < n$.
In this case, $0 < n - 1$, and so $n - 1 \in \mathbb{N}$.
Since n is smallest in $\mathbb{N}$ with $x < (1 - x)n$, we then have $(1 - x)(n - 1) \leq x$.
Then $n - 1 - x(n - 1) \leq x$, and so $n - 1 \leq x + x(n - 1)$.
This gives us $n - 1 \leq nx$, and so $\frac{n-1}{n} \leq x$.
Therefore, $\exists n \in \mathbb{N}$, $\frac{n-1}{n} \leq x < \frac{n}{n+1}$.
QED □

10. Using the principle of mathematical induction, prove $\forall x \in \mathbb{Z}$, if $\exists a \in \mathbb{Z}$, $x = 6a + 3$, then $\forall n \in \mathbb{N}$, $\exists b \in \mathbb{Z}$, $x^n = 6b + 3$.

Proof.
Let $x \in \mathbb{Z}$, and assume $\exists a \in \mathbb{Z}$, $x = 6a + 3$. Let $a \in \mathbb{Z}$ with $x = 6a + 3$.
Let $S = \{k \in \mathbb{N} \mid \exists b \in \mathbb{Z}, x^k = 6b + 3\}$.
Since $x^1 = x = 6a + 3$, we have $1 \in S$.
Let $n \in S$.
Then $\exists b \in \mathbb{Z}$, $x^n = 6b + 3$. Choose $b \in \mathbb{Z}$ with $x^n = 6b + 3$.
Let $c = 6ab + 3a + 3b + 1$.
$x^{n+1} = x^n x = (6b + 3)(6a + 3) = 36ab + 18a + 18b + 9 = 36ab + 18a + 18b + 6 + 3$.
Then $x^{n+1} = 6(6ab + 3a + 3b + 1) + 3 = 6c + 3$.
Thus, $n + 1 \in S$.
Therefore, S is inductive.
By the PMI, $\forall n \in \mathbb{N}$, $n \in S$. i.e., $\forall n \in \mathbb{N}$, $\exists b \in \mathbb{Z}$, $x^n = 6b + 3$.
QED □

11. Using the principle of mathematical induction, prove $\forall x \in \mathbb{Z}$, if 3 divides $x-1$, then $\forall n \in \mathbb{N}$, 3 divides $x^n - 1$.

Proof.
Let $x \in \mathbb{Z}$.
Assume 3 divides $x - 1$
Let $a \in \mathbb{Z}$ with $x - 1 = 3a$.
Let $S = \{k \in \mathbb{N} \mid 3 \text{ divides } x^k - 1\}$.
Since $x^1 - 1 = x - 1 = 3a$, we have $1 \in S$.
Let $n \in S$.
Let $b \in \mathbb{Z}$ with $x^n - 1 = 3b$.
Let $c = bx + a$.

$$\begin{aligned} x^{n+1} - 1 &= x^{n+1} - x + x - 1 \\ &= (x^n - 1)x + x - 1 \\ &= 3bx + 3a \\ &= 3(bx + a) \\ &= 3c \end{aligned}$$

Thus, 3 divides $x^{n+1} - 1$. Therefore, $n + 1 \in S$.
Therefore, S is inductive.
By the PMI, $\forall n \in \mathbb{N}$, $n \in S$. i.e., $\forall n \in \mathbb{N}$, 3 divides $x^n - 1$.
Therefore, if 3 divides $x - 1$, then $\forall n \in \mathbb{N}$, 3 divides $x^n - 1$.
QED □

12. Using the principle of mathematical induction, prove $\forall a, x, y \in \mathbb{Z}$, if a divides $x - y$, then $\forall n \in \mathbb{N}$, a divides $x^n - y^n$.

