5 Problems 1 solution

Pankaj Agarwal

E-mail: pamathsfac@gmail.com

Under the title '5 problems 1 solutions', we intend to discuss 5 problems which can be solved using the same concept. We intend to keep the concept basic. In this particular article, the concept we will be using is as follows.

If p is a prime number and $p > 3$, then p is of the form $6k + 1$ or $6k - 1$, where k is some integer and p^2 is of the form $24m + 1$ where m is some integer.

Proof. Any integer can be written in the form $6k + 0$, $6k + 1$, $6k + 2$, $6k + 3$, $6k + 4$, or $6k + 5$, for some integer k. But $6k + 0, 6k + 2, 6k + 4$ are multiples of 2, while $6k + 3$ is a multiple of 3. So, if p is a prime number and if $p > 3$, then only possibilities are for $6k + 1$ and $6k + 5$.

Case I: If $p = 6k + 1$, then $p^2 = 36k^2 + 12k + 1$, i.e., $p^2 = 12k(3k + 1) + 1$. But $k(3k + 1)$ is always even. So, $p^2 \equiv 1(\text{mod } 24)$.

Case II: If $p = 6k + 5$, then $p^2 = 36k^2 + 60k + 25 = 12k(3k + 5) + 24 + 1$. Again $k(3k + 5)$ is always even. So, $p^2 \equiv 1(\text{mod } 24)$.

So, in both cases p^2 is of the form $24k + 1$, for some integer k. □

Now, how will this concept be applied in problems? To see exactly how this concept will be used, let us look into some examples.

Problem 1. Find all primes p such that the number $p^2 + 11$ has exactly six different divisors (including 1 and the number itself).

(Russia, 1995)

Solution. If $p > 3$, then $p^2 = 24k + 1$, for some integer k. So, $p^2 + 11 = 12(2k + 1)$, which has more than 6 factors as 12 itself has 6 factors.

So, we just need to check for $p = 2$ and $p = 3$. If $p = 2$, then $p^2 + 11 = 15$, which has exactly 4 factors. If $p = 3$, then $p^2 + 11 = 20 = 2^2 \times 5^1$ has exactly 6 factors.

Therefore, $p = 3$ is the only possibility. □

Problem 2. Prove that $a^4 - 10a^2 + 9$ is divisible by 1920 for every prime number $a > 5$.

(Croatia, 1996)

Solution. Since $a > 5$ is a prime number, so $a^2 = 24k + 1$, for some integer k. Therefore,

$$\begin{aligned} a^4 - 10a^2 + 9 = \left(a^2 - 1\right)\left(a^2 - 9\right) &= 24k(24k - 8) \\ &= 24 \times 8 \times k \times (3k - 1). \end{aligned}$$

Now, $k(3k - 1)$ is always even. So, let $a^4 - 10a^2 + 9 = 24 \times 8 \times 2 \times m$, where m is some integer. That is, $a^4 - 10a^2 + 9$ is a multiple of $2^7 \times 3$.

Now, $1920 = 2^7 \times 3 \times 5$. So, we just need to prove that $a^4 - 10a^2 + 9$ is also a multiple of 5.

Since a is prime and $a > 5$. So, $a = 5\ell + 1$, $5\ell + 2$, $5\ell + 3$, or $5\ell + 4$, for some integer ℓ.

Now, $a^4 - 10a^2 + 9 = (a+1)(a-1)(a+3)(a-3)$. Again, if $a = 5\ell + 1, 5\ell + 2, 5\ell + 3$, or $5\ell + 4$, we have $a - 1, a + 3, a - 3$, or $a + 1$ is a multiple of 5 respectively. So, $a^4 - 10a^2 + 9$ is a multiple of 5.

Hence, $a^4 - 10a^2 + 9$ is a multiple of 1920. □

Problem 3. Let n be a positive integer and $p_1, p_2, p_3, \ldots, p_n$ be n prime numbers all greater than 5 such that 6 divides $p_1^2 + p_2^2 + p_3^2 + \cdots + p_n^2$. Prove that 6 divides n.

(RMO India, 1998)

Solution. Since $p_i > 5$ for all $i = 1, 2, 3, \ldots, n$, so $p_i^2 = 24k_i + 1$ for some integers k_i for all $i = 1, 2, 3, \ldots, n$.

