信息与计算科学导论
Number Theory
221502023 沈硕 第三次作业

Problem 24: (Adapted from Problems 777 and 778, [8]) [Difficulty Estimate=1.3] Prove the two propositions below, both of which are about Euler's Totient Function.
(1) (Recall that a perfect square is simply the square of an integer.) There are infinitely many positive integers n such that $n + \phi(n)$ is a perfect square.
(2) For $r \geq 1$, there is no positive integer n such that $\phi(n) = 2 \cdot 7^r$

Proof: (1) Note that $n = 5$ is a valid number.
Consider $n = p^{2k+1}$. If $p + \phi(p) = 2p - 1$ is a perfect square n^2, then $p^{2k+1} + \phi(p^{2k+1}) = p^{2k+1} + p^{2k}(p-1) = (p^k m)^2$ is also a perfect square.
Immediately $5, 5^3, 5^5, \cdots$ is a valid infinite sequence due to $k \in N^+$.
(2) Each n can be denoted by $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, where $p_1, p_2, \cdots, p_m$ are all primes, and $k_1, k_2, \cdots, k_m$ are all positive integers.
Now apply this to $\phi(n) = 2 \cdot 7^r$, we get $p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} = 2 \cdot 7^r$.
Since $r \geq 1$, then we must have $7|n$.
WLOG, let $p_1 = 7$ and $k_1 \geq 2$. Then immediately we see 6 is a factor in the left hand side but not in the right hand side, i,e, $6 \mid \phi(n)$ but $6 \nmid 2 \cdot 7^r$, so there doesn't exist such n.

Problem 25: (Putnam 1997-B5) [Difficulty Estimate=2.2] Prove that for $n \geq 2$, $2^{2^{\cdots^{2}}} (n\ terms) \equiv 2^{2^{\cdots^{2}}} (n-1\ terms)$ (mod n).

Give up.

Problem 26: (ARMO 2000-Grade 10-Day 1-Problem 1) [Difficulty Estimate=0.7] Evaluate

$$\lfloor\frac{2^0}{3}\rfloor+\lfloor\frac{2^1}{3}\rfloor+\lfloor\frac{2^2}{3}\rfloor+\cdots+\lfloor\frac{2^{100}}{3}\rfloor$$

Solution: $2^{2k}\equiv 1(mod\ 3), 2^{2k+1}\equiv 2(mod\ 3)$, where $k\in N$. So the original formula

$$\begin{aligned}&=\tfrac{1}{3}(2^0+2^1+\cdots+2^{100})-\tfrac{1}{3}(51+100)\\&=\tfrac{1}{3}\cdot\tfrac{1-2^{101}}{1-2}-\tfrac{152}{3}\\&=\tfrac{2^{101}-152}{3}\end{aligned}$$

Problem 27: (S. Berlov, ARMO 2014-Grade 11-Day 2-Problem 1) [Difficulty Estimate=2.3] Call a natural number n good if for any natural divisor a of n, we have that a + 1 is also divisor of n + 1. Find all good natural numbers.

Solution: First, notice that 1 and all the prime numbers bigger than 2 are all good numbers.
The next is to show other natural numbers are all not good numbers.
If n is a good number, denote that $n = ab, where a, b \in N^+$. Then
$a + 1 \mid ab + 1 \Rightarrow a + 1 \mid b - 1$.
Similarly we can get $b + 1 \mid a - 1$, so combine these two inequations:
$a + 1 < b - 1\ and\ b + 1 <\ a - 1$ we can immediately draw a contradiction unless a or b is 1.

Problem 28: [Difficulty Estimate=2.5] Write a complete proof for Example 48.

Example 48: (IMO Shortlist 2005-N6) Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that a = b.

Solution: $a^n + n \mid b^n + n \Rightarrow a^n + n \mid b^n - a^n$, so if for some p, s.t. $a^n \equiv -n(mod\ p)$, then $b^n \equiv a^n$ holds.

Assume $a \neq b$, then there exists a prime p, s.t. $p \nmid b - a$.

Then there definitely exist a positive integer k, s.t. $a \equiv k - 1(mod\ p)$.

After fixing k, we can let $n = k(p-1) + 1$. And this is a counterexample.

1. $a^n \equiv a^{k(p-1)+1} \equiv a \equiv k - 1 \equiv -kp + k - 1 \equiv -n(mod\ p)$.
2. $a^n \equiv a, b^n \equiv b(mod\ p)$. Since $p \nmid b - a \Rightarrow b \not\equiv a(mod\ p)$, i,e, $b^n \not\equiv a^n(mod\ p)$, then we draw a contradiction.

So there must be $a = b$.

Problem 29: [Difficulty Estimate=1.7] For what kind of odd primes p, is -3 a quadratic residue mod p? Prove your answer.

Solution: Of course 3 is not a valid odd prime number.

Then we should think of $p = 12k + 1, 12k + 5, 12k + 7, 12k + 11$, which definitely include all odd primes.

Case 1: p = 12k + 1.

$$\{a \mid a \leq \tfrac{p-1}{2}, -3a\ mod\ p > \tfrac{p-1}{2}, a \in Z_p^+\}$$
$$= \{a \mid 1 \leq a \leq 2k\ or\ 4k + 1 \leq a \leq 6k\ or\ 8k + 1 \leq a \leq 10k\}$$

Then this set has 6k elements, and by Gauss Lemma we can get that $-3 \in QR_p$.

