INTERNATIONAL MATHEMATICS SUMMER CAMP IMSC23

MOCK TEST 4 SOLUTIONS-NUMBER THEORY

Date: Thursday, 29th June 2023 **Time**: 13:10-15:10
Number of problems: 3 **Total points**: 21

Problems & Solutions

Problem 1. Find the number of integers c such that $-2023 \leq c \leq 2023$ and there exists an integer x such that $x^2 + c$ is a multiple of 2^{2023}

Solution. Mod 2^n, an odd number is a quadratic residue if and only if it is $\equiv 1 \pmod 8$. Indeed, note that $(2x+1)^1 \equiv 4x(x+1)+1 \equiv 1 \pmod 8$. Therefore, there are at most 2^{n-3} distinct odd quadratic residues modulo 2^n. On the other hand, I claim that if $0 < x < y < 2^{n-2}$ are odd, then $x^2 \not\equiv 0 \pmod{2^n}$. Indeed, note that $2^n > y^2 - x^2 > 0$, hence $x^2 \not\equiv y^2 \pmod{2^n}$. Therefore, we have at least 2^{n-3} odd quadratic residues modulo 2^n, so there must be exactly 2^{n-3} distinct odd quadratic residues, as desired. Therefore, there are exactly. Obviously, 2^k is a quadratic residue for k even, so we only have to count the number of integers c such that $c = 2^k(8i+1)$, k even, and $-2023 \leq c \leq 2023$. But this is just $506+127+31+8+4 = 676$.□

Marking scheme (additive):

- 4 points for proving that an odd number is quadratic residue modulo 2^n if and only if $n \equiv 1 \pmod 8$.
- 3 points for finalizing.

Problem 2. A positive integer m is perfect if the sum of all its positive divisors, 1 and m inclusive, is equal to $2m$. Determine the positive integers n such that n^n+1 is a perfect number.

Remark: The exam took place on 28.6.2023 . . . 28 and 6 are both perfect numbers :)

Solution. One can easily check that $n = 3$ works. We prove that it's the only solution. We'll define $\sigma(n)$ to be the sum of all divisors of n, and so we want to find n such that $\sigma(n^n + 1) = 2(n^n + 1)$. Note that $\sigma(ab) = \sigma(a)\sigma(b)$ if $\gcd(a, b) = 1$.
Lemma: If n is an even perfect number, then $n = 2^{p-1}(2^p - 1)$, where p is prime.
Proof of lemma: It is easy to prove that if $n = 2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are prime, then n is a perfect number. On the other hand, assume that n is an even perfect number and write $n = 2^i m$, m odd. We have that

$$2^{i+1}m = 2n = \sigma(n) = \sigma(2^i)\sigma(m) = \sigma(m)(2^{i+1} - 1)$$

hence $\sigma(m) = 2^{i+1}m/(2^{i+1}-1)$. Since $\sigma \in \mathbb{N}$, we must have that $2^{i+1}-1|m$. But then $\sigma(m) = m + m/(2^{i+1}-1)$, which are both divisors of m. Therefore, we must have that m is prime and $2^{i+1}-1 = m$. Rewriting, we have that $n = 2^{p-1}(2^p-1), p$ and $2^{p-1}-1$ prime.

Going back to the problem, assume that n is odd. We have that n^n+1 is even, so it must be of the form $2^{p-1}(2^p-1), p$ and $2^{p-1}-1$ prime. Since $n=1$ doesn't yield a solution, we can assume that $n>1$. Therefore,

$$2^{p-1}(2^p-1)n^n + 1 = (n+1)(n^{n-1} - \ldots + 1)$$

Since n is odd, the first factor is even and the second is odd. Note that as $n>1$, we have

$$n^{n-1} - \ldots + 1 \geq n^{n-2}(n-1) + 1 \geq 2n+1$$

On the other hand, we have that $n+1 \geq 2^{p-1}$ and $n^{n-1} - \ldots + 1 \leq 2^p - 1$, hence we must have equality in all the previous equalities, as

$$2^p - 1 \geq n^{n-1} - \ldots + 1 \geq 2n+1 = 2(n+1)-1 \geq 2^p - 1$$

In particular, we must have $n^{n-1} - \ldots + 1 = n^{n-2}(n-1)+1$, hence $n=3$, as desired.

