# $\nu_p$ aka Unique Prime Factorization

MA 5.0

Raymond Feng

March 19, 2021

# Last Time...

## Very Useful NT Lemma

An integer $n$ is a quadratic residue modulo every prime number if and only if $n$ is a perfect square.

## Iran TST 2011/12

Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a function for which the expression $af(a) + bf(b) + 2ab$ for all $a, b \in \mathbb{N}$ is always a perfect square. Prove that $f(a) = a$ for all $a \in \mathbb{N}$.

- $P(a, b)$ is the problem assertion.
- $P(a, p)$ for varying $p$ gives? By above useful lemma this gives us $af(a)$ is a perfect square for all $a$.
- $g(a) := \sqrt{af(a)}$. Problem becomes $g(a)^2 + g(b)^2 + 2ab$ always a square.
- $p \mid g(p) \implies p \leq g(p)$.
- $P(1, p)$ gives $g(p)^2 + 2p + g(1)^2$ is always a square.
- $$4g(p) + 4 > 2p + g(1)^2 \geq 2g(p) + 1 \implies 2p + g(1)^2 = 2g(p) + 1$$

  for large enough $p$.
- By size considerations, we get $g(p) = p$ for all $p \gg g(1)^2$.
- This then forces $g(1) = 1$.
- Easy part of HW: Finish the problem from here.

# Finishing up

- Ideas? (Recall the NT FE mantra :P)
- Goal: for fixed $n$, how can we show that $g(n) = n$?
- Fix $n$. Vary a gigantic prime $p \gg n, g(n)$. Then $p^2 + 2pn + n^2$ is a perfect square, but so is $p^2 + 2pn + g(n)^2$.
- This means that $g(n)^2 - n^2$ is the difference of 2 squares for infinitely many pairs of perfect squares.
- This means that $g(n)^2 = n^2 \implies g(n) = n$, QED.

## ISL 2011/N1

For any integer $d > 0$, let $f(d)$ be the smallest possible integer that has exactly $d$ positive divisors (so for example we have $f(1) = 1, f(5) = 16$, and $f(6) = 12$). Prove that for every integer $k \geq 0$ the number $f\left(2^k\right)$ divides $f\left(2^{k+1}\right)$.

- Regroup at 8:55pm.
- Ideas?
  - Each of $2^1, 3^1, 2^2, 5^1, 7^1, 3^2, \ldots$ gives an extra factor of 2 in number of factors.
- Consider the set $S = \left\{2^1, 2^2, 2^4, 2^8, \ldots\right\} \cup \left\{3^1, 3^2, 3^4, 3^8, \ldots\right\} \cup \left\{5^1, 5^2, 5^4, 5^8, \ldots\right\} \cup \ldots.$
- Valid numbers which have $2^k$ factors must necessarily be the product of some of the smallest elements in each set.
- $f(2^k)$ is just the product of the $k$ smallest elements in $S$.
- Finishes because $k$ smallest elements are a subset of the set of $k+1$ smallest elements.

# IMO 2010/3

## IMO 2010/3

Find all functions $g : \mathbb{N} \to \mathbb{N}$ such that

$$(g(m) + n)(g(n) + m)$$

is a perfect square for all $m, n \in \mathbb{N}$.

- Regroup at 9:10pm.
- Conjectured solution set: $g(x) = x + c$ for $c \geq 0$.
- Ideas?
  - mod $p$?
  - $g(pa)g(pb)$ is a QR mod $p$.
- **Hint:** Try proving that $p \mid g(a) - g(b) \implies p \mid a - b$.
- $g(a) + m$ and $g(b) + m$ are congruent mod $p$ (here assume that $p > 2$ for now). So we can ensure that $p \mid g(a) + m, g(b) + m$ but $p^2 \nmid g(a) + m, g(b) + m$ by choosing a specific $m$.
- Suppose the difference $g(a) - g(b) = xp$. Then we can always find 2 nonzero residues mod $p$ that differ by $x$ (only fails if $p = 2$ and $x$ is odd).
- Now we have $p \mid g(m) + a, g(m) + b$ which implies the desired.

