Math 310 Homework 4

Jacob Shiohira

August 29, 2017

Note: This homework took a total of 6 hours. I initially did it alone, but I did review with Jacob Warner.

Problem 1. Which of the following numbers are prime?

Note: Theorem 1.10 says let $n > 1$. If n has no positive prime factor less than or equal to $\sqrt{n}$, then n is prime.

(a) 701 - According to Theorem 1.10, $n > 1$ and $\sqrt{701} \approx 26.4764$. Then, $2, 3, 5, 7, 11, 13, 17, 19, 23$ are all the prime numbers less than $\sqrt{701}$ but none are factors of 701. Thus, 701 is prime.

(b) 1009 - According to Theorem 1.10, $n > 1$ and $\sqrt{1009} \approx 31.7648$. Then, $2, 3, 5, 7, 11, 13, 17, 19, 23,$ $29, 31$ are all the prime numbers less than $\sqrt{1009}$ but none are factors of 1009. Thus, 1009 is prime.

(c) 1949 - According to Theorem 1.10, $n > 1$ and $\sqrt{1949} \approx 44.1475$. Then, $2, 3, 5, 7, 11, 13, 17, 19, 23,$ $29, 31, 37, 41, 43$ are all the prime numbers less than $\sqrt{1949}$ but none are factors of 1949. Thus, 1949 is prime.

(d) 1951- According to Theorem 1.10, $n > 1$ and $\sqrt{1951} \approx 44.1701$. Then, $2, 3, 5, 7, 11, 13, 17, 19, 23,$ $29, 31, 37, 41, 43$ are all the prime numbers less than $\sqrt{1951}$ but none are factors of 1951. Thus, 1951 is prime.

Problem 2. Let p be an integer other than $0, \pm 1$ with this property: Whenever b and c are integers such that $p|bc$, then $p|b$ or $p|c$. Prove that p is prime. [$Hint$: If d is a divisor of p, say $p = dt$, then $p|d$ or $p|t$. Show that this implies $d = \pm p$ or $d = \pm 1$.

Consider $p \in \mathbb{Z}$, $p \neq 0, \pm 1$. Assume that there are integers b and c such that $p|bc$, and therefore, $p|b$ or $p|c$. We then want to show that p is a prime number. Consider $p > 1$, and remember that p is said to be prime if and only if $-p$ is prime. Suppose there exist integers d, t such that $p = dt$,

$$0 < d \leq p \text{ and } 0 < t \leq p.$$

By assumption $p|d$ or $p|t$. Thus, $d = p$ and $t = 1$ or $d = 1$ and $t = p$.

This then implies that the only positive divisors of p are 1 and p; therefore, the only divisors of p are ± 1 and $\pm p$. So, p is prime. $\square$

Problem 3. Prove that $(a, b) = 1$ if and only if there is no prime p such that $p|a$ and $p|b$.

Let $a, b, p \in \mathbb{Z}$, $p \neq 0, \pm 1$. Since the proposition features a biconditional, the proof proceeds into the following cases

1. If $(a, b) = 1$, then there is no prime p such that $p|a$ and $p|b$.
2. If there is no prime p such that $p|a$ and $p|b$, then $(a, b) = 1$.

We will proceed with two following cases by assuming the "if" part of the statement is true and trying to deduce the "then" part of the statement.

Case I If $(a, b) = 1$, then there is no prime p such that $p|a$ and $p|b$.

Suppose $(a, b) = 1$. We then want to show that there is no prime p such that $p|a$ and $p|b$. We say a and b are relatively prime since the $\gcd(a, b) = 1$. By definition, 1 is the largest integer that divides both a and b. Assume that $p|(a, b)$ and therefore $p|1$. However, it was said that $p \neq 0, \pm 1$ and thus $p > 1$. Therefore, there is no prime p such that $p|a$ and $p|b$.

Case II If there is no prime p such that $p|a$ and $p|b$, then $(a, b) = 1$.

We move forward with proof by contrapositive. Suppose there is no prime p such that $p|a$ and $p|b$. We then want to show that $(a, b) = 1$. Assume there exists an integer c such that $c|a$ and $c|b$. Then, we know $c|p$. Well, we know that $p \geq 2$ but that p does not divide a and p does not divide b. So, by assumption of $p > 1$ and by requirement of gcd, $0 < c < p$, where $p > 1$. Thus, c must equal 1 where $\gcd(a, b) = 1$.

Problem 4. Prove that $a|b$ if and only if $a^2|b^2$. $[Hint$: Exercise 19]

Let $a, b \in \mathbb{Z}$. Since the proposition features a biconditional, the proof proceeds in the following cases

1. If $a|b$, then $a^2|b^2$,
2. If $a^2|b^2$, then $a|b$.

We will proceed with two following cases by assuming the "if" part of the statement is true and trying to deduce the "then" part of the statement.

Case I If $a|b$, then $a^2|b^2$.

Assume $a|b$. By the definition of divisibility, $b = ak$ for some $k \in \mathbb{Z}$. Then, if both sides are squared, we get

$$\begin{aligned} b^2 &= (ak)^2 \\ &= a^2k^2 \end{aligned}$$

We get the most recent result because multiplication is distributive. Further, since the integers are closed under multiplication and addition, we know that k^2 also results in an integer. So, again by the definition of divisibility, $a^2|b^2$.

Case II If $a^2|b^2$, then $a|b$.

