Number Theory - Test #1 - Solutions

Summer 2023

Pat Rossi Name ______________________

Instructions

Show CLEARLY how you arrive at you answers.

You can look in your text for reference (Statements of theorems, definitions, etc.)

Do not search the internet, or consult with others, for solutions (other than, perhaps, my own website)

Due June 20, 2023 at 1pm

1. State the **Well Ordering Principle**

   Every non-empty set of non-negative integers (natural numbers) has a least (smallest) element.

   Alternativley, let S be a non-empty set of non-negative integers (natural numbers). Then $\exists\ x \in S$ such that $\forall s \in S$, $x \leq s$.

2. State the **First Principle of Mathematical Induction** (First Principle of Finite Induction)

   Let S be a set of positive integers having the following properties:

   (a) The integer $1 \in S$

   (b) Whenever $k \in S$, $k+1 \in S$ also.

   Then $S = \mathbb{N}$

3. State the **Binomial Theorem**

   For any real numbers a and b, and any natural number n, the following holds:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

   Or equivalently:

   For any real numbers a and b, and any natural number n, the following holds:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{i} b^{n-i}$$

4. State **Pascal's Rule**

   $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$; for $1 \leq k \leq n$

5. State the **Division Algorithm**

   Given integers a and b, with $b > 0$, there exist unique integers q and r such that

   $$a = qb + r \quad \text{with } 0 \leq r < b.$$

   q is called the *quotient* and r is called the *remainder.*

6. Define **greatest common divisor** of a and b, denoted $\gcd(a, b)$

   Let a and b be integers, with at least one of them not equal to zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the positive integer d satisfying the following:

   (a) $d|a$ and $d|b$

   (b) If $c|a$ and $c|b$, then $c \leq d$.

7. State **Divisibility Theorem 1**

   Suppose that integers a, b, c are such that $a|c$ and $b|c$ and such that $\gcd(a, b) = 1$. Then $(ab)\,|c$.

8. State **Divisibility Theorem 2 (Euclid's Lemma)**

   Suppose that integers a, b, c, are such that $a|bc$ and such that $\gcd(a, b) = 1$. Then $a|c$.

9. Define **relatively prime**

   Let a and b be integers, with at least one of them not equal to zero. Then a and b are said to be *relatively prime* exactly when $\gcd(a, b) = 1$.

   Alternatively, a and b are said to be *relatively prime* exactly when a and b have no common divisors larger than 1.

10. State **Theorem 2.2** (from our text)

For integersa, b, c, d, the following hold:

(a) $a|0, 1|a, a|a$

(b) $a|1 \Leftrightarrow a = \pm 1$

(c) If $a|b$ and $c|d$, Then $ac|bd$

(d) If $a|b$ and $b|c$, then $a|c$

(e) $a|b$ and $b|a \Leftrightarrow a = \pm b$

(f) If $a|b$ and $b \neq 0$, then $|a| \leq |b|$

(g) If $a|b$ and $a|c$, then $a|\,(bx + cy)$ for all $x, y \in \mathbf{N}$

11. Prove by Induction: $1+5+9+\ldots+(4n-3)=2n^2-n$

i.e., $\underbrace{\sum\limits_{i=1}^{n}(4i-3)=2n^2-n}_{P(n)}$

Proof.

$\boxed{\text{Show } P(n) \text{ is true for } n=1}$

$\sum\limits_{i=1}^{1}(4i-3)=4(1)-3=1=2(1)^2-(1)$

i.e., $\sum\limits_{i=1}^{1}(4i-3)=2(1)^2-(1)$

$\boxed{\text{Assume } P(n) \text{ is true for } n=k; \text{show } P(n) \text{ is true for } n=k+1}$

i.e., Assume that $\underbrace{\sum\limits_{i=1}^{k}(4i-3)=2k^2-k}_{\text{(induction hypothesis)}}$ is true, and show that this implies that

$\sum_{i=1}^{k+1}(4i-3)=2(k+1)^2-(k+1)$ is true.

