Math 117 Fall 2014 Homework 1 Solutions

Due Thursday Sept. 11 3pm in Assignment Box

Question 1. (5 pts) *Prove that 11 is prime but 57 is not.*

Proof.

- 11 is prime.

  First for any number $n > 11$, $n \nmid 11$. Now we check $1 | 11, 11 | 11$ but

  $$2 \nmid 11, 3 \nmid 11, 4 \nmid 11, 5 \nmid 11, 6 \nmid 11, 7 \nmid 11, 8 \nmid 11, 9 \nmid 11, 10 \nmid 11. \tag{1}$$

  Therefore the only divisors of 11 are 1 and 11, which means 11 is prime.

- 57 is not prime (that is 57 is composite). Since $57 = 3 \times 19$, $3 | 57$ and therefore 57 is not prime.

□

Question 2. (5 pts) *Let n be an arbitrary natural number. Prove that $4 \nmid (n^2 + 2)$. (Hint:[1])*

Proof. Let n be an arbitrary natural number. Then either n is even or n is odd. We discuss the two cases.

- n is even.

  By definition we know there is $k \in \mathbb{N}$ such that $n = 2k$. This gives $n^2 + 2 = (2k)^2 + 2 = 4k^2 + 2$. Now assume $4 | (n^2 + 2)$. Then there is $l \in \mathbb{N}$ such that

  $$4k^2 + 2 = n^2 + 2 = 4l \tag{2}$$

  which gives

  $$2 = 4l - 4k^2 = 4(l - k^2) \tag{3}$$

  which in turn leads to

  $$1 = 2(l - k^2). \tag{4}$$

  The left hand side is odd and the right hand side is even. Contradiction. Therefore $4 \nmid (n^2 + 2)$.

- n is odd.

  By definition there is $k \in \mathbb{N}$ such that $n = 2k - 1$. This gives

  $$n^2 + 2 = (2k - 1)^2 + 2 = 4k^2 - 4k + 3 = 2[2k^2 - 2k + 2] - 1. \tag{5}$$

  We have $2k^2 - 2k + 2 \in \mathbb{Z}$ and furthermore it is no less than 1. Therefore $n^2 + 2$ is odd and could not be divided by 4. □

Question 3. (5 pts) *Given that there are infinitely many pairs of prime numbers with difference $< 7 \times 10^7$. Prove that there is a natural number $d < 7 \times 10^7$ such that there are infinitely many pairs of prime numbers with difference exactly d.*

Proof. Assume the contrary. Then for every $d < 7 \times 10^7$ there are only finitely many pairs of primes with difference d. In other words, there are finitely many pairs with difference 1, finitely many pairs with difference 2, ..., finitely many pairs with difference $7 \times 10^7 - 1$. Since the sum of $7 \times 10^7 - 1$ numbers is still finite, we see that there are finitely many pairs with difference less than 7×10^7. This contradicts what is given. □

1. Discuss n even/odd.

QUESTION 4. (5 PTS) *Prove that there are infinitely many primes of the form* $4n+3$ *(that is when divided by* 4*, the remainder is* 3*. (Hint:*[2] *)*

Proof. We prove by contradiction. Assume the contrary. Then there are only finitely many primes of the form $4n+3$. We can list them as $p_1, \ldots, p_m$. Now define

$$q = 4\, p_1\, p_2 \cdots p_m - 1. \tag{6}$$

We will show that $q \div 4$ has remainders both 1 and 3 which is of course not possible.

On one hand, by our definition of q, we have

$$q = 4\,(p_1\, p_2 \cdots p_m - 1) + 3. \tag{7}$$

Therefore $q \div 4$ has remainder 3.

On the other hand, since $p_1, \ldots, p_m |\, (q+1)$, none of the p_i's could be a divisor for q. Together with the fact that q is odd, we see that, by the Fundamental Theorem of Arithmetic,

$$q = q_1\, q_2 \cdots q_k \tag{8}$$

where $q_1, q_2, \ldots, q_k$ are prime different from $p_1, \ldots, p_m, 2$. Now recall that a prime number is either 2 or odd, and every odd number when divided by 4 the remainder is either 1 or 3. Since by our assumption all the primes of the form $4n+3$ are among $p_1, \ldots, p_m$, all the q_i's must be of the form $4n+1$. Thus there are $r_1, \ldots, r_k \in \mathbb{N}$ satisfying

$$q_i = 4\, r_i + 1, \qquad i = 1, 2, \ldots, k \tag{9}$$

that is $q_1 = 4\, r_1 + 1, q_2 = 4\, r_2 + 1, \ldots, q_k = 4\, r_k + 1$.

Substituting these into (8) we have

$$q = (4\, r_1 + 1)\, (4\, r_2 + 1) \cdots (4\, r_k + 1). \tag{10}$$

Expansion of the right hand side product has 2^k terms, each term is a product of k numbers, the first one chosen from $4\, r_1$ and 1, the second one from $4\, r_2$ and 1, ... , the kth one from $4\, r_k$ and 1. We see that unless 1 is chosen every time, the result would be divided by 4. Therefore the remainder for $q \div 4$ would be $1 \times 1 \times 1 \times \cdots \times 1 = 1$.

Thus we have shown that the remainder of $q \div 4$ is at the same time 1 and 3. Contradiction. □

2. Consider $4\, p_1 \cdots p_n - 1$.