

MTH 4436 Homework set 3.1, Page 43

SPRING 2015

Pat Rossi

Name _____

1. It has been mentioned that there are infinitely many primes of the form $n^2 - 2$. Exhibit five such primes.

$n =$	$n^2 - 2 =$	Prime?
2	2	Yes!
3	7	Yes!
4	14	No!
5	23	Yes!
6	34	No!
7	47	Yes!
8	62	No!
9	71	Yes!

2. Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where p is either prime or 1, and $a \geq 0$.

Consider $n = 25$, and the difference between $n = 25$ and all of the primes (as well as $p = 1$) less than 25.

$p =$	$25 - p =$	$= a^2$???
1	24	No!
2	23	No!
3	22	No!
5	20	No!
7	18	No!
11	14	No!
13	12	No!
17	8	No!
19	6	No!
23	2	No!

3. Prove each of the assertions below:

- (a) Any prime of the form $3n + 1$ is also of the form $6m + 1$

Proof. Observe that $p = 2$ is NOT of the form $3n + 1$.

Therefore, any prime of the form $3n + 1$ must be odd, and of the form $2k + 1$.

$$\text{i.e., } p = 3n + 1 = 2k + 1$$

$$\Rightarrow 3n = 2k$$

$$\Rightarrow 2|3n$$

$$\Rightarrow (\text{by Euclid's Lemma}) 2|n \text{ (i.e., } n = 2m \text{ for some } m \in \mathbf{N})$$

$$\Rightarrow p = 3n + 1 = 3(2m) + 1 = 6m + 1$$

$$\text{i.e., } p = 6m + 1 \blacksquare$$

ALTERNATE PROOF:

Proof. Let p be a prime of the form $3n + 1$. Note that either n is either even or odd.

Case 1 (n is even)

Then $n = 2k$, for some integer, k .

$$\Rightarrow p = 3n + 1 = 3(2k) + 1 = 6k + 1 = 6m + 1$$

i.e., $p = 6m + 1$, where $m = k$.

Case 2 (n is odd)

This is impossible, for if n is odd, then $n = 2k + 1$, for some integer, k .

$$\Rightarrow p = 3n + 1 = 3(2k + 1) + 1 = 6k + 4 = 2(3k + 2)$$

$\Rightarrow p$ is even $\Rightarrow p = 2$.

Since $p = 2$ is NOT of the form $3n + 1$, this contradicts the assumption that p is of the form $3n + 1$.

Hence, if p is a prime of the form $3n + 1$, n must be even, and $p = 6m + 1$, from Case 1. ■

(b) Each integer of the form $3n + 2$ has a prime factor of this form.

Proof. (By contradiction) Observe that the proposition holds for $n = 1, 2$ as $3(1) + 2 = 5$, which is prime, and $3(2) + 2 = 8$ which has a prime factor of the form $3(0) + 2$.

Suppose, for the sake of deriving a contradiction, that the proposition is false. Let $N = 3k + 2$ be the smallest natural number for which the proposition fails. Since we're assuming that $N = 3k + 2$ has no prime factor of the form $3n + 2$, N cannot be prime.

By the Fundamental Theorem of Arithmetic, N must have a prime divisor, p , where $p \neq N$.

By the Division Algorithm, there are three possibilities:

1. $p = 3m$

In this case, note that m must equal 1, or else p cannot be prime. At any rate, $p \nmid N$ (i.e., $3 \nmid (3k + 2)$). Hence, $p \neq 3m$.

2. $p = 3m + 2$

This cannot happen, since we've assumed that $N = 3k + 2$ has no prime factor of the form $3n + 2$.

Hence, only the third case remains:

3. $p = 3m + 1$

Since p is a prime factor of $N = 3k + 2$, \exists a natural number h such that that $N = 3k + 2 = p \cdot h$.

What form does h have?

1. $h \neq 3j$, because we have already observed that $3 \nmid (3k + 2)$.

2. $h \neq 3j + 1$, otherwise, $N = 3k + 2 = p \cdot h = (3m + 1)(3j + 1) = 9mj + 3m + 3j + 1 = 3(3mj + m + j) + 1$, which is NOT of the form $3k + 2$.

Hence, only the third case remains:

3. $h = 3j + 2$

Since $h < N$, this implies that $h = 3j + 2$ has a prime factor of the form $3n + 2$. Therefore, $N = 3k + 2$ has a prime factor of the form $3n + 2$.

