Math 115A Homework 1

Ethan Martirosyan

January 22, 2024

Problem 1

By the Fundamental Theorem of Arithmetic, we may write $c = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ for some distinct primes $p_1, \ldots, p_k$ and $\beta_1, \ldots, \beta_k > 0$. Then $ab = p_1^{2\beta_1} \cdots p_k^{2\beta_k}$. Every prime p_i must divide a or b. To prove this, let us suppose that p_i does not divide a. Then, we claim that p_i must divide b. If p_i does not divide a, then $(a, p_i) = 1$. Then, there must exist integers l, m such that

$$al + p_i m = 1$$

Multiplying both sides by b, we find that

$$abl + p_i bm = b$$

Then p_i divides abl and $p_i bm$, so it also divides $abl + p_i bm = b$. This proves that p_i divides either a or b. If p_i divides a, then a must have all the copies of p_i in its prime factorization (if b contained any copies of p_i in its prime factorization, then (a, b) would be greater than 1, a contradiction). Since this is true for every prime p_i, we may conclude that a and b are equal to a product of terms from the list $p_1^{2\beta_1}, \ldots, p_k^{2\beta_k}$. Since $p_i^{2\beta_i} = (p_i^{\beta_i})^2$, we may conclude that there exist constants c_1 and c_2 such that $a = c_1^2$ and $b = c_2^2$.

Problem 2

First, we must prove that exactly one of x and y is even and the other is odd. For the sake of contradiction, we may first suppose that x and y are both even. We may write $x = 2p$ and $y = 2q$ for integers p and q. Then, we have

$$x^2 + y^2 = z^2 \implies (2p)^2 + (2q)^2 = z^2 \implies 4(p^2 + q^2) = z^2 \implies 4 \mid z^2 \implies 2 \mid z$$

Then, we have $(x, y, z) \geq 2$, which is false by assumption. Next, we may suppose that x and y are both odd. Thus, we may write $x = 2p + 1$ and $y = 2q + 1$ for some positive integers p and q. Notice that

$$x^2 + y^2 = (2p+1)^2 + (2q+1)^2 = 4p^2 + 4p + 1 + 4q^2 + 4q + 1 = 2(2p^2 + 2p + 2q^2 + 2q + 1) = z^2$$

Thus we find that $2 \mid z^2$, which implies that $2 \mid z$. We may write $z = 2t$. Then, we find that

$$2(2p^2 + 2p + 2q^2 + 2q + 1) = 4t^2$$

from which we obtain

$$2p^2 + 2p + 2q^2 + 2q + 1 = 2t^2$$

This says that an odd number is equal to an even number, which is false. Therefore, we know that one of x and y must be even and the other must be odd.

Next, we must show that

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1$$

Note that $(z+y)/2$ and $(z-y)/2$ are integers because z and y are both odd. Suppose that d is a common divisor of $\frac{z+y}{2}$ and $\frac{z-y}{2}$. Then it must divide their sum and difference, so $d \mid z$ and $d \mid y$. We claim that y and z are pairwise prime. If this were not the case, then there would be some prime p such that $p \mid y$ and $p \mid z$. From the relation $x^2 + y^2 = z^2$, we would have $p \mid x^2$, so that $p \mid x$, which would imply that x, y, z are not relatively prime. This is a contradiction. Thus, y and z are pairwise prime. Since d divides pairwise prime numbers, we have $d = 1$. This means that

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1$$

Now, we know that

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

and we just established that

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1$$

Appealing to problem 1, there must be integers m and n such that

$$\frac{z+y}{2} = m^2$$

and

$$\frac{z-y}{2} = n^2$$

Adding m^2 and n^2, we obtain

$$z = m^2 + n^2$$

Subtracting n^2 from m^2 yields

$$y = m^2 - n^2$$

Finally, we have

$$x^2 = z^2 - y^2 = m^4 + 2m^2n^2 + n^4 - (m^4 - 2m^2n^2 + n^4) = 4m^2n^2$$

so that

$$x = 2mn$$

Problem 3

We will prove this result by induction. First, let us suppose that $N = (4n_1 + 1)(4n_2 + 1)$, where n_1 and n_2 are integers. We obtain

$$(4n_1 + 1)(4n_2 + 1) = 16n_1n_2 + 4n_1 + 4n_2 + 1 = 4(4n_1n_2 + n_1 + n_2) + 1$$

Now, let us suppose that N is the product of the primes $4n_1 + 1, \ldots, 4n_{k+1} + 1$. By our induction hypothesis, we know that

$$(4n_1 + 1) \cdots (4n_k + 1) = 4m + 1$$

for some integer m. Then, we find that

$$(4m + 1)(4n_{k+1} + 1) = 16mn_{k+1} + 4m + 4n_{k+1} + 1 = 4(4mn_{k+1} + m + n_{k+1}) + 1$$

By induction, we have shown that if N is a product of any number of primes of the form $4n + 1$, then $N = 4M + 1$, where M is an integer.