# Continued

- $p = 2$ case: If $g(a) \equiv g(b) \pmod 4$ then we can find $m$ so that $g(a) + m \equiv g(b) + m \equiv 2 \pmod 4$.
- If $g(a) \equiv g(b) + 2 \pmod 4$: $m = 2^{2k+1} - g(a)$ (for some integer $k \geq 1$).
  - Then $m + g(b) = 2^{2k+1} - g(a) + g(b) \equiv 2 \pmod 4$.
  - This gives $\nu_2(g(a) + m), \nu_2(g(b) + m)$ are both odd. :)
- **Corollaries:**
  - Injectivity!
  - $g(n+1) = g(n) \pm 1$.
- We actually always have $g(n+1) = g(n) + 1$ by injectivity and the fact that the range is the natural numbers. QED.

# Iran TST 2013/1/5

## Iran TST 2013/1/5

Do there exist natural numbers $a, b$ and $c$ such that $a^2 + b^2 + c^2$ is divisible by $2013(ab + bc + ca)$?

- Regroup at 9:50pm.
- Ideas?
  - Write as
  $$(a + b + c)^2 = (2013k + 2)(ab + bc + ca).$$
  - Can also assume WLOG that $\gcd(a, b, c) = 1$.
- Exists some $p \equiv 2 \pmod 3$ with $\nu_p(2013k + 2)$ odd.
- This gives us that $p | a + b + c, ab + bc + ca$.
- Then $c \equiv -a - b \pmod p \implies ab + b(-a - b) + (-a - b)a = -a^2 - ab - b^2 \equiv 0 \pmod p$.
- $a^3 \equiv b^3 \pmod p$ which means $a \equiv b \pmod p$ (using the fact that $3 \nmid p - 1$).
- We finally get $p \mid a, b$, contradiction.

# TST 2021/1

**TST 2021/1**

Determine all integers $s \geq 4$ for which there exist positive integers $a$, $b$, $c$, $d$ such that $s = a + b + c + d$ and $s$ divides $abc + abd + acd + bcd$.

- $a + b + c + d \mid abc + abd + acd + bcd$. Suppose $p$ be a prime factor of $a + b + c + d$.
- $$p \mid abc + (ab + bc + ca)(-a - b - c) = -(a + b)(b + c)(c + a)$$
- Generalizing, we have
$$s \mid (a + b)(b + c)(c + a).$$
- If $s$ is prime, die by size.
- If $s = mn$ $(m, n > 1)$ is composite, $a = 1, b = m - 1, c = n - 1, d = (m - 1)(n - 1)$.

## USAMO 1985/1

Determine whether or not there are any positive integral solutions of the simultaneous equations

$$x_1^2 + x_2^2 + \cdots + x_{1985}^2 = y^3,$$

$$x_1^3 + x_2^3 + \cdots + x_{1985}^3 = z^2$$

with distinct integers $x_1, x_2, \ldots, x_{1985}$.

- Think the answer is no (3 to 1 vote).
- Answer is actually yes!
- **Key Idea:** Both equations nonhomogeneous. Therefore, we can plug in *random* things for the $x_i$ and then scale all $x$'s to assert some control over $y, z$.
- Suppose we have $N = 1^2 + 2^2 + 3^2 + 4^2 + \ldots + 1985^2, M = 1^3 + 2^3 + \ldots + 1985^3$.
- Want $k^2N$ is a cube and and $k^3M$ is a square.
- For each prime $p$, we can use CRT to generate an exponent $e$ so that $3 \mid \nu_p(k^2N) = \nu_p(N) + 2e, 2 \mid \nu_p(k^3M) = \nu_p(M) + 3e$.