This contradicts our choice of k as the smallest natural number such that our proposition fails.

Hence, each integer of the form $3n + 2$ has a prime factor of this form. ■

Alternate Proof:

(By contradiction) Suppose, for the sake of deriving a contradiction, that the proposition is false. Let $N = 3n_1 + 2$ be a natural number for which the proposition fails. Since we're assuming that $N = 3n_1 + 2$ has no prime factor of the form $3n + 2$, N cannot be prime.

By the Fundamental Theorem of Arithmetic, $N = 3n_1 + 2$ must have two factors $p_1, q_1 > 1$.

Observe that they must be of the form:

$$p_1 = 3n_2 + 2$$

$$q_1 = 3k_2 + 1$$

By our "contradiction hypothesis," $p_1 = 3n_2 + 2$ is not prime. Hence, by the Fundamental Theorem of Arithmetic, $p_1 = 3n_2 + 2$ must have two factors $p_2, q_2 > 1$.

Observe that they must be of the form:

$$p_2 = 3n_3 + 2$$

$$q_2 = 3k_3 + 1$$

By our "contradiction hypothesis," $p_2 = 3n_3 + 2$ is not prime. Hence, by the Fundamental Theorem of Arithmetic, $p_2 = 3n_3 + 2$ must have two factors $p_3, q_3 > 1$.

Observe that they must be of the form:

$$p_3 = 3n_4 + 2$$

$$q_3 = 3k_4 + 1$$

Proceeding inductively, we obtain an infinite, strictly decreasing sequence of *natural numbers*:

$$3n_1 + 2, 3n_2 + 2, 3n_3 + 2, \dots$$

This contradicts the Well Ordering Principle which states that every non-empty set of non-negative integers has a least element.

Since the assumption that there exists a natural number $3n + 2$ that doesn't have a prime factor of the same form leads to a contradiction, It must be false.

Hence, each integer of the form $3n + 2$ has a prime factor of this form. ■

- (c) The only prime of the form $n^3 - 1$ is 7.

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. ■

(d) The only prime p for which $3p + 1$ is a perfect square is $p = 5$.

Proof. Suppose that $3p + 1$ is a perfect square. Then $3p + 1 = k^2$ for some $k \in \mathbf{N}$.

$$\Rightarrow 3p = k^2 - 1$$

$$\Rightarrow 3p = (k + 1)(k - 1)$$

Since the Fundamental Theorem of Arithmetic tells us that the factorization of a number into to prime factors is unique, it must be the case that

$$k - 1 = 3 \text{ and } (k + 1) = p$$

i.e., $k - 1 = 3$ and $(k + 1) = 5$.

Thus, $k = 4$, and $3p + 1 = k^2 = 16$.

Therefore, $p = 5$. ■

(e) The only prime of the form $n^2 - 4$ is 5.

Proof. Suppose that $n^2 - 4$ is prime. Note that $n \geq 3$, otherwise $n^2 - 4$ is not a natural number. Consequently, $n^2 - 4 \geq 3^2 - 4 = 5$. Thus, in order for $n^2 - 4$ to be prime, it must be odd. This, in turn, implies that n^2 must be odd, and therefore, n must be odd.

$$\Rightarrow n = 2k + 1 \text{ for some } k \in \mathbf{N}.$$

$$\Rightarrow n^2 - 4 = (2k + 1)^2 - 4 = 4k^2 + 4k - 3 = (2k + 3)(2k - 1).$$

Since $n^2 - 4$ is prime, one of these factors must be 1, obviously, the smaller factor, $(2k - 1)$.

$$2k - 1 = 1 \Rightarrow k = 1$$

$$\Rightarrow n^2 - 4 = (2(1) + 3)(2(1) - 1) = 5. \blacksquare$$

4. If $p \geq 5$ is a prime number, Show that $p^2 + 2$ is composite.

Proof. Since p is prime and $p \geq 5$, p must be odd.

i.e., $p = 6k + 1$ or $p = 6k + 5$

Thus, either $p^2 + 2 = (6k + 1)^2 + 2 = 36k^2 + 12k + 3 = 3(12k^2 + 4k + 1)$,

or $p^2 + 2 = (6k + 5)^2 + 2 = 36k^2 + 60k + 27 = 3(12k^2 + 20k + 9)$.

