Math 780/780I **Test 1** Name: Answer Key.

1. (a) State the ***binomial theorem.***

Solution: For any real numbers x and y and integer $n \geq 0$

$$(x+y)^n = \sum_{k=1}^{n} \binom{n}{k} x^k y^{n-k}$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

(These numbers are the ***binomial coefficients***.) $\square$

(b) Prove $\displaystyle\sum_{k=0}^{n} (-2)^k \binom{n}{k} = (-1)^n$

Solution: In part (a) let $x = -2$ and $y = 1$ to get

$$(-1)^n = (-2+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-2)^k 1^{n-k} = \sum_{k=0}^{n} (-2)^k \binom{n}{k}.$$ $\square$

2. (a) State the ***Fundamental Theorem of Summation Theory.***

Solution: Let $f \colon \mathbb{Z} \to \mathbb{R}$ be a function from the integers to the real numbers, and let F be an anti-difference of f, that is $\Delta F = f$, where $\Delta F(x) = F(x+1) - F(x)$ is the difference operator. Then for any integers $a < b$

$$\sum_{k=a}^{b} f(x) = F(b+1) - F(a).$$

(This is the discrete analogue of the Fundamental Theorem of Calculus, $\int_a^b f(x)\, dx = F(b) - F(a)$ where F is an anti-derivative of f, that is $F' = f$.) $\square$

(b) Define the ***third following power*** $x^{\underline{3}}$.

Solution: This is

$$x^{\underline{3}} = x(x-1)(x-2).$$

More generally for any positive integer p the corresponding falling powers is

$$x^{\underline{p}} = \underbrace{x(x-1)\cdots(x-p+1)}_{p \text{ terms in the product}}.$$ $\square$

(c) Show that $\Delta x^{\underline{3}} = 3x^{\underline{2}}$.

Solution: Using the definition of of the difference operator Δ,

$$\begin{aligned}
\Delta x^{\underline{3}} &= \Delta(x+1)^{\underline{3}} - \Delta x^{\underline{3}} \\
&= (x+1)x(x-1) - x(x-1)(x-2) \\
&= \big((x+1)-(x-2)\big)x(x-1) && \text{(Factor out } x(x-1).\text{)} \\
&= 3x^{\underline{2}}.
\end{aligned}$$

□

(d) Compute $\displaystyle\sum_{k=1}^{42} k(k-1)$.

Solution: From part (b) we have that if $f(x) = x^{\underline{2}}$ and $F(x) = \frac{1}{3}x^{\underline{3}}$ then $\Delta F = f$. Thus from the Fundamental Theorem of Summation Theory

$$\begin{aligned}
\sum_{k=1}^{42} k(k-1) &= \sum_{k=1}^{42} k^{\underline{2}} \\
&= \frac{43^{\underline{3}}}{3} - \frac{1^{\underline{3}}}{3} \\
&= \frac{43^{\underline{3}}}{3} - 0 \\
&= \frac{43 \cdot 42 \cdot 41}{3}.
\end{aligned}$$

If was fine to leave the answer like that. If you did want to multiply it out the result is

$$\sum_{k=1}^{42} k(k-1) = \frac{43 \cdot 42 \cdot 41}{3} = 24{,}682.$$

□

3. (a) Define p is a ***prime number***.

Solution: The integer p is prime iff $p > 1$ and the only positive factors of p are p and 1. □

(b) Prove there are infinitely many prime numbers.

Solution: Towards a contradiction, assume that there are only[1] finitely many primes. Let $p_1, p_2, \ldots, p_n$ a list of all the primes. Let

$$N = p_1 p_2 \cdots p_n + 1.$$

[1]Many of you said "assume there are finitely many primes", when it should be "there are only finitely many primes". That there are finitely many primes, does not rule out that there are infinitely many primes.

This will have at least one prime factor. Let p be a prime factor of N. Then $p \neq p_j$ for any j as p divides evenly into N, while each p_j has a remainder of 1 when divided into N. Thus p is a prime not in the list $p_1, p_2, \ldots, p_n$, contradicting that this was a list of all the primes. $\square$

4. State the ***Fundamental Theorem of Arithmetic***.

Solution: Each integer greater than one has a unique factorization into primes. Explicitly an integer $a > 1$ there are primes $p_1, p_2, \ldots, p_m$ (repeats are allowed) with

$$a = p_1 p_2 \cdots p_m.$$

By uniqueness we mean that if $q_1 q_2, \ldots, q_n$ are also primes with

$$a = q_1 q_2 \cdots q_m$$

then $m = n$ and after reordering $p_j = q_j$ for $j = 1, 2, \ldots, m$. $\square$

5. (a) Define a ***divides*** b. That is $a \mid b$.

Solution: This means that $a \neq 0$ and there is an integer k such that $b = ak$. $\square$

(b) If $a \mid b$ prove that $2a^3$ divides $8b^5 + 6a^3c$ for any integer c.

Solution: As $a \mid b$, there is an integer k such that $b = ak$. Then

$$8b^5 + 6a^3c = 8(ak)^5 + 6a^3c = 2a^3(4a^2k^5 + 3c) = 2a^2k'$$

where $k' = (4a^2k^5 + 3c)$ is an integer. Therefore $2a^3 \mid (b^5 + 6a^3c)$ $\square$

(c) Show that if n is positive and odd, that $5^n + 3^n$ is divisible by 8.