And similarly we can deal with the other 3 conditions. The conclution is that $-3 \in QR_p \iff p = 12k + 1\ or\ 12k + 7$.

Problem 30: (adapted from [9]) [Difficulty Estimate=2.5] Suppose $m = 2^a p^b$, where p is an odd prime, and $a \leq 3$ and $b \leq 2$ are integers. What is $\Pi_{r^2 \equiv 1(mod\ m)} r$? Prove your answer.

Give up.

Problem 31: Give up.

Problem 32: [9] [Difficulty Estimate=2.3] Suppose p is an odd prime and $a, b, c \not\equiv 0(mod\ p)$. Prove that the equation $ax^2 + by^2 + cz^2 \equiv 0(mod\ p)$ has at least p solutions $(x, y, z) \in Z_p^3$.

Solution: Recall the Example 57 [12]: For any prime p, any $a \in Z_p^\star$, there exists an integer $b(1 \leq b \leq p-1)$ such that the equation $x^2 + y^2 + a = bp$ has an integer solution.
We can see this Example from a new perspective. That is to say, $\forall a \in Z_p^\star$, a can be displayed as the sum of two quadratic residues.
Even better, we can similarly reach that $\forall a \in Z_p^\star$, a can be displayed as the sum of two quadratic non-residues.
Armed with this powerful conclution, we can deal with the original problem with great ease.
Obviously, x^2 is a quadratic residue. If a is a quadratic residue, then ax^2 is still a quadratic residue. After fixing a, with x traversing all elements in $Z_p^\star$, we can see ax^2 traverse all elements in quadratic residue.
If a is not a quadratic residue, similarly we can get that ax^2 traverse all quadratic non-residues. And this is the same to by^2 and cz^2.
Examine the original equation. There definitely are two elements, which are both quadratic residues or both quadratic non-residues. WLOG, they are ax^2

and by^2, and the equation change to $u + v \equiv w(mod\ p)$. w can traverse quadratic residues or quadratic non-residues, both of which has $(p - 1)/2$ elements. And for each w choosed, by the conclution mentioned before, there must exists a solution (u,v). Since ax^2 and by^2 both can traverse all elements, the solution must can be shown by x, y, i,e, it is valid. And (v,u) is also a valid solution, so now for each w, we have 2 solutions. Summing up them leads to $p - 1$ solutions, while the remaining one is (0,0,0), so there are at least p solutions.

Problem 33: (USA TST 2008, Problem 4) [Difficulty Estimate=3.2] Recall that a perfect square is simply the square of an integer. Prove that, for any integer n, $n^7 + 7$ is not a perfect square. (Hint from [2]: Use Lemma 2.)

Solution: Prove this by contradiction. Assume that $n^7 + 7 = a^2$. Apply mod 4 to each side. $a^2 \equiv 0\ or\ 1\ (mod\ 4)$, $n^7 + 7 \equiv n^7 + 3 \equiv 3\ or\ 0\ or\ 2 (mod\ 4)$, so the only possibility is that $n^7 + 7 \equiv a^2 \equiv 0,\ n \equiv 1,\ a \equiv 0\ or\ 2\ (mod\ 4)$. To draw a contradiction, there must be a form that the left hand side can be factorized, and the right hand side can be show as two perfect square numbers' sum. And that is $n^7 + 2^7 = a^2 + 11^2$, where the left hand side can be displayed as $(n + 2)(n^6 - 2n^5 + 4n^4 - \cdots + 2^6)$.
Use Lemma 2. Since $gcd(a, 11) = 1$, each odd factor of $a^2 + 11^2$ has the form of $4k + 1$. However, $n + 2 \equiv 3,\ n^6 - 2n^5 + 4n^4 - \cdots + 2^6 \equiv 3\ (mod\ 4)$, this is the contradiction. Then $n^7 + 7$ is not a perfect square.

Problem 34: [Difficulty Estimate=1.8] Suppose $\{S_1, S_2\}$ is a partition of $Z_p^\star$, for an odd prime p. For any $x, y \in S_1$, and any $z, u \in S_2$, we always have $xy, zu \in S_1$ and $xz, yu \in S_2$. Prove $S_1 = QR_p$ and $S_2 = QNR_p$.

Solution: We can choose $y = x$, then $x^2 \in S_1$, so S_1 contains all the quadratic residues, and S_2 can only contain quadratic non-residue.
Take $z \in S_2$, then $zk^2 \in S_2$ for all k, so S_2 contains all the quadratic non-residues.
Since all the quadratic residues and quadratic non-residues can form the $Z_p^\star$, we get $S_1 = QR_p$ and $S_2 = QNR_p$.

Problem 35: (Spring 2022, Quiz 3-2) [Difficulty Estimate=2.5] Prove that the equation $4xy - x - y = z^2$ has no solution in positive integers.

Solution: $4xy - x - y = z^2 \;\Rightarrow\; (4x-1)(4y-1) = (2z)^2 + 1$.
Since $gcd(2z, 1) = 1$, so all the odd factors of $(2z)^2 + 1$ has the form of $4k + 1$. But both $4x - 1$ and $4y - 1$ don't have that form, so this equation cannot hold, i,e, it has no solution in positive integers.

Problem 36: (IMO 2020 Shortlist-N2, adpated) [Difficulty Estimate=3.2] Please prove the following two propositions. Feel free to use (1) in the proof of (2).
(1) For any prime p such that $p \equiv 1\ (mod\ 3)$, for any $x \in Z_p^\star$, either x has three cube roots, or it has none.

Give up.
Others give up too.