Either way, $p^2 + 2$ is composite. ■

5. ~

(a) Given that p is prime and $p|a^n$, prove that $p^n|a^n$.

Proof. By Corollary 1 (page 41), If p is a prime and $p|(a_1 a_2 \dots a_n)$, then $p|a_k$ for some k for $1 \leq k \leq n$.

Thus, given that $p|a^n$, if we let $a_k = a$ for $1 \leq k \leq n$, we have $p|(a_1 a_2 \dots a_n)$ and the corollary applies. Therefore, $p|a_k$ (i.e., $p|a$).

$$\Rightarrow a = pm \text{ for some } m \in \mathbf{Z}.$$

$$\Rightarrow a^n = (pm)^n = p^n m^n.$$

i.e., $a^n = p^n m^n \Rightarrow p^n|a^n$. ■

- (b) If $\gcd(a, b) = p$, a prime, what are the possible values of $\gcd(a^2, b^2)$, $\gcd(a^2, b)$, $\gcd(a^3, b^2)$?

$$\boxed{\gcd(a^2, b^2)}$$

If $\gcd(a, b) = p$, then either a or b has *exactly* one factor of p . (Otherwise, $p^2|a$ and $p^2|b$, and $\gcd(a, b) \geq p^2$.)

Without loss of generality, let's say that a has one factor of p .

By the Fundamental theorem of arithmetic, a and b can be factored into primes: $a = p \cdot p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ and $b = p^i \cdot q_1^{s_1} q_2^{s_2} \dots q_j^{s_j}$, for $i \geq 1$, where $p_m \neq q_n$ for $1 \leq m \leq k$ and $1 \leq n \leq j$.

$$\Rightarrow a^2 = p^2 \cdot p_1^{2r_1} p_2^{2r_2} \dots p_k^{2r_k} \text{ and } b^2 = p^{2i} \cdot q_1^{2s_1} q_2^{2s_2} \dots q_j^{2s_j}$$

Observe that p is still the only prime factor that a and b have in common, but now, both a and b have exactly a factor of p^2 in common.

i.e., $\gcd(a^2, b^2) = p^2$.

$$\boxed{\gcd(a^2, b)}$$

Again, either a or b has *exactly* one factor of p . If a has exactly one factor of p , then $a = p \cdot p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ and $b = p^i \cdot q_1^{s_1} q_2^{s_2} \dots q_j^{s_j}$, for $i \geq 1$, where $p_m \neq q_n$ for $1 \leq m \leq k$ and $1 \leq n \leq j$.

Thus $a^2 = p^2 \cdot p_1^{2r_1} p_2^{2r_2} \dots p_k^{2r_k}$ and therefore, a^2 has exactly two factors of p , and b has at least one factor of p .

Thus, $\gcd(a^2, b) = p$ if b has exactly one factor of p , and $\gcd(a^2, b) = p^2$ if b has more than one factor of p .

On the other hand, if b has exactly one factor of p , then $a = p^i \cdot p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ and $b = p \cdot q_1^{s_1} q_2^{s_2} \dots q_j^{s_j}$, for $i \geq 1$, where $p_m \neq q_n$ for $1 \leq m \leq k$ and $1 \leq n \leq j$.

Thus, $a^2 = p^{2i} \cdot p_1^{2r_1} p_2^{2r_2} \dots p_k^{2r_k}$, and a^2 and b have one factor of p in common.

In this case, $\gcd(a^2, b) = p$.

All cases considered:

$\gcd(a^2, b) = p^2$ when b has at least two factors of p .

$\gcd(a^2, b) = p$ when b has exactly one factor of p .

$$\boxed{\gcd(a^3, b^2)}$$

Again, either a or b has *exactly* one factor of p . If a has exactly one factor of p , then $a = p \cdot p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ and $b = p^i \cdot q_1^{s_1} q_2^{s_2} \dots q_j^{s_j}$ where $p_m \neq q_n$ for $1 \leq m \leq k$ and $1 \leq n \leq j$.

Thus $a^3 = p^3 \cdot p_1^{3r_1} p_2^{3r_2} \dots p_k^{3r_k}$ and $b^2 = p^{2i} \cdot q_1^{2s_1} q_2^{2s_2} \dots q_j^{2s_j}$, for $i \geq 1$.

