MTH 4436 Test #2 - Solutions

Fall 2021

Pat Rossi Name ______________________

Instructions. Show CLEARLY how you arrive at your answers

1. Define *prime*

   An integer $p \geq 2$ is *prime* exactly when its only positive divisors are 1 and p.

2. Define *Diophantine Equation*

   A *Diophantine Equation* is an equation that admits (allows) only integer solutions.

3. State the Fundamental Theorem of Arithmetic

   Every positive integer $n > 1$ is prime or can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.

Problems 4-6: **State Three Theorems/Lemmas/Corollaries Regarding Primes.**

Here are some possibilities:

4. There are infinitely many primes.

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

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

- If $p, q_1, q_2, \ldots, q_n$ are all primes and $p|q_1q_2\ldots q_n$, then $p = q_i$ for some i, where $1 \leq i \leq n$.

- If n is composite, then n has a prime factor $p \leq \sqrt{n}$

6. Every positive integer $n > 1$ is either a prime or the product of primes. This product is unique, disregarding the order of the prime factors.

7. 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.

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

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

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. ■

From Problems 8-9, select one.

8. Prove: The only prime of the form $n^3 - 1$ is 7.

(a) **Proof.** Observe: $n^3 - 1 = (n-1)(n^2 + n + 1)$.

Note that $n = 1$ yields $n^3 - 1 = 0$ (not prime).

Also, $n = 2$ yields $n^3 - 1 = 7$ (prime).

For $n > 2$, we have $n^3 - 1 = \underbrace{(n-1)}_{\geq 2}\underbrace{(n^2 + n + 1)}_{\geq 2}$, and is therefore composite. ■

9. If $p \geq 5$ is prime, prove that $p^2 + 2$ is composite. (Hint: Consider the forms that p can take when divided by 6.)If $p \geq 5$ is prime, prove that $p^2 + 2$ is composite. (Hint: Consider the forms that p can take when divided by 6.)

   Proof. Let the hypothesis be given. (i.e. suppose that $p \geq 5$ is prime.)

   Then p must be odd, and not a multiple of 3.

   By the Division Algorithm, p must assume one of the following six forms:

$$6k,\ 6k + 1,\ 6k + 2,\ 6k + 3,\ 6k + 4,\ 6k + 5$$

   Since p must be odd and not a multiple of 3, p must either be of the form $6k + 1$ or $6k + 5$

   If $p = 6k + 1$, then $p^2 + 2 = (6k + 1)^2 + 2 = 36k^2 + 12k + 3 = 3\left(12k^2 + 4k + 1\right)$, which is composite.

   If $p = 6k + 5$, then $p^2 + 2 = (6k + 5)^2 + 2 = 36k^2 + 60k + 27 = 3\left(12k^2 + 20k + 9\right)$, which is composite. ■

From Problems 10-11, select one.

10. Show that any composite three-digit number must have a prime factor less than or equal to 31.

    Proof. Let n be a composite, three digit number. Since $31^2 = 961$ and $32^2 = 1024$, it must be the case that $\sqrt{n} < \sqrt{1000} < 32$.

    Since every composite number n must have a prime factor p less than or equal to its own square root, this means that

$$p \leq \sqrt{n} < 32$$

    i.e., n must have a prime factor p less than or equal to 31. ■

11. Show that the sum of twin primes p and $p+2$ is divisible by 12, provided that $p > 3$.

Proof. Let $c = p + (p+2)$, where p and $p+2$ are prime. Since $\gcd(3,4) = 1$, it will follow that if $3|c$ and $4|c$, then $(3 \cdot 4)\,|c$.

i.e., $12|c$.

Hence our proof boils down to showing that $3|c$ and $4|c$. (i.e., $3|\,[p+(p+2)]$ and $4|\,[p+(p+2)]$)

$$\boxed{3|\,[p+(p+2)]}$$

Note that p must have one of the following three forms:

$p = 3k$; $p = 3k+1$; $p = 3k+2$,   for some natural number k.