Given that 6 divides $p_1^2 + p_2^2 + p_3^2 + \cdots + p_n^2$, i.e., 6 divides $24\left(k_1 + k_2 + k_3 + \cdots + k_n\right) + n$. Therefore, 6 divides n. □

Problem 4. Determine the gcd of all numbers of the form $p^8 - 1$, where p is a prime number and $p > 5$.

(Belgium, Flanders Math Olympiad, 1996)

Solution. As p is a prime number and $p > 5$, we get $p^2 = 24k + 1$ for some integer k. Therefore,

$$p^8 - 1 = \left(p^2 - 1\right)\left(p^2 + 1\right)\left(p^4 + 1\right) = 24k\left(p^2 + 1\right)\left(p^4 + 1\right).$$

Since $p^2 = 24k + 1$, we get $p^2 + 1$ and $p^4 + 1$ both are even, but neither of them is divisible by 3 and 4.

Again, by Fermat's Little Theorem, we get $p^4 - 1$ is a multiple of 5. So, $p^8 - 1$ is a multiple of 5. Therefore, $p^8 - 1$ is a multiple of $24 \times 2 \times 2 \times 5 = 480$. So, the required gcd is a multiple of 480.

Now,

$$7^8 - 1 = (7^2 - 1)(7^2 + 1)(7^4 + 1) = 24 \times 2 \times (7^2 + 1)(7^4 + 1) = 480 \times 2 \times \frac{(7^2 + 1)(7^4 + 1)}{20},$$

and

$$11^8 - 1 = (11^2 - 1)(11^2 + 1)(11^4 + 1) = 24 \times 5 \times (11^2 + 1)(11^4 + 1) = 480 \times 5 \times \frac{(11^2 + 1)(11^4 + 1)}{20}.$$

Now,

$$\gcd\left(2 \times \frac{(7^2 + 1)(7^4 + 1)}{20}, 5 \times \frac{(11^2 + 1)(11^4 + 1)}{20}\right) = \gcd\big(25 \times 1201, 61 \times 7321\big) = 1.$$

Therefore the required gcd is 480. □

Similar Question: Determine the largest positive integer that divides $p^6 - 1$ for all primes $p > 7$.

(Junior Balkan Maths Olympiad, Shortlist, 2016)

Problem 5. Let $p_1 < p_2 < p_3 < p_4$ and $q_1 < q_2 < q_3 < q_4$ be two sets of prime numbers, such that $p_4 - p_1 = 8$ and $q_4 - q_1 = 8$. Suppose $p_1 > 5$ and $q_1 > 5$. Prove that 30 divides $p_1 - q_1$.

(INMO, 2012)

Solution. Since $p_1, q_1 > 5$, so both p_1 and q_1 are of the form $6k + 1$ or $6k - 1$, for some integer k.

If $p_1 = 6k + 1$, then $p_4 = p_1 + 8 = 6k + 9$ becomes a multiple of 3, which is not possible as p_4 is a prime number. Similarly, q_1 can also not be of the form $6k + 1$.

So, let $p_1 = 6m - 1$ and $q_1 = 6n - 1$, for some integers m and n. Therefore, $p_1 - q_1 = 6(m - n)$. That is $p_1 - q_1$ is a multiple of 6.

If $p_1 = 6m - 1$ is a prime, then the next possible primes are of the form $6m + 1$, $6m + 5$, $6m + 7$, ... But $p_4 = 6m + 7$, so the possible form of p_1, p_2, p_3 and p_4 are $6m - 1$, $6m + 1$, $6m + 5$ and $6m + 7$ respectively. Similarly, the possible form of q_1, q_2, q_3 and q_4 are $6n - 1$, $6n + 1$, $6n + 5$ and $6n + 7$ respectively. So, if $p_1 = x$, then $p_2 = x + 2$, $p_3 = x + 6$ and $p_4 = x + 8$. And so is for the q's.

Now, any prime $p_1 > 5$ can be of the form $5k + 1$, $5k + 2$, $5k + 3$ or $5k + 4$, for some integer k.

If $p_1 = 5k + 2$, then $p_4 = p_1 + 8 = 5k + 10$, a multiple of 5, which is not possible.

If $p_1 = 5k + 3$, then $p_2 = p_1 + 2 = 5k + 5$, a multiple of 5, which is not possible.

If $p_1 = 5k + 4$, then $p_3 = p_1 + 6 = 5k + 10$, a multiple of 5, which is not possible.

But, p_1 may be of the form $5k + 1$, and the same is true for q_1.

Therefore, $p_1 - q_1$ is a multiple of 5.

Hence 30 divides $p_1 - q_1$. □