Therefore, a^3 has exactly three factors of p , and b^2 has at least two factors of p .

In this case, $\gcd(a^3, b^2) = p^2$ if b has exactly one factor of p .

$\gcd(a^3, b^2) = p^3$ if b has more than one factor of p .

On the other hand, if b has exactly one factor of p , then $a = p^i \cdot p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ and $b = p \cdot q_1^{s_1} q_2^{s_2} \dots q_j^{s_j}$, for $i \geq 1$, where $p_m \neq q_n$ for $1 \leq m \leq k$ and $1 \leq n \leq j$.

Thus, $a^3 = p^{3i} \cdot p_1^{3r_1} p_2^{3r_2} \dots p_k^{3r_k}$, and $b^2 = p^2 \cdot q_1^{2s_1} q_2^{2s_2} \dots q_j^{2s_j}$, and a^3 and b^2 have two factors of p in common.

In this case, $\gcd(a^3, b^2) = p^2$.

All cases considered:

i.e., $\gcd(a^3, b^2) = p^3$ when b has more than one factor of p .

$\gcd(a^3, b^2) = p^2$ when b has exactly one factor of p .

6. Establish each of the following statements:

(a) Every integer of the form $n^4 + 4$, with $n > 1$ is composite.

Proof. Observe: $n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2)$

If $n = 1$, then $\underbrace{(n^2 - 2n + 2)}_{=1} \underbrace{(n^2 + 2n + 2)}_{=5} = 1 \cdot 5$ which is prime.

For $n > 1$, both terms are greater than 1, and hence, $n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2)$ is composite. ■

(b) If $n > 4$ is composite, then n divides $(n - 1)!$

Proof. Suppose that $n > 4$ is composite.

Then n has a prime factor $p \leq \sqrt{n}$.

Case 1: $n = p^2$

In this case, we must show that $(n - 1)!$ contains two distinct factors of p . Since $p = \sqrt{n} < n - 1$, p is one of the factors of $(n - 1)!$

For the other factor of p , we claim that $2p \leq n - 1$, and hence, $2p$ is a factor of $(n - 1)!$

To see this, observe:

$$n > 4$$

$$\Rightarrow p = \sqrt{n} > 2$$

$$\text{i.e., } p > 2$$

$$\Rightarrow p \cdot p > 2 \cdot p$$

$$\text{i.e., } p^2 > 2p$$

$$\text{But } n = p^2$$

$$\text{Hence, } n > 2p \Rightarrow n - 1 \geq 2p.$$

Case 2: $n = pb$ with $p \neq b$

Again $p < \sqrt{n} < n - 1$, so p is a factor of $(n - 1)!$

We must show that $b < n - 1$, and hence, b is a factor of $(n - 1)!$

Since $p \geq 2$, we have $n = pb \geq 2b$

$$\text{i.e., } n \geq 2b \Rightarrow \frac{n}{2} \geq b$$

Observe: $n - 1 > \frac{n}{2}$ for $n > 2$

$$\text{Hence, } n - 1 > \frac{n}{2} \geq b.$$

$$\text{i.e., } n - 1 > b.$$

Therefore, b is a factor of $(n - 1)!$ ■

(c) Any integer of the form $8^n + 1$ where $n \geq 1$, is composite.

Proof. Observe: $8^n + 1 = (2^3)^n + 1 = (2^n)^3 + 1^3 = (2^n + 1)((2^n)^2 - 2^n + 1)$ which is composite. ■

(d) Each integer $n > 11$ can be written as the sum of two composite numbers.

Proof. Case 1: (n is even)

Since n is even, $n = 2k$ for some $k \geq 6$.

Hence, $n = 2(k - 3) + 6$ (The sum of two composites)

Case 2: (n is odd)

Since n is odd, $n = 2k + 1$ for some $k \geq 5$.

Hence, $n = 2(k - 4) + 9$ (The sum of two composites) ■

7. Find all the prime numbers that divide $50!$

Observe: $50! = 50 \cdot 49 \cdot 48 \cdot \dots \cdot 3 \cdot 2 \cdot 1$

By the corollary to Theorem 3.1, any prime p that divides this product must divide one of these factors. Hence, $50!$ contains no prime factor greater than 50.

Furthermore, every prime factor less than 50 appears explicitly in the factorization $50! = 50 \cdot 49 \cdot 48 \cdot \dots \cdot 3 \cdot 2 \cdot 1$.

