Number theory problems

November 17, 2019

Numbers a, b, n, k, d below are positive integers, p is prime number.

1. $a^2 + b \vdots b^2 + a$ and $a + b > 2$. Prove that $b^2 + a$ is composite integer.

   Solution.

   - If $a = b$ then condition $a + b > 2$ means $a \geq 2$ and $b^2 + a = (a + 1)a$. Both multipliers are greater than 1, so this number is composite.
   - Otherwise $(a^2 + b) - (b^2 + a) = (a^2 - b^2) - (a - b) = (a - b) \cdot (a + b - 1) \vdots b^2 + a$. Let $x = a + b - 1 < a + b \leq a + b^2 = b^2 + a$ and $y = |a - b| < a + b \leq b^2 + a$. If $b^2 + a$ is prime and $xy \vdots b^2 + a$ then $x \vdots b^2 + a$ or $y \vdots b^2 + a$, but both x and y are less than $b^2 + a$. So $b^2 + a$ is composite.

2. Solve equation: $a(a + 1) = b(b + 2)$.

   Solution. If $a \leq b$ then $a(a+1) < a(a+2) \leq b(b+2)$. Otherwise $a(a+1) > (a-1)((a-1)+2) \geq b(b+2)$. There are no solutions.

3. Prove that there exist 2020 consecutive positive integers such that exactly 19 integers among them are prime numbers.

   Solution. Let $f(n)$ be number of prime numbers between n and $n + 2019$ inclusively. $f(1) > 19$ because 71 is 20-th prime number. $f(2021! + 2) = 0$ because $2021! + k$ is divisible by k for $k = 2 \ldots 2021$. Also note that $|f(n + 1) - f(n)| \leq 1$.

   Let's start with $n = 1$ and increase it repeatedly. Value of the function changes by zero or one, $f(1) > 19$, $f(2021! + 2) < 19$, so there exists n between 1 and $2021! + 2$ such that $f(n) = 19$.

4. Prove that $239^{30} + 30^{239}$ is composite integer.

   Solution. Use Fermat's little theorem: $239^{30} \equiv 1 \pmod{31}$. Also $30^{239} \equiv (-1)^{239} \equiv -1 \pmod{31}$. It means that $239^{30} + 30^{239} \equiv 0 \pmod{31}$. Obviously $239^{30} + 30^{239} > 31$, so this number is composite.

5. $p = 4k + 3$, $a^2 + b^2 \vdots p$. Prove that $b \vdots p$ (Note: use quadratic characters)

   Solution. Assume that b is not divisible by p. Then there exists $c = b^{-1} \pmod{p}$. $c^2 \cdot (a^2 + b^2) \equiv (ac)^2 + (bc)^2 \equiv (ac)^2 + 1 \pmod{p}$ and $-1 \equiv (ac)^2$. Now you can use that (-1) is not quadratic residue modulo $p = 4k + 3$, but let's prove it.

   $1 \equiv (ac)^{p-1} \equiv (ac)^{4k+2} \equiv (ac)^{2^{2k+1}} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$. But if $1 \equiv -1 \pmod{p}$ then $2 \vdots p$, but p is odd prime, it gives us a contradiction.

6. $p > 2$, $2^p - 1 \vdots d$. Prove that $d = 2kp + 1$.

   Solution. Assume that d is prime. $2 \not\equiv 1 \pmod{d}$ and $2^p \equiv 1 \pmod{d}$. p has no proper divisors except for 1, so p is the least number k such that $2^k \equiv 1 \pmod{d}$. Value $k = \phi(n)$ also suits this equation, so $d - 1 = \phi(d) \vdots p$. $2^p - 1$ is odd, so d is also odd, it means that $d \equiv 1 \pmod{2p}$, then there exists k such that $d = 2kp + 1$.

   If d is not prime then d is product of several prime divisors of $2^p - 1$ which equal to 1 modulo $2p$, so d also equals to 1 modulo $2p$.

7. $p = 3k + 2$. Prove that for any a equation $x^3 \equiv a \pmod{p}$ has exactly one solution (Note: use generator modulo p).

   Solution. You can use generator modulo p to easily prove that, but let's do the following. If $x^3 \equiv a \pmod{p}$ then using Fermat's little theorem we get $a^{3k^2} \equiv x^{9k^2} \equiv (x^{3k+1} \cdot x^{-1})^{3k} \equiv x^{-3k} \equiv x^{-3k+3k+1} \equiv x \pmod{p}$. It means that value of x is clearly defined by value of a^{3k^2}.

