Number Theory - Test #2 - 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)

1. State **Theorem 2.9**

   The linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = \gcd(a, b)$. If (x_0, y_0) is any particular solution of this equation, then all other solutions are of the form:

   $$(x, y) = (x_0, y_0) + \left(\frac{b}{d}t, -\frac{a}{d}t\right) \quad t \in \mathbb{Z}$$

   $$\text{i.e., } x = x_0 + \frac{b}{d}t \text{ and } y = y_0 - \frac{a}{d}t \quad t \in \mathbb{Z}$$

2. Define the **prime** and **composite**

   An integer $p > 1$ is a **prime number** (or **prime**) exactly when its only positive divisors are 1 and p. Otherwise, it is **composite.**

3. State **Theorem 3.1**

   If p is prime and $p|ab$, then either $p|a$ or $p|b$.

4. State **Corollary 1** (p. 40)

   If p is prime and $p|a_1a_2\ldots a_n$, then $p|a_k$ for some k, where $1 \leq k \leq n$.

5. State **Theorem 3.2 (**the **Fundamental Theorem of Arithmetic)**

   Every positive integer $n > 1$ is either prime or the product of primes; this representation is unique, apart from the order in which the primes appear.

6. State the Corollary on page 42

   Any positive integer $n > 1$ can be written uniquely in a canonical form

   $$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

   for primes $p_1 < p_2 < \ldots < p_r$, and positive integers $k_1, k_2, \ldots, k_r$.

7. Prove: $\sqrt{2}$ is irrational.

   Proof. Suppose, for the sake of deriving a contradiction, that $\sqrt{2}$ is rational. Then there exist natural numbers m and n such that $\sqrt{2} = \frac{m}{n}$.

   Without loss of generality, we can assume that m and n are relatively prime. (If m and n are **not** relatively prime, then we can cancel common factors in the numerator and denominator of $\frac{m}{n}$, yielding a fraction whose numerator and denominator are relatively prime.)

   $\sqrt{2} = \frac{m}{n}$

   $\Rightarrow 2 = \frac{m^2}{n^2}$

   $\Rightarrow 2n^2 = m^2$

   $\Rightarrow 2 | m^2$

   $\Rightarrow 2 | m$

   $\Rightarrow \exists\ k \in \mathbb{N}$ such that $m = 2k$.

   Thus, $2n^2 = m^2 = (2k)^2 = 4k^2$

   i.e., $2n^2 = 4k^2$

   $\Rightarrow n^2 = 2k^2$

   $\Rightarrow 2 | n^2$

   $\Rightarrow 2 | n$

   i.e., $2 | m$ and $2 | n$.

   This contradicts the assumption that m and n are relatively prime.

   Since the assumption that $\sqrt{2}$ is rational leads us to this contradiction, $\sqrt{2}$ must be irrational. ■

8. Prove: There are infinitely many primes

   Proof. (By contradiction) Suppose, for the sake of deriving a contradiction, that there are only finitely many primes, $p_1 < p_2 < \ldots < p_n$. Consider the number $P = p_1 p_2 \ldots p_n + 1$.

   Observe that $P > p_i$ for any i where $1 \leq i \leq n$.

   Since P is larger than the largest prime, P must be composite.

   Therefore, P has a prime divisor, let's call it p_k.

   (i.e., $p_k | P$)

   Also, $p_k | \left(p_1 p_2 \ldots p_n\right)$, since p_k appears explicitly as a factor.

   Thus, $p_k | \left(P - p_1 p_2 \ldots p_n\right) \Rightarrow p_k | \left(1\right) \Rightarrow p_k = \pm 1$.

   This contradicts the fact that p_k is prime.

   Since the assumption that there are only finitely many primes leads to a contradiction, the assumption must be false.

   Hence, there must be infinitely many primes. ■

9. Prove: For any $n \in \mathbb{N}$, there exists a sequence of n consecutive composite numbers

   Proof. Let $n \in \mathbb{N}$ be given.

   Consider the sequence of n consecutive natural numbers:

   $$(n+1)! + 2, \quad (n+1)! + 3, \quad (n+1)! + 4, \ldots, (n+1)! + (n+1)$$

   Every term in the sequence is a composite number. Here's why:

   $(n+1)! = (n+1) \cdot n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 4 \cdot 3 \cdot 2 \cdot 1$

   Thus, $k | \left(n+1\right)!$, for every k such that $1 \leq k \leq n+1$

   Note also that: $k | \left(n+1\right)!$ and $k | k$

   Thus k divides every linear combination of $(n+1)!$ and k, including $(n+1)! + k$, for every k such that $1 \leq k \leq n+1$.