(i.e., show that $\sum_{i=1}^{k+1}(4i-3)=(k+1)(2k+1)$ is true.)

Observe: $\sum_{i=1}^{k+1}(4i-3)=\left(\sum_{i=1}^{k}(4i-3)\right)+((4(k+1)-3))=(2k^2-k)+((4(k+1)-3))$

by induction hypothesis

$$=(2k^2+3k+1)=(k+1)(2k+1).$$

i.e., $\sum_{i=1}^{k+1}i=(k+1)(2k+1)$.

Thus, $\sum_{i=1}^{n}(4i-3)=2n^2-n$ for all natural numbers, n. ■

12. Prove by Induction: $2 \cdot 6 \cdot 10 \cdot 14 \cdot \ldots \cdot (4n-2) = \frac{(2n)!}{n!}$

i.e., $\prod_{i=1}^{n} (4i-2) = \frac{(2n)!}{n!}$

Proof.

$\boxed{\text{Show true for } n = 1}$

$$\prod_{i=1}^{1} (4i-2) = (4(1)-2) = 2 = \tfrac{2}{1} = \tfrac{(2(1))!}{(1)!}$$

i.e., $\prod_{i=1}^{1} (4i-2) = \frac{(2(1))!}{(1)!}$

$\boxed{\text{Assume true for } n = k; \text{show true for } n = k+1}$

i.e., Assume that $\underbrace{\prod_{i=1}^{k} (4i-2) = \frac{(2k)!}{k!}}_{\text{(induction hypothesis)}}$ is true, and show that this implies that

$\prod_{i=1}^{k+1} (4i-2) = \frac{[2(k+1)]!}{(k+1)!}$ is true.

Observe: $\prod_{i=1}^{k+1} (4i-2) = \left(\prod_{i=1}^{k} (4i-2)\right)[4(k+1)-2] = \frac{(2k)!}{k!}[4(k+1)-2] = \frac{(2k)!}{k!}[4k+2]$

by induction hypothesis

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

$$= \frac{[2(k+1)]!}{(k+1)!}.$$

i.e., $\prod_{i=1}^{k+1} (4i-2) = \frac{(2k+2)!}{(k+1)!}$.

Thus, $\prod_{i=1}^{n} (4i-2) = \frac{(2n)!}{n!}$ for all natural numbers, n. ∎

13. Prove: $\binom{n}{0}3^n - \binom{n}{1}3^{n-1} + \binom{n}{2}3^{n-2} - \binom{n}{3}3^{n-3} + \ldots + (-1)^n = 2^n$

Proof.