Proof.
Let $a, x, y \in \mathbb{Z}$.
Assume a divides $x - y$
Let $p \in \mathbb{Z}$ with $x - y = ap$.
Let $S = \{k \in \mathbb{N} \mid a \text{ divides } x^k - y^k\}$.
Since $x^1 - y^1 = x - y = ap$, we have $1 \in S$.
Let $n \in S$.
Let $q \in \mathbb{Z}$ with $x^n - y^n = aq$.
Let $r = qx + py^n$.

$$\begin{aligned} x^{n+1} - y^{n+1} &= x^{n+1} - y^n x + y^n x - y^{n+1} \\ &= (x^n - y^n)x + y^n(x - y) \\ &= aqx + apy^n \\ &= a(qx + py^n) \\ &= ar \end{aligned}$$

Thus, a divides $x^{n+1} - y^{n+1}$. Therefore, $n + 1 \in S$.
Therefore, S is inductive.
By the PMI, $\forall n \in \mathbb{N}$, $n \in S$. i.e., $\forall n \in \mathbb{N}$, a divides $x^n - y^n$.
Therefore, if a divides $x - y$, then $\forall n \in \mathbb{N}$, a divides $x^n - y^n$.
QED □

13. Using the principle of mathematical induction, prove $\forall x \in \mathbb{R}$, if $0 < x < 1$, then $\forall n \in \mathbb{N}$, $x^n < 1$.

Proof.
Let $x \in \mathbb{R}$.
Assume $0 < x < 1$.
Let $S = \{k \in \mathbb{N} \mid x^k < 1\}$.
Since $x^1 < 1$ by our assumption, we have $1 \in S$.
Let $n \in S$.
Then $x^n < 1$.
Since $0 < x$, we have $x^n(x) < 1(x)$, and so $x^{n+1} < x$.
Now, $x^{n+1} < x$ and $x < 1$, which gives us $x^{n+1} < 1$. Therefore, $n + 1 \in S$.
Therefore, S is inductive.
By the PMI, $\forall n \in \mathbb{N}$, $n \in S$. i.e., $\forall n \in \mathbb{N}$, $x^n < 1$.
Therefore, if $0 < x < 1$, then $\forall n \in \mathbb{N}$, $x^n < 1$.
QED □

14. Using the principle of mathematical induction, prove $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} 4k + 3 = 2n^2 + 5n$.

Proof.
Let $S = \{n \in \mathbb{N} \mid \sum_{k=1}^{n} 4k + 3 = 2n^2 + 5n\}$.
$\sum_{k=1}^{1} 4k + 3 = 4(1) + 3 = 7 = 2 + 5 = 2(1)^2 + 5(1)$.
Thus, $1 \in S$.
Let $n \in S$.
Then $\sum_{k=1}^{n} 4k + 3 = 2n^2 + 5n$.

$$\begin{aligned}
\sum_{k=1}^{n+1} 4k + 3 &= \left(\sum_{k=1}^{n} 4k + 3\right) + 4(n+1) + 3 \\
&= 2n^2 + 5n + 4(n+1) + 3 \\
&= 2n^2 + 4n + 7 + 5n \\
&= 2n^2 + 4n + 2 + 5 + 5n \\
&= 2(n^2 + 2n + 1) + 5(n+1) \\
&= 2(n+1)^2 + 5(n+1)
\end{aligned}$$

Thus, $n + 1 \in S$.
Therefore, S is inductive.
By the PMI, $\forall n \in \mathbb{N}$, $n \in S$.
QED □

15. Using the principle of mathematical induction, prove $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} \frac{1}{2^k} = 1 - \frac{1}{2^n}$.

Proof.
Let $S = \left\{ n \in \mathbb{N} \;\middle|\; \sum_{k=1}^{n} \frac{1}{2^k} = 1 - \frac{1}{2^n} \right\}$.
$\sum_{k=1}^{1} \frac{1}{2^k} = \frac{1}{2^1} = \frac{1}{2} = 1 - \frac{1}{2} = 1 - \frac{1}{2^1}$.
Thus, $1 \in S$.
Let $n \in S$.
Then $\sum_{k=1}^{n} \frac{1}{2^k} = 1 - \frac{1}{2^n}$.