   Thus, $(n+1)! + k$ is composite for every k such that $1 \leq k \leq n+1$. ■

10. Prove: $\{3, 5, 7\}$ is the only sequence of three consecutive odd prime numbers.

Proof. Let $n, n+2, n+4$ be a sequence of three consecutive odd numbers.

By the Division Algorithm, n must have exactly one of the following forms:

$n = 3k$, for some $k \in \mathbb{N}$

$n = 3k+1$, for some $k \in \mathbb{N}$

$n = 3k+2$, for some $k \in \mathbb{N}$

Case 1: $n = 3k$, for some $k \in \mathbb{N}$

In this case $n = 3k$ is only prime when $k = 1$.

Thus, $3, 5, 7$ is the only sequence of odd prime numbers in which the first number has the form $n = 3k$

Case 2: $n = 3k+1$, for some $k \in \mathbb{N}$

In this case $n + 2 = (3k+1) + 2 = (3k+3) = 3\,(k+1)$ is not prime for any $k \in \mathbb{N}$.

Thus, there are no sequences of odd prime numbers in which the first number has the form $n = 3k+1$

Case 3: $n = 3k+2$, for some $k \in \mathbb{N}$

In this case $n + 4 = (3k+2) + 4 = (3k+6) = 3\,(k+2)$ is not prime for any $k \in \mathbb{N}$.

Thus, there are no sequences of odd prime numbers in which the first number has the form $n = 3k+2$

This exhausts all possibilities.

Hence, $\{3, 5, 7\}$ is the only sequence of three consecutive odd prime numbers. ■

11. A local high school sells season tickets to their home football games. The season tickets are sold as single season tickets ($60 apiece) or in pars of season tickets ($105 per pair, so that both Mom and Dad can watch “Junior”). If total sales from season tickets amounts to $41,640, how many single season tickets and season ticket pairs have been sold? (Assume that at least one of each are sold. There are about 100 possibilities. List the “general formula.” In addition, list the first three (x, y) pairs, as well as the last three (x, y) pairs.)

Let x be the number of single season tickets that are sold

Let y be the number of season ticket pairs that are sold

Then $\underbrace{60}_{a} x + \underbrace{105}_{b} y = \underbrace{41640}_{c}$

First, we should check to make sure that this pair of Diophantine equations has a solution.

$d = \gcd(60, 105) = 15$

Also: $41640 = 2776\,(15) + 0$

Since $d|c$, the system has a solution.

We now use the Euclidean Algorithm to find a particular solution (x_0, y_0) to the related equation

$$\underbrace{60}_{a} x + \underbrace{105}_{b} y = 15$$

$105 = (1)\,(60) + 45$ (Eq. 1)

$60 = (1)\,(45) + 15$ (Eq. 2)

$45 = (3)\,(15) + 0$

From Eq. 2, $15 = 60 - 45$ (Eq. 3)

From Eq. 1, $45 = 105 - 60$

Substituting Eq. 1 into Eq. 3, We have: $15 = 60 - (105 - 60) \Rightarrow 15 = (2)\,(60) - 105$

We must rewrite this in the form of our original “equation,” $60x + 105y = 41640$

Thus, we have: $60\,(2) + 105\,(-1) = 15$

To get our particular solution, we must multiply both sides by $\frac{c}{d} = \frac{41640}{15} = 2776$

$\Rightarrow 2776\left(60\left(2\right) + 105\left(-1\right)\right) = 2776\left(15\right)$

$\Rightarrow 60\left(2 \cdot 2776\right) + 105\left(-1 \cdot 2776\right) = 41640$

$\Rightarrow 60\underbrace{(5552)}_{x_p} + 105\underbrace{(-2776)}_{y_p} = 41640$

Thus, $(x_p, y_p) = (5552, -2776)$

All other solutions are of the form: $(x_p, y_p) + \left(\frac{b}{d}t, -\frac{a}{d}t\right)$, for $t \in \mathbb{Z}$

i.e., $(5552, -2776) + \left(\frac{105}{15}t, -\frac{60}{15}t\right)$, for $t \in \mathbb{Z}$

$(x, y) = (5552, -2776) + (7t, -4t)$, for $t \in \mathbb{Z}$

$x = 5552 + 7t$; $y = -2776 - 4t$, for $t \in \mathbb{Z}$

Only those values of t which yield values of $x \geq 1$ and $y \geq 1$ are acceptable.