Problem 4

By the Fundamental Theorem of Arithmetic, we may factor the number $N = 4p_1 \cdots p_k + 3$ into primes as follows:

$$N = q_1 \cdots q_j$$

First, we claim that some q_i is of the form $4n+3$. Suppose this were not true. Then every q_i must be of the form $4n+1$, so their product would also be of the form $4M+1$ by Problem 3. However, it is evident that N is of the form $4M+3$, so there must exist some prime q_i of the form $4n+3$, which we may denote q. Next, we claim that this q is not equal to any of $p_1, \ldots, p_k$. Notice that none of the primes $p_1, \ldots, p_k$ divide N. If some p_i did divide N, then it would also have to divide $3 = N - p_1 \cdots p_k$, which cannot happen because we assumed that $p_1, \ldots, p_k$ were all greater than 3. Since q does divide N, it is evident that q is not equal to any of the primes $p_1, \ldots, p_k$.

Problem 5

Suppose there were only finitely many primes $p_1, \ldots, p_k$ of the form $4n+3$. As in problem 4, we may consider the number $N = 4p_1 \cdots p_k + 3$. In problem 4, we proved that N has some prime factor q that is of the form $4n+3$ that is not equal to any of the primes $p_1, \ldots, p_k$. This contradicts the assumption that $p_1, \ldots, p_k$ constituted the complete list of primes of the form $4n+3$. Thus there must be infinitely many primes of the form $4n+3$.

Problem 6

Suppose that there were only finitely many primes $p_1, \ldots, p_k$ of the form $6n + 5$. Consider the number

$$N = 6p_1 \cdots p_k + 5$$

By the Fundamental Theorem of Arithmetic, we may factorize N into primes as follows:

$$N = q_1 \ldots q_j$$

We claim that one of these primes q_i must be of the form $6n+5$. For the sake of contradiction, suppose that all of the primes $q_1, \ldots, q_j$ were of the form $6n + 1$. Then their product would also be of the form $6n + 1$. To see this, consider the integers $6n + 1$ and $6m + 1$. Their product is

$$(6n + 1)(6m + 1) = 36mn + 6n + 6m + 1 = 6(6mn + n + m) + 1$$

By induction, it is evident that the product $q_1 \cdots q_j$ would be of the form $6n + 1$ which contradicts the fact that N is of the form $6n + 5$. Thus, there must exist some prime q of the form $6n + 5$ in the prime factorization of N. Next, we claim that q is not equal to any prime in the list $p_1, \ldots, p_k$. Notice that q divides N by construction, but none of the primes $p_1, \ldots, p_k$ divide N. If any of these primes did divide $N = 6p_1 \cdots p_k + 5$, then it would also have to divide $N - 6p_1 \cdots p_k = 5$, which cannot happen. Since q divides N but none of the primes $p_1, \ldots, p_k$ divide N, we know that q is not equal to any of the primes $p_1, \ldots, p_k$. Thus, we may conclude that there must be infinitely many primes of the form $6n + 5$.

Problem 7

For the sake of contradiction, suppose that

$$S_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

was an integer. Then the product of S_n with any other integer must also be an integer (since integers are closed under multiplication). We aim to construct an integer whose product with S_n is not an integer. Let k be the largest integer such that $2^k \leq n$. Let N be equal to $2^{k-1} \cdot p$ (where p is the product of all the odd integers less than n). We claim that for every integer m that is less than or equal to n and not equal to 2^k, N/m is an integer. Let m be an arbitrary integer less than or equal to n and not equal to 2^k. We may write $m = 2^a \cdot b$, where b is odd. First, we claim that b divides p. This is evident because b is an odd number less than n so it divides p by the definition of p (recall that p was defined to be the product of all odd integers less than n). Next, we claim that $a \leq k-1$. Suppose that $a \geq k$. If $b = 1$ and $a = k$, then $m = 2^k$, contradicting our assumptions on m. If $b > 1$ or $a > k$, then $m = 2^a \cdot b \geq 2^{k+1} > n$, again contradicting our assumptions about m. Thus, we may deduce that $a \leq k-1$. Now, we note that $2^a \mid 2^{k-1}$ and $b \mid p$, so $m = 2^a \cdot b \mid 2^{k-1} \cdot p = N$. Let us consider $N/2^k$. This is equal to $2^{k-1}p/2^k = p/2$. Since p is odd, this is not an integer. Notice that

$$NS_n = \sum_{j=1}^{n} \frac{N}{j} = \sum_{j \neq 2^k} \frac{N}{j} + \frac{N}{2^k} = \sum_{j \neq 2^k} \frac{N}{j} + \frac{p}{2}$$

Notice that the first sum is an integer, but $p/2$ is not. Thus, NS_n is not an integer. Since N is an integer, we must conclude that S_n is not an integer.