Name: ______________________________

# 1 Leftovers from Test 1

1. Prove that $1+2+3+\cdots+n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

2. Prove that $1+3+5+\cdots+(2n-1) = n^2$ for all $n \in \mathbb{N}$.

3. Define the sequence $a_n$ as follows

$$a_1 = 1 \text{ and for } n > 1,\ a_n = \sqrt{a_{n-1}+2}$$

   (a) Compute the first four terms of the sequence.
   (b) Prove $a_n$ is increasing. That is, prove $a_n < a_{n+1}$ for all $n \in \mathbb{N}$.
   (c) Prove $a_n < 4$ for all $n \in \mathbb{N}$.

4. Complete the following definitions.

   - Let $f : A \to B$ we say $f$ is **injective** if and only if ...
   - Let $f : A \to B$ we say $f$ is **surjective** if and only if ...

5. Define the function $f : [2,5] \to [2,11]$ by $f(x) = 3x-4$. Prove $f$ is injective and prove $f$ in surjective.

6. Define the function $f : (0,\infty) \to (0,1)$ by $f(x) = \frac{x}{x+1}$. Prove $f$ is injective and prove $f$ in surjective.

7. Prove the following for the functions $f : A \to B$ and $g : B \to C$.

   (a) If $f$ is injective and $g$ is injective then $g \circ f$ is injective.
   (b) If $f$ is surjective and $g$ is surjective then $g \circ f$ is surjective.
   (c) If $g \circ f$ is injective then $f$ is injective.
   (d) If $g \circ f$ is surjective then $g$ is surjective.

# 2 Cardinality

8. Complete the following definitions for the sets $A$ and $B$.

   - $A \sim B$ if and only if ...
   - $A$ is **finite** if and only if ...
   - $A$ is **denumerable** if and only if ...

- $A$ is **countable** if and only if ...
- $A$ is **uncountable** if and only if ...

9. Prove the following pairs of sets have the same cardinality.
   (a) $A = (3, 5)$ and $B = (3, 20)$
   (b) $A = [3, 5)$ and $B = (3, 20]$
   (c) $(0, 1)$ and $(0, \infty)$
   (d) $\mathbb{N}$ and $E = \{2n | n \in \mathbb{N}\}$ (the evens)
   (e) $\mathbb{N}$ and $\mathbb{Z}$
   (f) $\mathbb{N}$ and $\mathbb{Q}^+$
10. Prove $\mathbb{R}$ is uncountable.
11. Prove if $A$ is uncountable and $B$ is uncountable then $A \setminus B$ is countable.
12. Prove the irrationals are uncountable.

## 3 Number Theory

13. Let $a, b, c \in \mathbb{Z}$. If $a|b$ then $a|bc$.
14. Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$ where $b \neq 0$ then $a|c$.
15. Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$ then $a|(bx + cy)$ for every pair of integers $x, y$.
16. Let $a, b \in \mathbb{N}$. If $a|b$ then $a \leq b$.
17. Prove. Let $a, b, c \in \mathbb{Z}$ with $a, c \neq 0$. If $a|b$ and $c|d$ then $ac|(ad + bc)$.
18. Prove. Let $a, b, c \in \mathbb{Z}$ with $a, c \neq 0$. If $ac|bc$ then $a|b$.
19. Prove $3|(n^3 - n)$ for all $n \in \mathbb{Z}$.
20. Find a pair of integers $x$, $y$ so that $ax + by = gcd(a, b)$ for each pair below.
   (a) $a = 17$ and $b = 125$
   (b) $a = 85$ and $b = 126$
   (c) $a = 168$ and $b = 40$
21. Let $a$ and $b$ be odd integers. Prove $4|(a - b)$ or $4|(a + b)$.
22. Let $a$ be an odd integer. Prove $8|a^2 - 1$.