This yields: $1 \leq 5552 + 7t$ and $1 \leq -2776 - 4t$

$\Rightarrow 1 - 5552 \leq 7t$ and $2777 \leq -4t$

$\Rightarrow -5551 \leq 7t$ and $2777 \leq -4t$

$\Rightarrow -\frac{5551}{7} \leq t$ and $-\frac{2777}{4} \geq t$

$\Rightarrow -\frac{5551}{7} \leq t \leq -\frac{2777}{4}$

$\Rightarrow -793 \leq t \leq -694.25$

Since t is an integer, this inequality becomes $-793 \leq t \leq -695$

i.e., $x = 5552 + 7t$; $y = -2776 - 4t$, for $t \in \mathbb{Z}$ and $-793 \leq t \leq -695$

For $t = -793, -792, -791, \ldots, -697, -696, -695$, we have:

$t=-793$	$x=5552+7\left(-793\right)=1$	$y=-2776-4\left(-793\right)=396$
$t=-792$	$x=5552+7\left(-792\right)=8$	$y=-2776-4\left(-792\right)=392$
$t=-791$	$x=5552+7\left(-791\right)=15$	$y=-2776-4\left(-791\right)=388$
$\vdots$	$\vdots$	$\vdots$
$t=-697$	$x=5552+7\left(-697\right)=673$	$y=-2776-4\left(-697\right)=12$
$t=-696$	$x=5552+7\left(-696\right)=680$	$y=-2776-4\left(-696\right)=8$
$t=-695$	$x=5552+7\left(-695\right)=687$	$y=-2776-4\left(-695\right)=4$

12. Prove: If $p \neq 5$ is an odd prime number, then either p^2-1 or p^2+1 is divisible by 10

Proof. Let the hypothesis be given. (i.e., Suppose that $p \neq 5$ is an odd prime number.)

Our strategy will be to show that $2|\left(p^2-1\right)$ and $2|\left(p^2+1\right)$, and that either:

$5|\left(p^2-1\right)$, in which case $\left(2\cdot 5\right)|\left(p^2-1\right)$, by Euclid's Lemma,

or

$5|\left(p^2+1\right)$, in which case $\left(2\cdot 5\right)|\left(p^2+1\right)$, by Euclid's Lemma.

$\boxed{2|\left(p^2-1\right) \text{ and } 2|\left(p^2+1\right)}$

To show that $2|\left(p^2-1\right)$ and $2|\left(p^2+1\right)$, observe that since p is an odd prime, $p=2k+1$, for some natural number k.

$\Rightarrow p^2=\left(2k+1\right)^2=4k^2+4k+1=2\left(2k^2+2k\right)+1$

i.e., $p^2=2\left(2k^2+2k\right)+1$

Hence, $p^2-1=\left[2\left(2k^2+2k\right)+1\right]-1=2\left(2k^2+2k\right)$

i.e., $2|\left(p^2-1\right)$

Similarly, $p^2+1=\left[2\left(2k^2+2k\right)+1\right]+1=2\left(2k^2+2k\right)+2=2\left(2k^2+2k+1\right)$

i.e., $2|\left(p^2+1\right)$

$$\boxed{5|\left(p^2-1\right) \text{ or } 5|\left(p^2+1\right)}$$

Note that since $p \neq 5$ and p is a prime number, $5 \nmid p$. Otherwise, p would not be prime.

Thus, by the Division Algorithm, p must have one of the following four forms:

$p = 5n+1$, in which case, $p^2 = (5n+1)^2 = 25n^2+10n+1 = 5\left(5n^2+2n\right)+1 = 5k+1$

$p = 5n+2$, in which case, $p^2 = (5n+2)^2 = 25n^2+20n+4 = 5\left(5n^2+4n\right)+4 = 5k+4$

$$= (5k+4)+1-1 = (5k+5)-1 = 5(k+1)-1$$

$p = 5n+3$, in which case, $p^2 = (5n+3)^2 = 25n^2+30n+9 = 5\left(5n^2+6n+1\right)+4 = 5k+4$

$$= (5k+4)+1-1 = (5k+5)-1 = 5(k+1)-1$$

$p = 5n+4$, in which case, $p^2 = (5n+4)^2 = 25n^2+40n+16 = 5\left(5n^2+8n+3\right)+1 = 5k+1$

i.e., p^2 must either have the form: $p^2 = 5k+1$ or $p^2 = 5(k+1)-1$

In the case in which $p^2 = 5k+1$, $p^2-1 = 5k$. (i.e., $5|\left(p^2-1\right)$)