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{1}{2^k} &= \left(\sum_{k=1}^{n} \frac{1}{2^k} \right) + \frac{1}{2^{n+1}} \\
&= 1 - \frac{1}{2^n} + \frac{1}{2^{n+1}} \\
&= 1 - \frac{2}{2^{n+1}} + \frac{1}{2^{n+1}} \\
&= 1 - \frac{1}{2^{n+1}}
\end{aligned}$$

Thus, $n + 1 \in S$.
Therefore, S is inductive.
By the PMI, $\forall n \in \mathbb{N}$, $n \in S$.
QED □

16. Prove $\forall a, b \in \mathbb{R}$, if $a < b$, then $(-\infty, b) \setminus (-\infty, a) = [a, b)$.

Proof.
Let $a, b \in \mathbb{R}$.
Assume $a < b$.
Let $x \in \mathbb{R}$ and assume $x \in (-\infty, b) \setminus (-\infty, a)$.
Then $x \in (-\infty, b)$, so $x < b$, and $x \notin (-\infty, a)$, so $a \leq x$.
Since $a \leq x$ and $x < b$, we have $x \in [a, b)$.
Therefore, $\forall x \in \mathbb{R}$, if $x \in (-\infty, b) \setminus (-\infty, a)$, then $x \in [a, b)$.
Thus, $(-\infty, b) \setminus (-\infty, a) \subseteq [a, b)$.
Conversely, let $x \in \mathbb{R}$ and assume $x \in [a, b)$.
Then $a \leq x$ and $x < b$.
Since $a \leq x$, we have $x \notin (-\infty, a)$.
Since $x < b$, we have $x \in (-\infty, b)$.
Now, $x \in (-\infty, b)$ and $x \notin (-\infty, a)$, so $x \in (-\infty, b) \setminus (-\infty, a)$.
Therefore, $[a, b) \subseteq (-\infty, b) \setminus (-\infty, a)$.
Therefore, $(-\infty, b) \setminus (-\infty, a) = [a, b)$.
Therefore, if $a < b$, then $(-\infty, b) \setminus (-\infty, a) = [a, b)$.
Therefore, $\forall a, b \in \mathbb{R}$, if $a < b$, then $(-\infty, b) \setminus (-\infty, a) = [a, b)$. □

17. Prove $(-\infty, 3] \setminus (1, 2) = (-\infty, 1] \cup [2, 3]$.

Proof.
Let $x \in \mathbb{R}$ and assume $x \in (-\infty, 3] \setminus (1, 2)$.
Then $x \in (-\infty, 3]$, so $x \leq 3$, and $x \notin (1, 2)$, so either $x \leq 1$ or $2 \leq x$.
Case 1: $x \leq 1$.
In this case, we have $x \in (-\infty, 1]$, so $x \in (-\infty, 1] \cup [2, 3]$.
Case 2: $2 \leq x$.
Now, $2 \leq x$ and $x \leq 3$, so $x \in [2, 3]$.
This implies that $x \in (-\infty, 1] \cup [2, 3]$.
Therefore, $(-\infty, 3] \setminus (1, 2) \subseteq (-\infty, 1] \cup [2, 3]$.
Conversely, let $x \in \mathbb{R}$ and assume $x \in (-\infty, 1] \cup [2, 3]$.
Then $x \in (-\infty, 1]$ or $x \in [2, 3]$.
Case 1: $x \in (-\infty, 1]$.
In this case, $x \leq 1$, so $x \notin (1, 2)$.
Also, since $x \leq 1$ and $1 \leq 3$, we have $x \leq 3$, so $x \in (-\infty, 3]$.
Now, $x \in (-\infty, 3]$ and $x \notin (1, 2)$, so $x \in (-\infty, 3] \setminus (1, 2)$.
Case 2: $x \in [2, 3]$.
In this case, $2 \leq x$, so $x \notin (1, 2)$, and $x \leq 3$, so $x \in (-\infty, 3]$.
Again, we have $x \in (-\infty, 3]$ and $x \notin (1, 2)$, so $x \in (-\infty, 3] \setminus (1, 2)$.
Therefore, $(-\infty, 1] \cup [2, 3] \subseteq (-\infty, 3] \setminus (1, 2)$.
Therefore, $(-\infty, 3] \setminus (1, 2) = (-\infty, 1] \cup [2, 3]$. □