8. Let $f(n,k) = \#\{d = k \dots n \mid n \vdots d\}$. Find $f(1001,1) + f(1002,2) + \dots + f(2000,1000)$.

   Solution. For $x = 1 \dots 1000$ number x can be used in calculation of $f(1001,1), f(1002,2), \dots f(1000+x,x)$. Exactly one of $\{1001, 1002, \dots, 1000+x\}$ is divisible by x, so every x adds 1 to the required sum.

   Every $y = 1001 \dots 2000$ adds 1 to the sum (in component $f(y, y-1000)$).

   Higher numbers do not add anything, so the answer is 2000.

9. Let $a_1, \dots, a_{10}$ be distinct positive integers. Let $M = \{a_1, \dots, a_{10}, -a_1, \dots, -a_{10}\}$. Prove that there exists nonempty $S \subset M$ such that $\forall i : \{a_i, -a_i\} \not\subset S$ and $\sum\limits_{x \in S} x \vdots 1001$.

   Solution. Let $M' = \{a_1, \dots, a_{10}\}$. Note that there are exactly 1024 subsets of M', so there exist distinct subsets S_1 and S_2 such that $sum(S_1) \equiv sum(S_2) \pmod{1001}$.

   Also $sum(S_1 \setminus S_2) \equiv sum(S_1) - sum(S_1 \cap S_2) \equiv sum(S_2) - sum(S_1 \cap S_2) \equiv sum(S_2 \setminus S_1) \pmod{1001}$. Let $S_1' = S_1 \setminus S_2$ and $S_2' = S_2 \setminus S_1$ then $sum(S_1') \equiv sum(S_2') \pmod{1001}$ and $S_1' \cap S_2' = \emptyset$.

   Let $S = S_1' \cup \{-x | x \in S_2'\}$. Obviously such S suits conditions in the statement.

10. Positive integer n is called Carmichael (or Fermat pseudoprime) number if $\forall a : a^n - a \vdots n$. Prove that n is Carmichael number iff for all prime divisor p of n: $p^2 \nmid n$ and $p - 1 \mid n - 1$.

    Solution.

    - If n is Carmichael number then $p^2 \nmid n$. Assume that $n \vdots p^2$. And if $a = p$ then $a^n - a$ is divisible by p but not divisible by p^2, so $a^n - a$ is not divisible by n.
    - If n is Carmichael number then $p - 1 \mid n - 1$. Let g be generator modulo p and $a = g$. Then $g^n \equiv g \pmod{n}$ and $g^{n-1} \equiv 1 \pmod{p}$. Then $n - 1 \vdots \phi(p) = p - 1$.
    - If $p^2 \nmid n$ and $p - 1 \mid n - 1$ then n is Carmichael number. Let's fix any a and prime divisor p of n. If a is divisible by p then $a^n - a$ is divisible by p, otherwise $a^{n-1} - 1 \equiv a^{p-1}{}^{\frac{n-1}{p-1}} - 1 \equiv 1^{\frac{n-1}{p-1}} - 1 \equiv 0 \pmod{p}$ and $a^n - a$ is divisible by p too.

      For any prime divisor p of n we got that $a^n - a$ is divisible by p. Then $a^n - a$ is divisible by product of all distinct prime divisors of n and if all prime divisors of n are distinct then $a^n - a$ is divisible by n.

11. Prove that for any $n > 1$ number $3^n - 1$ is not divisible by $2^n - 1$.

    Solution.

    - If n is even then $3^n - 1$ is not divisible by 3 and $2^n - 1 = 4^{\frac{n}{2}} - 1$ is divisible by 3, so $3^n - 1$ is not divisible by $2^n - 1$.
    - If n is odd then let's use Jacobi symbols. Assume that $3^n - 1 \vdots 2^n - 1$:

      $$1 = \left(\frac{1}{2^n-1}\right) = \left(\frac{1+(3^n-1)}{2^n-1}\right) = \left(\frac{3^n}{2^n-1}\right) = \left(\frac{3}{2^n-1}\right)^n = \left(\frac{3}{2^n-1}\right)$$

      The last equation is correct since n is odd. Using Gauss quadratic reciprocity for Jacobi symbols we get:

      $$\left(\frac{3}{2^n-1}\right) = \left(\frac{2^n-1}{3}\right) \cdot \left(\frac{3}{2^n-1}\right) = (-1)^{2^{n-1}-1} = -1$$

      So we got a contradiction.