Case 1: $p = 3k$

This can't happen, because this would make p composite, contrary to hypothesis.

Case 2: $p = 3k+1$

This can't happen, because this would make $p+2 = (3k+1)+3 = 3k+3 = 3\,(k+1)$.

i.e., $p+2$ would be composite, contrary to hypothesis.

This leaves ...

Case 3: $p = 3k+2$ (This MUST be the case!)

Hence, $p+2 = (3k+2)+2 = 3k+4$.

Observe: $p+(p+2) = (3k+2)+(3k+4) = 3k+6 = 3\,(k+2)$

Thus, $3|\,[p+(p+2)]$

$$\boxed{4|\,[p+(p+2)]}$$

Since $p > 3$, p must be odd. Hence, $p = 2k+1$, for some natural number k.

Thus, $p+(p+2) = (2k+1)+[(2k+1)+2] = 4k+4 = 4\,(k+1)$

Thus, $4|\,[p+(p+2)]$, and our claim is proved. ■

12. Construct the Sieve of Eratosthenes for $n \leq 200$, and list all of the primes less than 200.

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			
101		103				107		109	
		113							
						127			
131						137		139	
								149	
151						157			
		163				167			
		173						179	
181									
191		193				197		199	

Thus, we find the primes less than 200 to be: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199$.

13. Test the number 4079 to determine whether it is prime or composite.

First, Observe that: $\sqrt{4079} = 63.87$, so if 4079 is composite, it must have a prime factor less than or equal to 63.

Next, Observe:

$$
\begin{aligned}
4079 &= (2039)\,(2) + 1 \\
4079 &= (1359)\,(3) + 2 \\
4079 &= (815)\,(5) + 4 \\
4079 &= (582)\,(7) + 5 \\
4079 &= (370)\,(11) + 9 \\
4079 &= (313)\,(13) + 10 \\
4079 &= (239)\,(17) + 16 \\
4079 &= (214)\,(19) + 13 \\
4079 &= (177)\,(23) + 8 \\
4079 &= (140)\,(29) + 19 \\
4079 &= (131)\,(31) + 18 \\
4079 &= (110)\,(37) + 9 \\
4079 &= (99)\,(41) + 20 \\
4079 &= (94)\,(43) + 37 \\
4079 &= (86)\,(47) + 37 \\
4079 &= (76)\,(53) + 51 \\
4079 &= (69)\,(59) + 8 \\
4079 &= (66)\,(61) + 53
\end{aligned}
$$

Since 4079 does not have a prime divisor less than or equal to its square root, it is prime.

14. A Farmer goes to town to buy sheep and goats. Each sheep costs \$54 and each goat costs \$21. If the farmer spends \$3036, determine all of the possible combinations of sheep and goats that he could have purchased.

Let s be the number of sheep

Let g be the number of goats

Our problem can be represented as $54s + 21g = 3036$

Since $\gcd(54, 21) = 3$, and $3|3036$, the equation can be solved.

Next, we repeatedly apply the Division Algorithm to obtain $\gcd(54, 21) = 3$.

$54 = q_1(21) + r_1$
$54 = (2)(21) + 12$ eq.1
Repeat with 21 and 12.
$21 = q_2(12) + r_2$
$21 = (1)(12) + 9$ eq.2
Repeat with 12 and 9.
$12 = q_3(9) + r_3$
$12 = (1)(9) + 3$ eq.3
Repeat with 9 and 3.
$9 = q_4(3) + r_4$
$9 = (3)(3) + 0$
$\gcd(54, 21)$ is the last non-zero divisor.
$\gcd(54, 21) = 3$

Since $\gcd(54, 21)\,|3036$, the equation $54s + 21g = 3036$ has infinitely many solutions.

First though, we solve the related equation, $54s + 21g = \gcd(54, 21)$

(i.e., $54s + 21g = 3$).