18. Prove $\langle 5 \rangle \cap \langle 4 \rangle = \langle 20 \rangle$.

Proof.
Let $x \in \mathbb{Z}$ and assume $x \in \langle 5 \rangle \cap \langle 4 \rangle$.
Then $x \in \langle 5 \rangle$ and $x \in \langle 4 \rangle$.
Choose $a, b \in \mathbb{Z}$ with $x = 5a$ and $x = 4b$.
Put $c = b - a$.
$x = 5x - 4x = 5(4b) - 4(5a) = 20b - 20a = 20c$.
Therefore, $\exists c \in \mathbb{Z}$, $x = 20c$.
Thus, $x \in \langle 20 \rangle$.
Therefore, $\langle 5 \rangle \cap \langle 4 \rangle \subseteq \langle 20 \rangle$
Conversely, let $x \in \mathbb{Z}$ and assume $x \in \langle 20 \rangle$.
Accordingly, choose $q \in \mathbb{Z}$ with $x = 20q$.
Put $s = 4q$.
Then $x = 20q = 5(4q) = 5s$.
Therefore, $\exists s \in \mathbb{Z}$, $x = 5s$, which means $x \in \langle 5 \rangle$.
Put $t = 5q$.
$x = 20q = 4(5q) = 4t$.
Therefore, $\exists t \in \mathbb{Z}$, $x = 4t$. Thus, $x \in \langle 4 \rangle$.
We now have $x \in \langle 5 \rangle$ and $x \in \langle 4 \rangle$, which means $x \in \langle 5 \rangle \cap \langle 4 \rangle$.
Therefore, $\langle 20 \rangle \subseteq \langle 5 \rangle \cap \langle 4 \rangle$.
Therefore, $\langle 5 \rangle \cap \langle 4 \rangle = \langle 20 \rangle$. □

19. Prove $\forall m, n \in \mathbb{Z}$, if m divides n, then $n + \langle m \rangle = \langle m \rangle$.

Proof.
Let $m, n \in \mathbb{Z}$.
Assume m divides n.
Choose $q \in \mathbb{Z}$ with $n = mq$.
Let $x \in n + \langle m \rangle$.
Choose $a \in \mathbb{Z}$ with $x = n + ma$.
Let $b = q + a$.
Now, $x = n + ma = mq + ma = m(q + a) = mb$.
This proves $x \in \langle m \rangle$.
Thus, $n + \langle m \rangle \subseteq \langle m \rangle$.
Conversely, let $x \in \langle m \rangle$.
Choose $u \in \mathbb{Z}$ with $x = mu$.
Let $v = u - q$.
Now, $x = mu = n + mu - n = n + mu - mq = n + m(u - q) = n + mv$.
This proves $x \in n + \langle m \rangle$.
Thus, $\langle m \rangle \subseteq n + \langle m \rangle$.
Therefore, $n + \langle m \rangle = \langle m \rangle$.
Therefore, if m divides n, then $n + \langle m \rangle = \langle m \rangle$.
QED. □

20. Prove $\langle 10 \rangle + \langle 15 \rangle = \langle 5 \rangle$.

Proof.
Let $x \in \langle 10 \rangle + \langle 15 \rangle$.
Choose $a, b \in \mathbb{Z}$ with $x = 10a + 15b$.
Let $c = 2a + 3b$.
Now, $x = 10a + 15b = 5(2a + 3b) = 5c$.
Thus, $x \in \langle 5 \rangle$.
Therefore, $\langle 10 \rangle + \langle 15 \rangle \subseteq \langle 5 \rangle$.
Conversely, let $x \in \langle 5 \rangle$.
Choose $u \in \mathbb{Z}$ with $x = 5u$.
Let $v = -u$.
Now, $x = 5u = -10u + 15u = 10v + 15u$.
This proves $x \in \langle 10 \rangle + \langle 15 \rangle$.
Therefore, $\langle 5 \rangle \subseteq \langle 10 \rangle + \langle 15 \rangle$.
QED. □