Assume now that n is even, so n^n+1 is odd (note that the existence of odd perfect numbers is still an open conjecture). We will prove that $3|n$. If this is not the case, then $n^n+1 \equiv 2 \pmod 3$. Therefore, $N := n^n+1$ is not a square, hence $d + N/d$ is divisible by 3 for each divisor d of n. In particular, we have that

$$\sigma(N) = \sum_{d|N} d = \sum_{d|N, d<\sqrt{N}} d + \frac{N}{d} \equiv 0 \pmod 3$$

However, we assumed that $N \equiv 2 \pmod 3$, so we get a contradiction. Therefore, we have that $3|n$.

Let $k = n^{n/6}$ and note that

$$n^n + 1 = k^6 + 1 = (k^2+1)(k^4-k^2+1)$$

It is easy to prove that $\gcd(k^2+1, k^4-k^2+1) = 1$, so

$$2(n^n+1) = \sigma(n^n+1) = \sigma(k^2+1)\sigma(k^4-k^2+1)$$

Therefore, $v_2(\sigma(k^2+1)\sigma(k^4-k^2+1)) = v_2(2(n^n+1)) = 1$, so exactly one of k^2+1, k^4-k^2+1 is odd. But $\sigma(x)$ is odd if and only if x is a perfect square. However, k^2-1 is not a perfect square, and neither is k^4-k^2+1, as $(k^2-1)^2 < k^4-k^2+1 < (k^2)^2$. Therefore, n^n+1 is not a perfect number.

Marking scheme (additive):

- 1 point for proving that if n is an even perfect number, then $n = 2^{p-1}(2^p-1), p$ and $2^{p-1}-1$ prime.
- 1 point for proving that if n is odd, then $n=3$.
- 2 points for proving that if n is even, then 3 divides n.
- 3 points for finalizing.
- Ph.D. for proving there aren't any odd perfect numbers (or giving an example)

Problem 3. Let P be the set of all primes, and let M be a non-empty subset of P. Suppose that for any non-empty subset $p_1, p_2, ..., p_k$ of M, all prime factors of $p_1 p_2 ... p_k + 1$ are also in M. Prove that $M = P$

Proof. Assume there is a prime $p \notin M$. Some residues $\pmod p$ occur infinitely often as primes in M, and others only occur finitely often. Take all primes in M equivalent to the latter residues (only finitely many) and put them in a subset $S \in M$. Call a finite subset T of M good if $S \in T$. Denote $P(T)$ as the product of the elements in T.

We create a sequence of good subsets. Take $T_1 = S$, and suppose $P(S) = s$. Let the prime factorization of $s + 1$ be $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Note $p_1, p_2, \dots p_k \in M \setminus S$.

In the prime factorization, replace each $p_i^{a_i}$ with a_i distinct primes in $M \setminus S$ equivalent to $p_i \pmod p$, so the primes replacing $p_i^{a_i}$ and $p_k^{a_k}$ are disjoint for any $i \neq k$. This can be done since there are infinitely many primes in $M \setminus S$ that are $\equiv p_i \pmod p$. Then the product of these primes taken over all $p_i^{a_i}$ is $\equiv s + 1 \pmod p$. If T_2 is the union of these primes and S, then $P(T_2) \equiv s^2 + s \pmod p$.

Extending this process creates a sequence of good subsets $T_1, T_2, T_3 \dots$ with products equivalent to $s, s^2 + s, s^3 + s^2 + s \dots$ modulo p.

Claim. Unless $s \equiv 0 \pmod p$, the sequence $s + 1, s^2 + s + 1, s^3 + s^2 + s + 1, \dots$ must eventually hit $0 \pmod p$.

Proof of the claim. If $s \equiv 1$, then $s^{n-1} + s^{n-2} + \dots + 1 \equiv 0 \pmod p$. Otherwise, see that

$$0 \equiv \frac{s^{p-1} - 1}{s - 1} = s^{p-2} + s^{p-3} + \cdots + 1 \pmod p$$

So eventually we'll get a good subset T where the $P(T) + 1 \equiv 0 \pmod p$, implying $p \in M$, contradiction.

Marking scheme(additive):

- 2 points for fixing $p \notin M$ and considering the set S of residues that appear finitely many in M.
- 3 points for creating the sequence of good subsets.
- 2 points for finalizing.