In the case in which $p^2 = 5(k+1)-1$, $p^2+1 = 5(k+1)$. (i.e., $5|\left(p^2+1\right)$)

This exhausts all cases. In all cases, either $5|\left(p^2-1\right)$ or $5|\left(p^2+1\right)$ ■

Remark: The proof above is **my** proof. A number of my students submitted a different proof - similar, but with minor variations. I like their proof better. What do you think?

Alternate Proof: Submitted by Chelsey Adamson, Jackson Baker, Madison Butler, Bayleigh Edberg, Emmaline Hughes, Clayton Lang, Meagan Long, Elizabeth Rowe, Lauren Veazey,

Proof. Let the hypothesis be given. (i.e., Suppose that $p \neq 5$ is an odd prime number.)

Applying the Division Algorithm to p, using $d = 10$ as the divisor, there are 4 possibilities:

$p = 10q+1$; $p = 10q+3$; $p = 10q+7$; $p = 10q+9$.

$\boxed{p = 10q + 1}$

In this case, $p^2 = (10q + 1)^2 = 100q^2 + 20q + 1$

$p^2 - 1 = (100q^2 + 20q + 1) - 1 = 100q^2 + 20q = 10\left(10q^2 + 2q\right)$

i.e., $p^2 - 1 = 10\left(10q^2 + 2q\right)$, and consequently, $10|\left(p^2 - 1\right)$

$\boxed{p = 10q + 3}$

In this case, $p^2 = (10q + 3)^2 = 100q^2 + 60q + 9$

$p^2 + 1 = (100q^2 + 60q + 9) + 1 = 100q^2 + 60q + 10 = 10\left(10q^2 + 6q + 1\right)$

i.e., $p^2 + 1 = 10\left(10q^2 + 6q + 1\right)$, and consequently, $10|\left(p^2 + 1\right)$

$\boxed{p = 10q + 7}$

In this case, $p^2 = (10q + 7)^2 = 100q^2 + 140q + 49$

$p^2 + 1 = (100q^2 + 140q + 49) + 1 = 100q^2 + 140q + 50 = 10\left(10q^2 + 14q + 5\right)$

i.e., $p^2 + 1 = 10\left(10q^2 + 14q + 5\right)$, and consequently, $10|\left(p^2 + 1\right)$

$\boxed{p = 10q + 9}$

In this case, $p^2 = (10q + 9)^2 = 100q^2 + 180q + 81$

$p^2 - 1 = (100q^2 + 180q + 81) - 1 = 100q^2 + 180q + 80 = 10\left(10q^2 + 18q + 8\right)$

i.e., $p^2 - 1 = 10\left(0q^2 + 18q + 8\right)$, and consequently, $10|\left(p^2 - 1\right)$

This exhausts all cases, and in each case either $10|\left(p^2 - 1\right)$ or $10|\left(p^2 + 1\right)$ ■

13. Prove: A positive integer $a > 1$ is a perfect square if and only if, in the canonical form of a, all of the exponents of the primes are even integers.

Proof. Let $a > 1$ be a positive integer.

(a is a perfect square.) $\Rightarrow$ (In the canonical form of a, all of the exponents of the primes are even integers.)

Suppose that $a > 1$ is a perfect square.

Then $a = b^2$, for some natural number $b > 1$

By the Fundamental Theorem of Arithmetic, $b = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, for primes $p_1 < p_1 < \ldots < p_r$.

$a = b^2 = \left(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\right)^2 = p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r}$

i.e., $a = p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r}$.

Note that, in the canonical form of a, all of the exponents of the primes are even integers.

(In the canonical form of a, all of the exponents of the primes are even integers.) $\Rightarrow$ (a is a perfect square.)

Suppose that $a > 1$ and that, in the canonical form of a, all of the exponents of the primes are even integers.

Then $a = p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r}$, for primes $p_1 < p_1 < \ldots < p_r$.

$\Rightarrow a = p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r} = \left(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\right)^2$

i.e., a is a perfect square. ■