12. (Kummer's lemma). Given a, b and p. Let k_1 be maximum d such that $C_{a+b}^a \vdots p^d$. Let k_2 be number of carryings in process of addition in columns of numbers a and b in numeral system with base p. Prove that $k_1 = k_2$.

    Hint. Prove that both k_1 and k_2 equal to the following:

    $$\sum_{n=1}^{\infty} \left\lfloor \frac{a+b}{p^n} \right\rfloor - \left\lfloor \frac{a}{p^n} \right\rfloor - \left\lfloor \frac{b}{p^n} \right\rfloor$$

13. Someone calculated pairwise gcd of 10 positive integers. Is it possible that 45 resulting values equal to $1, 2, 3, \ldots, 45$?

Solution. How many numbers of initial 10 integers are divisible by 17? Both cases give us a contradiction.

- If at most two of them are divisible by 17 then their gcd equal to 17 (or 34) and gcd 34 (or 17) can't be obtained.
- If at least three of them are divisible by 17 then there are at least three pairs of numbers such that their gcd is divisible by 17, but we have only 17 and 34.

14. You are given a multiset S of 101 integers. It is known that $\forall x \in S$: $\exists S_1, S_2 \subset S$: $|S_1| = |S_2| = 50$, $S_1 \cap S_2 = \varnothing$, $S_1 \cup S_2 \cup \{x\} = S$ and $\sum\limits_{y \in S_1} y = \sum\limits_{z \in S_2} z$. Prove that all numbers in S are equal. (Bonus: try to prove it if S consists of real numbers, not integers)

Solution. Let's call multiset M *good* if M has property from the statement. We are given that S is good. Assume that not all numbers in S are equal. Note the following:

- If we add any positive integer to all the numbers from S then S is still good. After this operation not all numbers in S are equal.
- If we multiply all the numbers from S by the same nonzero multiplier then S is still good. After this operation not all numbers in S are equal.
- For any $x \in S$: $sum(S) = x + sum(S \setminus \{x\}) = x + sum(S_1) + sum(S_2) = x + 2\ sum(S_2) \equiv x \pmod 2$, so the numbers in S have the same parity.

Let's add to the all numbers of S value $1 - min(S)$. Then all the numbers in S are positive integers and $min(S) = 1$. Built a sequence of multisets:

- $S_0 = S$. Note that $min(S_0) = 1$, so all the numbers in S_0 are odd.
- S_k is obtained from S_{k-1} by adding 1 to all the numbers from S_{k-1} and multiplying it by $\frac{1}{2}$. If all the numbers in S_{k-1} are odd then all the numbers from S_k are integers and $min(S_k) = \frac{min(S_{k-1})+1}{2} = \frac{1+1}{2} = 1$, so $min(S_k) = 1$ and all the numbers in S_k are odd.

Let $m_k = max(S_k)$. Note that $m_0 > min(S) = 1$ because not all numbers in S are equal. If $m_{k-1} > min(S_{k-1}) = 1$ then $m_k = \frac{m_{k-1}+1}{2} > \frac{1+1}{2} = 1 = min(S_k)$. Also $m_k = \frac{m_{k-1}+1}{2} < \frac{m_{k-1}+m_{k-1}}{2} = m_{k-1}$, so m_k is strictly decreasing sequence of positive integers greater than 1.

If $n = m_0$ then such sequence can't be larger than $n - 1$ elements, but this sequence is infinite. It gives us a contradiction and all the elements of S are equal.

Bonus hint. One can easily prove the same for multisets of rational numbers: it is enough to multiply all the fractions from multiset by their common denominator to make them integers. After that one can reformulate the *goodness* of multiset by building system of linear equations and noticing the rank of resulting matrix. After that one can use that value of rank does not depend on whether we consider this matrix as matrix with rational entries or as matrix with real entries.

15. Find all n such that $n^2 + 3 \vdots \phi(n)$.

Solution. You can find solution here at the second page.

16. Does there exist a field such that its multiplicative group is isomorphic to its additive group?

Solution. You can find solution here at the first page.