Hence the prime factors of $50!$ are exactly the prime numbers less than 50.

$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$

8. If $p \geq q \geq 5$, and p and q are both prime, prove that $24 \mid (p^2 - q^2)$.

Proof. Let the hypotheses be given. (i.e., Suppose that $p \geq q \geq 5$, and p and q are both prime.)

Our proof hinges on four important observations.

Observation #1: p and q have the form $2k + 1$, AND p and q can only have the forms $3k + 1$ or $3k + 2$.

Since p and q are both prime and both greater than or equal to 5, neither p nor q is even and neither p nor q is a multiple of 3.

Thus, p and q must have the form $2k + 1$ (with reference to 2 as a divisor),

AND p and q can only have the forms $3k + 1$ or $3k + 2$ (with reference to 3 as a divisor).

Observation #2: $\forall n \in \mathbb{N}$, $n^2 + n$ is even.

The reason for this is simple. Either n is even or it is odd.

If n is even, then $n = 2k$ for some $k \in \mathbb{N}$

$$\Rightarrow n^2 + n = n(n + 1) = 2k(n + 1).$$

(i.e., $2 \mid (n^2 + n)$)

If n is odd, then $n + 1$ is even, and $n + 1 = 2k$ for some $k \in \mathbb{N}$,

$$\Rightarrow n^2 + n = n(n + 1) = n(2k) = 2(nk).$$

(i.e., $2 \mid (n^2 + n)$)

Observation #3: $8 \mid (p^2 - q^2)$

By Observation #1, $p = 2j + 1$ and $q = 2k + 1$ for some $j, k \in \mathbb{N}$.

Thus, $(p^2 - q^2) = (2j + 1)^2 - (2k + 1)^2 = (4j^2 + 4j + 1) - (4k^2 + 4k + 1)$

$$= 4 \left[\underbrace{(j^2 + j)}_{\text{even}} - \underbrace{(k^2 + k)}_{\text{even}} \right] = 4(2m) = 8m \text{ for some } m \in \mathbb{N}.$$

i.e., $(p^2 - q^2) = 8m$ for some $m \in \mathbb{N}$.

Therefore, $8 \mid (p^2 - q^2)$

Observation #4: $3 \mid (p^2 - q^2)$

By Observation #1, p and q can only have the forms $3k + 1$ or $3k + 2$ for some $k \in \mathbb{N}$.

If $p = 3j + 1$ and $q = 3k + 1$, then

$$\begin{aligned} p^2 - q^2 &= (3j + 1)^2 - (3k + 1)^2 = (9j^2 + 6j + 1) - (9k^2 + 6k + 1) \\ &= [(9j^2 + 6j) - (9k^2 + 6k)] = 3[(3j^2 + 2j) - (3k^2 + 2k)] = 3m \text{ for some } m \in \mathbb{N} \end{aligned}$$

If $p = 3j + 2$ and $q = 3k + 1$, then

$$\begin{aligned} p^2 - q^2 &= (3j + 2)^2 - (3k + 1)^2 = (9j^2 + 12j + 4) - (9k^2 + 6k + 1) \\ &= [(9j^2 + 12j + 3) - (9k^2 + 6k)] = 3[(3j^2 + 4j + 1) - (3k^2 + 2k)] \\ &= 3m \text{ for some } m \in \mathbb{N} \end{aligned}$$

($p = 3j + 1$ and $q = 3k + 2$ is similar to the previous case.)

If $p = 3j + 2$ and $q = 3k + 2$, then

$$\begin{aligned} p^2 - q^2 &= (3j + 2)^2 - (3k + 2)^2 = (9j^2 + 12j + 4) - (9k^2 + 12k + 4) \\ &= [(9j^2 + 12j) - (9k^2 + 12k)] = 3[(3j^2 + 4j) - (3k^2 + 4k)] \\ &= 3m \text{ for some } m \in \mathbb{N} \end{aligned}$$

Thus, in each case, $3 \mid (p^2 - q^2)$ (end of Observation #4)

We have established that $8 \mid (p^2 - q^2)$ and $3 \mid (p^2 - q^2)$.

Since 3 and 8 are relatively prime, their product 24 also divides $(p^2 - q^2)$, by Corollary 2, page 23. ■