Solution: We use the identity

$$(x + y)^n = (x + y)(x^{n-1} - x^{n-1}y + x^{n-3}y^2 - \cdots + y^{n-1})$$

which holds for all odd $n \geq 1$. Letting $x = 5$ and $y = 3$ gives

$$5^n + 3^n = (5 + 3)\left(5^{n-1} - 5^{n-2}3 + \cdots + 3^{n-1}\right) = 8(\text{Some integer})$$

and so $8 \mid (5^n + 3^n)$. $\square$

6. (a) Define what it means for $I \subseteq \mathbb{Z}$ to be an ***ideal.***

Solution: $I \subseteq \mathbb{Z}$ is an ideal iff $I \neq \varnothing$,

(i) If $x, y \in I$, then $x + y \in I$. (Closed under sums)
(ii) If $x \in I$ and $a \in \mathbb{Z}$ then $ax \in I$. (Closed under multiplication by elements of $\mathbb{Z}$.) $\square$

(b) Let $a \in \mathbb{Z}$. Define the ***principal ideal*** I_a.

Solution: I_a is the set of all multiples of a. That is

$$I_a = \{ka : k \in \mathbb{Z}\}.$$

$\square$

(c) State the ***division algorithm***.

Solution: For any integers a and b with $a \neq 0$, there are unique integers q and r such that

$$b = qa + r \qquad \text{and} \qquad 0 \leq r < |a|.$$

Note: On this several you just wrote "$b = qa + r$ with $0 \leq r < |a|$" without say that q and r depend on a and b. But it is *very important.* In application of the division algorithm we start with $a \neq 0$ and b, and then find the quotient q and remainder r. $\square$

(d) Let $I \neq \{0\}$ be an ideal and let a be the smallest positive element of I. Use the division algorithm to prove that $I = I_a$.

Solution: As $a \in I$ and any element of I_a is a multiple of a, we see any element of I_a is an element of I as I is closed under multiplication by elements of $\mathbb{Z}$. Therefore $I_a \subseteq I$.

Let $b \in I$. By the division algorithm there are integers q and r with

$$b = qa + r \qquad \text{and} \qquad 0 \leq r < a.$$

(We have $r < a$ rather than $r < |a|$ as a is positive.) Then $r = b + (-q)a$ and $b \in I$ (by assumption), $(-q)a \in I$ (as $a \in I$ and I is closed under multiplication by elements of $\mathbb{Z}$), and therefore $r = b + (-q)a$ (I is closed under sums). If $r \neq 0$ then r would be a positive element of I which is less than a, contradicting that a is the smallest positive element of I. Therefore $r = 0$.

But $r = 0$ gives that $b = qa$ and therefore $b \in I_a$. As b was an arbitrary element of I this implies $I \subseteq I_a$. Whence we have $I \subseteq I_a$ and $I_a \subseteq I$ which implies $I = I_a$ as required. $\square$

7. (a) Define the ***greatest common divisor*** of a and b.

Solution: d is the ***greatest common divisor*** of a and b iff a and b are not both zero, $d \mid a$, $d \mid b$, and if c is any integer that divides both a and b, $c \leq d$. We write $d = \gcd(a, b)$. $\square$

(b) State ***Bézout's theorem***.

Solution: Let a and b are integers, not both zero, then there are integers x and y such that
$$ac + by = \gcd(a, b).$$
□

(c) Define what it means for a and b to be ***relatively prime.***

Solution: a and b are ***relatively prime*** iff $\gcd(a, b) = 1$. □

(d) Use Bézout's theorem to prove that if $\gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Solution: As $a \mid bc$, there is an integer k such that
$$bc = ak.$$
Because $\gcd(a, b) = 1$, Bézout's gives us integers x and y such that
$$ax + by = 1.$$
Multiply this by c
$$acx + bcy = c.$$
Use $bc = ak$ in this to get
$$acx + aky = c$$
which implies $c = a(cx + ky)$. As $(cx + ky)$ is an integer this gives that $a \mid c$. □

8. Define a sequence of integers h_n by
$$h_1 = 1, \qquad h_2 = 2, \qquad \text{and for } n \geq 3 \qquad h_n = h_{n-1} + 2h_{n-2}.$$
Compute h_1, h_2, h_3, h_4, h_5, make a guess on the value of h_n, and prove your result by induction.

Solution: To start:
$$\begin{aligned}
h_1 &= 1 \\
h_2 &= 2 \\
h_3 &= h_2 + 2h_1 = 2 + 2 \cdot 1 = 4 = 2^2 \\
h_4 &= h_3 + 2h_2 = 4 + 2 \cdot 2 = 8 = 2^3 \\
h_5 &= h_4 + 2h_3 = 8 + 2 \cdot 4 = 16 = 2^4.
\end{aligned}$$
Form this we conjecture $h_n = 2^{n-1}$.

We now proves this holds by induction. A good base case is $n = 1$, as $h_1 = 1 = 2^{1-1}$ or $h_2 = 2 = 2^{2-1}$.

Now assume the result is true for n, that is $h_n = 2^{n-1}$, and also $h_{n-1} = 2^{n-2}$. This is our induction hypothesis. We now wish to show the result holds for $n+1$, that is that $h_{n+1} = 2^{(n+1)-1}$.

$$
\begin{aligned}
h_{n+1} &= h_n + 2h_{n-1} && \text{(From the recursion defining the sequence)} \\
&= 2^{n-1} + 2 \cdot 2^{n-2} && \text{(From the induction hypothesis.)} \\
&= 2^{n-1} + 2^{n-1} \\
&= 2 \cdot 2^{n-1} \\
&= 2^n \\
&= 2^{(n+1)-1}
\end{aligned}
$$

which closes the induction and completes the proof. $\square$