By Eq. 3, we have $3 = 12 - (1)(9)$ Eq. 4
By Eq. 2, we have $9 = 21 - (1)(12)$
Thus, Eq. 4 becomes $3 = 12 - (1)(21 - (1)(12))$
$\Rightarrow 3 = (2)(12) - (1)(21)$ Eq. 5
By Eq. 2, we have $12 = (54) - (2)(21)$
Thus, Eq. 5 becomes $3 = (2)[(54) - (2)(21)] - (1)(21)$
$\Rightarrow 3 = (2)(54) - (5)(21)$
i.e., $54(2) + 21(-5) = 3$ Eq. 6
Now, to find a particular solution of $54s + 21g = 3036$,
we multiply both sides of Eq.6 by 1012 $(3036 = 3 \cdot 1012)$
$\Rightarrow 1012[54(2) + 21(-5)] = 1012(3)$
$\Rightarrow 54(2024) + 21(-5060) = 3036$

Thus, $(s_0, g_0) = (2024, -5060)$ is a particular solution of the related equation $54s + 21g = 3036$.

Next, we find the homogeneous solution (s_h, g_h).

This is given by:

$(s_h, g_h) = \left(\frac{b}{d}t, -\frac{a}{d}t\right), \quad$ for $t \in \mathbf{Z}$; where $d = \gcd(a, b)$.

Thus,

$(s_h, g_h) = \left(\frac{21}{3}t, -\frac{54}{3}t\right) = (7t, -18t), \quad$ for $t \in \mathbf{Z}$

i.e., $(s_h, g_h) = (7t, -18t), \quad$ for $t \in \mathbf{Z}$

To find the general solution, we add the particular solution and the homogeneous solution

Hence, $(s, g) = (2024, -5060) + (7t, -18t), \quad$ for $t \in \mathbf{Z}$

$$s = 2024 + 7t; \quad g = -5060 - 18t \quad \text{for } t \in \mathbf{Z}$$

The nature of the problem requires that both s and g be non-negative.

$\Rightarrow s = 2024 + 7t \geq 0$ and $g = -5060 - 18t \geq 0$

$\Rightarrow 7t \geq -2024$ and $-5060 \geq 18t$

$\Rightarrow t \geq -289.14$ and $-281.11 \geq t$

i.e., $-289 \leq t \leq -282$

Thus, we have eight viable solutions:

$\boxed{t = -282}$

$s_1 = 2024 + 7(-282) = 50; \quad g_1 = -5060 - 18(-282) = 16$

$(s_1, g_1) = (50, 16)$

$\boxed{t = -283}$

$s_2 = 2024 + 7(-283) = 43; \quad g_2 = -5060 - 18(-283) = 34$

$(s_2, g_2) = (43, 34)$

$\boxed{t = -284}$

$s_3 = 604 + 7(-284) = 36; \quad g_3 = -1510 - 18(-284) = 52$

$(s_3, g_3) = (36, 52)$

$\boxed{t = -285}$

$s_4 = 604 + 7\,(-285) = 29; \quad g_4 = -1510 - 18\,(-285) = 70$

$(s_4, g_4) = (29, 70)$

$\boxed{t = -286}$

$s_5 = 604 + 7\,(-286) = 22; \quad g_5 = -1510 - 18\,(-286) = 88$

$(s_5, g_5) = (22, 88)$

$\boxed{t = -287}$

$s_6 = 604 + 7\,(-287) = 15; \quad g_6 = -1510 - 18\,(-287) = 106$

$(s_6, g_6) = (15, 106)$

$\boxed{t = -288}$

$s_7 = 604 + 7\,(-288) = 8; \quad g_7 = -1510 - 18\,(-288) = 124$

$(s_7, g_7) = (8, 124)$

$\boxed{t = -289}$

$s_8 = 604 + 7\,(-289) = 1; \quad g_8 = -1510 - 18\,(-289) = 142$

$(s_8, g_8) = (1, 142)$