23. Let $a$ and $b$ be integers, not both zero, where $d = \gcd(a, b)$. Prove for all $k \in \mathbb{N}$ that $k \gcd(a, b) = \gcd(ka, kb)$.
24. Let $a \in Z$ and $n \in \mathbb{N}$ . Prove $\gcd(a + n, a)|n$
25. Let $n \in \mathbb{N}$. If $n|35m + 26$ and $n|7m + 3$ for some integer $m$, what can $n$ be?
26. Let $a, b, c$ be integers with $a \neq 0$. Prove if $a|bc$ and $\gcd(a, b) = 1$ then $a|c$.
27. Let $b, c \in \mathbb{Z}$ and $p$ be a prime. Prove If $p|bc$ then $p|b$ or $p|c$.
28. Prove or disprove the following:
    (a) For all $n \in \mathbb{Z}$, $2n$ and $4n + 3$ are relatively prime.
    (b) For all $n \in \mathbb{Z}$, $2n + 1$ and $3n + 2$ are relatively prime.
29. Prove $\sqrt{5}$ is irrational.
30. There are infinitely many primes.
31. Prove If $k$ is composite then $2^k - 1$ is composite.
32. Prove If $2^k - 1$ is prime then $k$ is prime.

# 4 The Symmetric Group

33. Write out the set $S_4$.
34. How many elements are in the sets $S_3$, $S_5$ and $S_n$?
35. For the following elements of $S_4$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

    (a) Compute $\sigma \circ \tau$.
    (b) Compute $\gamma^3$.
    (c) Compute $\sigma^{-1}$.
    (d) Compute $(\sigma \circ \tau)^{-1}$.
    (e) Compute $\sigma^{-1} \circ \tau^{-1}$.
    (f) Compare Problem 35d and Problem 35e.
36. Write down the multiplication table for the following subsets of $S_3$.
    (a) $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$
    (b) $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$

# 5 Group Theory

37. Complete the following definitions.

- $*$ is a **binary operation** on the set S if and only if ...
- $(G, *)$ is a **group** if and only if ...
- $(G, *)$ is an **Abelian group** if and only if ...

38. Which properties (G1, G2 or G3) fails for the following binary operations.

(a) Let $*$ be defined on $\mathbb{R}^+$ by $a * b = \sqrt{ab}$.

(b) Let * be defined on $\mathbb{R}^+$ by $a * b = a/b$.

(c) Let $*$ be defined on $\mathbb{R}^+$ by $a * b = a + b + ab$.

39. Define the following algebraic structure $(\mathbb{Z}, *)$ by $a * b = a + b - 2$.

(a) Compute 1*2, 2*3, 0*0 and 4*2.

(b) What is the identity of this algebraic structure? Call it $e$.

(c) Prove $(\mathbb{Z}, *)$ satisfies G1. That is, Prove
if $a, b, c \in \mathbb{Z}$ then $a * (b * c) = (a * b) * c$.

(d) Prove $(\mathbb{Z}, *)$ satisfies G2. That is, Prove that the $e$ you identified in Problem 39b satisfies
$a * e = e * a = a$ for all $a \in \mathbb{Z}$.

(e) Prove $(\mathbb{Z}, *)$ satisfies G3. That is, Prove
if $a \in \mathbb{Z}$ then there is $b \in \mathbb{Z}$ so that $a * b = b * a = e$.

(f) Prove $(\mathbb{Z}, *)$ satisfies G4. That is, Prove
if $a, b \in \mathbb{Z}$ then $a * b = b * a$.

40. Define the following algebraic structure $(\mathbb{Q}^+, *)$ by $a * b = 4ab$.

(a) Compute $1 * \frac{1}{2}$, $4 * 1$, $\frac{1}{4} * \frac{1}{3}$ and $4 * 2$.

(b) What is the identity of this algebraic structure? Call it $e$.

(c) Prove $(\mathbb{Q}^+, *)$ satisfies G1. That is, Prove
if $a, b, c \in \mathbb{Q}^+$ then $a * (b * c) = (a * b) * c$.

(d) Prove $(\mathbb{Q}^+, *)$ satisfies G2. That is, Prove that the $e$ you identified in Problem 40b satisfies
$a * e = e * a = a$ for all $a \in \mathbb{Q}^+$.

(e) Prove $(\mathbb{Q}^+, *)$ satisfies G3. That is, Prove
if $a \in \mathbb{Z}$ then there is $b \in \mathbb{Q}^+$ so that $a * b = b * a = e$.

(f) Prove $(\mathbb{Q}^+, *)$ satisfies G4. That is, Prove
if $a, b \in \mathbb{Q}^+$ then $a * b = b * a$.

41. Definitions of **closed**.

42. For the group $(S_3, \circ)$ Show

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

is a group.

43. For the group $(S_3, \circ)$ Show

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

is **not** a group.