Gregory Croisdale, HW2

8/31/2020

University of Tennessee

Problems 9, 10, 11, 26, 27, 32, 42, and 47.

9. Prove that any prime of the from $3k + 1$ is of the form $6k + 1$.

To say that $3k + 1$ is of the form $6k + 1$ is the same as saying that $3k + 1 = 3(2 \cdot j) + 1$; i.e, k is an even number.

Let us prove this by contradiction (assuming k is odd). Assume $\exists j \in \mathbb{Z} : 3(2j + 1) + 1$ is prime.

This can be rewritten as $6j + 4$. However, it can be plainly seen that $2|(6j + 4)$ and $\nexists j \in \mathbb{Z} : (6j + 4) = 2$. $6j + 4$ cannot be prime.

Therefore, our original assumption is false. k must be even.

10. Prove that any positive integer of the form $3k + 2$ has a prime factor of the same form; similarly for each of the forms $4k + 3$ and $6k + 5$.

$3k + 2$:

Let us assume that $3k + 2$ does not have a prime factor of the same form. We know that it must have at least one prime factor by the fundamental theory of arithmetic. Let's call it p. p must take the form of either $p = 3a$ or $p = 3a + 1$.

Case I: $p = 3a \Rightarrow p = 3$ (as 3 is the only prime in that form). However, we know that $3 \nmid 3k + 2$, so $p \neq 3$.

Case II: $p = 3a + 1$. Keep in mind that we know that none of the prime factors are of the form $3k$ and we are assuming that none are of the form $3k + 2$.
$\Rightarrow \exists b \in \mathbb{Z} : (3b + 1) \cdot (3a + 1) | 3k + 2$.
However, $(3b + 1) \cdot (3a + 1) = 9ab + 3a + 3b + 1 \equiv 1 \pmod 3$. Because $3k + 2 \equiv 2 \pmod 3$, $(3b + 1) \cdot (3a + 1) \nmid 3k + 2$.

Therefore, p must be of the form $3k + 2$.

$4k + 3$:

As a consequence of the division algorithm, we know that all integers must take the form of either $4k, 4k + 1, 4k + 2$, or $4k + 3$. Let's prove the existence of prove a prime factor of the form $4k + 3$ by assuming that such a factor does not exist.

Case I: $4k | 4k + 3$. This can be instantly dismissed, as $4k$ is even and $4k + 3$ is not.

Case II: $4k + 2 | 4k + 3$. Likewise, we can dismiss this case, as $4k + 2$ is even and $4k + 3$ is not.

Case III: $4k + 1 | 4k + 3$. Because of the eliminations we made in Cases I and II, we can conclude that all prime factors are of the form $4k + 1$. $(4k_1 + 1)(4k_2 + 1) = 4(4k_1k_2 + k_1 + k_2)$ which is another number of the same form. Therefore, we cannot possibly obtain a number of the form $4k + 3$.

Because none of these possibilities fulfill our requirements, we can conclude that a number that fulfils the form $4k + 3$ has a prime factor of the same form.

$6k + 5$:

As a consequence of the division algorithm, we know that all integers must take the form of either $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4$, or $6k + 5$. Let's prove the existence of prove a prime factor of the form $6k + 5$ by assuming that such a factor does not exist.

Case I: $6k | 6k + 5$. This can be instantly dismissed, as $6k$ is even, but $6k + 5$ is not.

Case II: $6k + 2 | 6k + 5$ This can be instantly dismissed, as $6k + 2$ is even, but $6k + 5$ is not.

Case III: $6k + 3 | 6k + 5$ This can be instantly dismissed, as $6k + 3$ is divisible by 3, but $6k + 5$ is not.

Case IV: $6k + 4 | 6k + 5$. This can be instantly dismissed, as $6k + 4$ is even, but $6k + 5$ is not.

Case V: $6k + 1 | 6k + 5$. We know that we need at least one other prime factor, p, in order to reach $6k + 5$. By our previous cases, however, we know that it must be of the form $6k + 1$. Because to numbers of the same form multiplied together are the same form, we know that $p \cdot 6k + 1 \nmid 6k + 5$. Therefore, $6k + 1$ cannot be a prime factor.

Because we have disproved the existence of all of the other possible prime factors, we know that a prime factor of the form $6k + 5$ must exist for all numbers of the form $6k + 5$.

11. If x and y are odd, prove that x^2+y^2 cannot be a perfect square.

Let $x=(2k+1)$ and let $y=(2j+1)$ where $k,j\in\mathbb{Z}$.

$\Rightarrow x^2+y^2=(2k+1)^2+(2j+1)^2=4k^2+4k+4j^2+4j+2=2(2k^2+2k+2j^2+2j+1)$.

Let us assume that a^2 = $2(2k^2+2k+2j^2+2j+1)$.

This implies that $a=\pm\sqrt{2}\sqrt{2k^2+2k+2j^2+2j+1}$.

Because $2k^2+2k+2j^2+2j+1$ is of the form $2\cdot n+1$, it must be odd.