Observe: $2^n = (3 + (-1))^n = \sum_{i=0}^{n} \binom{n}{i} 3^{n-i} (-1)^i$

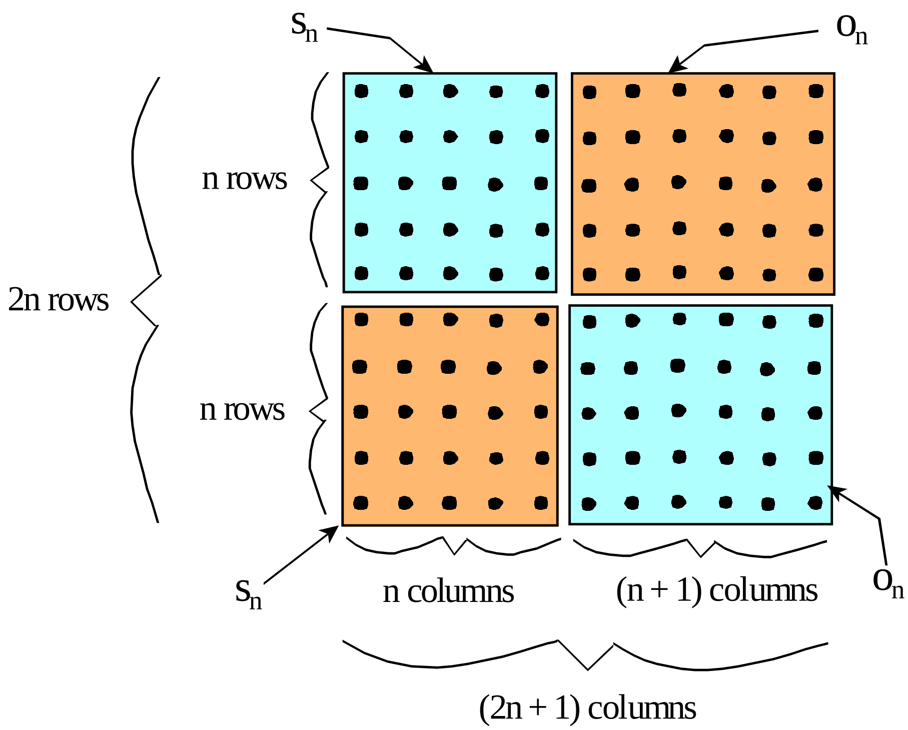
$$= \binom{n}{0}3^n - \binom{n}{1}3^{n-1} + \binom{n}{2}3^{n-2} - \binom{n}{3}3^{n-3} + \ldots + (-1)^n \quad \blacksquare$$

14. Show, algebraically and with "dot diagrams," that $2o_n + 2s_n = o_{2n}$

Algebraically: $2o_n + 2s_n = 2n(n+1) + 2n^2 = 2n[(n+1) + n] = 2n(2n+1) = o_{2n}$

i.e., $2o_n + 2s_n = o_{2n}$

Using "dot diagrams:"



The entire array of dots, 2n rows and (2n + 1) columns, constitutes o_{2n}

15. Show, algebraically and with "dot diagrams," that $o_n + o_{n+1} + 2s_{n+1} = s_{2n+2}$

Algebraically: $o_n + o_{n+1} + 2s_{n+1} = n(n+1) + (n+1)[(n+1)+1] + 2(n+1)^2$

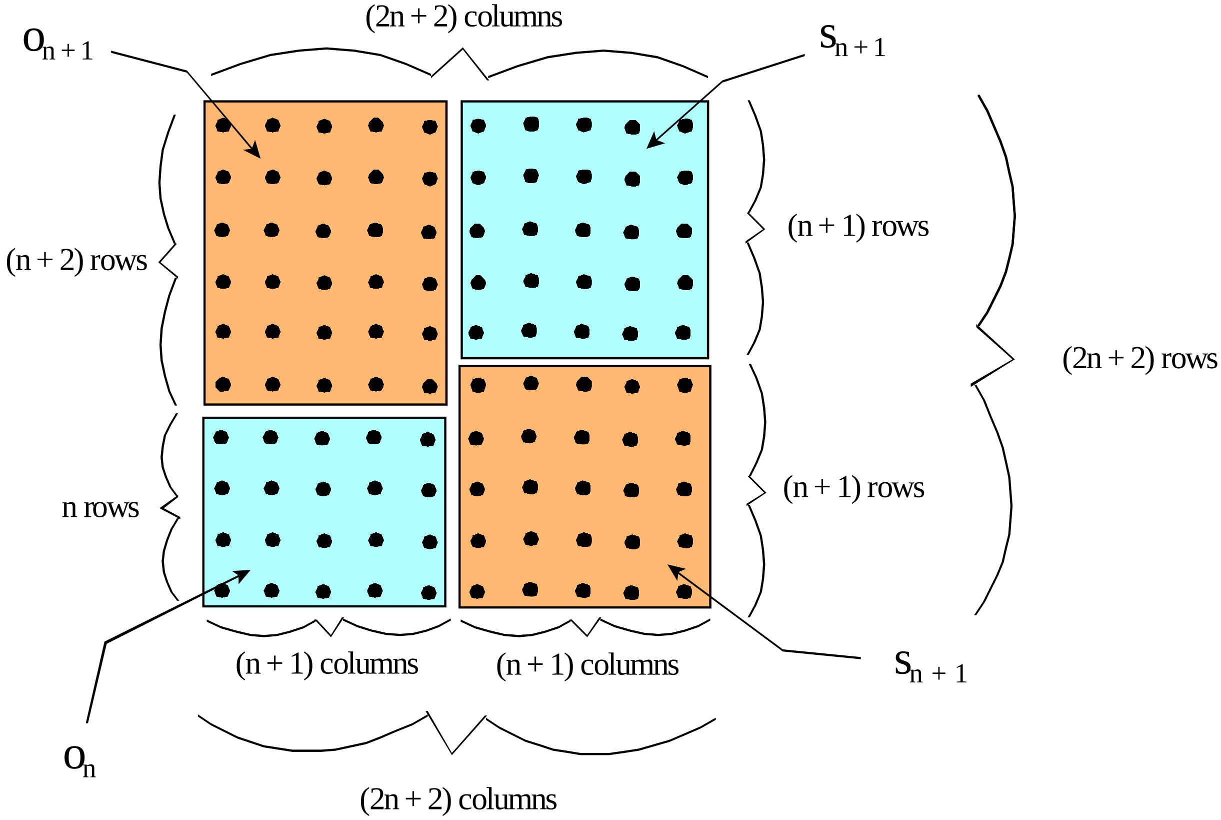
$= n(n+1) + (n+1)(n+2) + 2(n+1)^2 = (n+1)[n+(n+2)] + 2(n+1)^2$