By the fundamental theorem of arithmetic,

$$a = p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k} \quad b = p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}$$

where $p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ and $b = p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}$ are positive, distinct primes and $r_i, s_i \geq 0$. From *Exercise 19*, we know $a|b$ if $r_i \leq s_i$ for all i. So, it follows that $a^2 = p_1^{2r_1}p_2^{2r_2}\cdots p_k^{2r_k}$ and $b^2 = p_1^{2s_1}p_2^{2s_2}\cdots p_k^{2s_k}$. Since we assumed that $a^2|b^2$, then, we see that $2r_i \leq 2s_i$ for all i (again, Exercise 19). By dividing by 2 on both sides, we see that $r_i \leq s_i$ follows for all i. Thus, $a|b$.

We have seen that $a|b \implies a^2|b^2$ from Case I and $a^2|b^2 \implies a|b$ from Case II. Thus, by combining those two results, we get that $a|b$ if and only if $a^2|b^2$. $\square$

Problem 5. Prove that for all $n \geq 1$,

$$\sum_{i=1}^{n} i^2 = \tfrac{n(n+1)(2n+1)}{6}.$$

We will proceed using induction. First, we will show that the proposition holds for the base case ($n = 1$) and then see that the proposition holds for all n.

Base Case: $n = 1$

The sum of i from 1 to 1 is in fact just 1. Additionally, by plugging into the right hand side of the equation, we get

$$\tfrac{1(2)(3)}{6} = 1.$$

Thus, the proposition holds for the base case.

Inductive Case: For $m > 1$ and $1 \leq k \leq m$, suppose

$$\sum_{i=1}^{k} i^2 = \tfrac{k(k+1)(2k+1)}{6}.$$

Then, for $m+1$, we want to show that $\sum\limits_{i=1}^{m+1} i^2 = \frac{(m+1)(m+2)(2m+3)}{6} = \frac{2m^3+9m^2+13m+6}{6}$. Well,

$$\sum_{i=1}^{m+1} i^2 = [1^2 + 2^2 + ... + m^2] + (m+1)^2. \tag{1}$$

Thus, by using the inductive hypothesis, we get

$$\begin{aligned}
\sum_{i=1}^{m+1} i^2 &= \sum_{i=1}^{m} i^2 + (m+1)^2 \\
&= \frac{m(m+1)(2m+1)}{6} + (m+1)^2 \\
&= \frac{2m^3+3m^2+m}{6} + \frac{6(m^2+2m+1)}{6} \\
&= \frac{(2m^3+3m^2+m)+(6m^2+12m+6)}{6} \\
&= \frac{2m^3+9m^2+13m+6}{6}.
\end{aligned}$$

The proposition holds for all $1 \le k \le m+1$, so the proposition must hold for all n. $\square$

Problem 6. Use induction to prove that for all $n \ge 1$,

$$\tfrac{d}{dx}(x^n) = nx^{n-1}.$$

(Use the fact that $\frac{d}{dx}(x) = 1$ and the product rule $\frac{d}{dx}(fg) = f\frac{dg}{dx} + g\frac{df}{dx}$.)

We will proceed using induction. First, we will show that the proposition holds for the base case ($n = 1$) and then see that the proposition holds for all n.

Base Case: $n = 1$

Remember that we are using the fact that $\frac{d}{dx}(x) = 1$, which proves the left side of the equation holds. Then, we look at the right side of the equation,

$$1x^{1-1} = 1x^0 = 1.$$

Thus, the proposition holds for the base case $n = 1$.

Inductive Case: For $m > 1$ and $1 \le k \le m$, suppose

$$\tfrac{d}{dx}(x^k) = kx^{k-1}.$$

Then, we want to show that for $m+1$, $\frac{d}{dx}(x^{m+1}) = \frac{d}{dx}(x^m x^1)$. We will now utilize the product rule, as stated above.

$$\frac{d}{dx}(x^m x) = x^m \frac{dx}{dx} + \frac{d}{dx}(x^m)x.$$

By using the inductive hypothesis,

$$\begin{aligned}
\frac{d}{dx}(x^m x) &= x^m \frac{d}{dx} + \frac{d}{dx}(x^m)x \\
&= x^m 1 + (mx^{m-1})x \\
&= x^m + mx^{m-1+1} \\
&= (1+m)x^m \\
&= (m+1)x^{(m+1)-1}
\end{aligned}$$

The proposition holds for all $1 \leq k \leq m+1$, so the proposition must hold for all n. $\square$

Problem 7. Prove or disprove: If n is an integer and $n > 2$, then there exists a prime p such that $n < p < n!$.

Suppose n is an integer and $n > 2$. We then want to show that there exists a prime p such that $n < p < n!$. We are trying to prove a property for all n, thus we will proceed by induction.

Base Case Since we assumed $n > 2$, our base case is represented by $n = 3$. For $n = 3$, we need to find a prime p such that $3 < p < 3 \cdot 2 \cdot 1 = 3! = 6$. Well, 5 is a prime integer that satisfies the inequality. Thus, the proposition holds for the base case of $n = 3$.

Inductive Step Suppose $m \geq 3$ and for all $3 \leq k \leq m$, there exists a prime p that satisfies $k < p < k!$. We then want to show that the proposition holds for $m+1$ by showing there exists a prime p such that $(m+1) < p < (m+1)!$.

$$\begin{aligned}
(m+1) &< (m+1)! \\
(m+1) &< (m+1)m! \\
1 &< m!
\end{aligned}$$

The proposition holds for all $3 \leq k \leq m+1$, so the proposition must hold for all n. $\square$