Therefore, $2\nmid 2k^2+2k+2j^2+2j+1\Rightarrow\sqrt{2}\nmid\sqrt{2k^2+2k+2j^2+2j+1}$.

The only way to turn $\sqrt{2}$ into an integer is to multiply it by itself. However, we have just proved that the expression cannot produce another $\sqrt{2}$. This means that $\sqrt{2}|a\Rightarrow a\notin\mathbb{Z}$.

Therefore, x^2+y^2 cannot be a perfect square.

26. Prove that there are infinitely many primes of the form $4n+3$; of the form $6n+5$.

$4n+3$:

Let us assume that there are finitely many primes of the form $4n+3$. We will make a product of all such primes and subtract one to find a coprime.

$a=(p_1p_2...p_n)$. Note that $4a-1$ is of the form $4a+3$. Let $b=4a-1$.

By the proof we completed in problem 11, we know that b has at least one prime factor of the form $6n+5$.

However, we also know that $p_1,p_2...p_n\nmid b$, as it was specifically constructed as a coprime.

We also know that $\exists k\in\mathbb{N}: k\leq b$, $k|b$, and k is prime.

Because we know that none of the finitely many primes of the form $4n+3$ divide b, $k=b$.

This results in a contradiction, as k is prime and is not in $p_1,p_2...p_n$. Therefore, our original assumption is false.

There must be infinitely many primes of the form $4n+3$.

$6n + 5$:

Let us assume that there are finitely many primes of the form $6n + 5$. We will make a product of all such primes and subtract one to find a coprime.

$a = (p_1 p_2 \ldots p_n)$. Note that $6a - 1$ is of the form $6n + 5$. Let $b = 6a - 1$.

By the proof we completed in problem 11, we know that b has at least one prime factor of the form $6n + 5$.

However, we also know that $p_1, p_2 \ldots p_n \nmid b$, as it was specifically constructed as a coprime.

We also know that $\exists k \in \mathbb{N} : k \leq b$, $k|b$, and k is prime.

Because we know that none of the finitely many primes of the form $6n + 5$ divide b, $k = b$.

This results in a contradiction, as k is prime and is not in $p_1, p_2 \ldots p_n$. Therefore, our original assumption is false.

There must be infinitely many primes of the form $6n + 5$.

27. Prove that any $n|(n-1)!$ for all composite $n > 4$.

Because n is not prime and by the fundamental theorem of arithmetic we know that $\exists i, j \in \mathbb{Z} : ij = n$ and $i, j < n$.

Because of the definition of factorial, we know that $\forall x \in \mathbb{N} : x \leq a, x|a!$. Likewise, we can say that when $a = n - 1$, $x|(n-1)!$ when $x \leq (n-1)$.

Because $i, j < n$, we can say that $i, j|(n-1)!$ and $ij = n \Rightarrow n|(n-1)!$.

32. Show that $n^4 + 4$ is composite for all $n > 1$.

$n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2)$.

If we let $a = (n^2 - 2n + 2)$ and $b = (n^2 + 2n + 2)$, we see that $n^4 + 4 = ab$ and $a, b \in \mathbb{Z}$.

42. If $2^n + 1$ is an odd prime for some integer n, prove that n is a power of 2.

Let's prove this by contradiction - let us assume that $2^n + 1$ is an odd prime, but n is not a power of two.

This means that $\exists a, b \in \mathbb{Z} : ab = n$, a is odd, and $1 \leq a, b < n$.

This is an identity revealed in class:

$2^k + 1 = (2 + 1)(2^{k-1} - 2^{k-2} + 2^{k-3} - \ldots + 1)$ when k is odd.

Then $2^n + 1 = 2^{ab} + 1 = (2^a)^b + 1 = (2+1)^b(2^{k-1} - 2^{k-2} + 2^{k-3} - \ldots + 1)^b$

$\Rightarrow 3|2^n + 1$.

47. Prove that $2+\sqrt{-6}$ and $2-\sqrt{-6}$ are primes in the class C of numbers $a+b\sqrt{-6}$

Let us assume that $2 \pm \sqrt{-6}$ is composite.

$$\Rightarrow \exists a,b,c,d \in \mathbb{Z} : |(a+b\sqrt{-6})| \cdot |(c+d\sqrt{-6})| = |2 \pm \sqrt{-6}|.$$
$$\Rightarrow |(a+b\sqrt{-6})| \cdot |(c+d\sqrt{-6})| = \sqrt{10}.$$
$$\Rightarrow |(a+b\sqrt{-6})| = \sqrt{2} \text{ and } |(c+d\sqrt{-6})| = \sqrt{5}$$
$$\text{(Or we could flip the terms around, but that's arbitrary.)}$$
$$\Rightarrow \sqrt{a^2+6b} = \sqrt{2} \Rightarrow b = \frac{1}{6}(2-a^2)$$
$$\Rightarrow b \notin \mathbb{Z}.$$

Therefore, $2 \pm \sqrt{-6}$ cannot be composite. It must be prime in its class.