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

$= 4(n+1)^2 = 2^2(n+1)^2 = [2(n+1)]^2 = (2n+2)^2 = s_{2n+2}$

i.e., $o_n + o_{n+1} + 2s_{n+1} = s_{2n+2}$

Using "dot diagrams:"



The entire array of dots, (2n + 2) rows and (2n + 2) columns, constitutes S_{2n+2}

16. Prove that the cube of a natural number cannot be of the form $4n + 2$

Let m be an integer. By the Division Algorithm, either:

$$m = 4k$$
$$m = 4k + 1$$
$$m = 4k + 2$$
$$m = 4k + 3$$

Observe:

If $m = 4k$, then:

$m^3 = (4k)^3 = 64k^3 = 4\,(16k^3) = 4n$, where $n = 16k^3$

If $m = 4k + 1$, then:

$m^3 = (4k+1)^3 = 64k^3 + 48k^2 + 12k + 1 = 4\,(16k^3 + 12k^2 + 3k) + 1$

$= 4n + 1$, where $n = 16k^3 + 12k^2 + 3k$

If $m = 4k + 2$, then:

$m^3 = (4k+2)^3 = 64k^3 + 96k^2 + 48k + 8 = 4\,(16k^3 + 24k^2 + 12k + 2) = 4n$,

where $n = 16k^3 + 24k^2 + 12k + 2$

If $m = 4k + 3$, then:

$m^3 = (4k+3)^3 = 64k^3 + 144k^2 + 108k + 27 = (64k^3 + 144k^2 + 108k + 24) + 3$

$= 4\,(16k^3 + 36k^2 + 27k + 6) + 3 = 4n + 3$, where $n = 16k^3 + 36k^2 + 27k + 6$

i.e., for any integer m, m^3 cannot be of the form: $4n + 2$

17. Prove that for any integer a, $\gcd(5a+2, 7a+3) = 1$

Proof.

Recall that if $a|b$ and $a|c$, then $a|(bx+cy)$ for all $x, y \in \mathbf{N}$

i.e., a divides any linear combination of b and c)

Therefore, since $d|(5a+2)$ and $d|(7a+3)$, d divides any linear combination of $(5a+2)$ and $d|(7a+3)$

Specifically, d divides $7(5a+2) - 5(7a+3) = -1$

i.e., $d|(-1) \Rightarrow d = \pm 1$

Since d must be positive, $d = 1$ $\blacksquare$