UBC MATH CIRCLE 2024 PROBLEM SET 9 SOLUTION

Problem 1. *Prove that the equation $x^2 - 5y^2 = 1$ has infinitely many solutions in integers.*

Solution. Note that $(9, 4)$ is a solution to the equation above. Consider the subset $\mathbb{Z}[\sqrt{5}] \subset \mathbb{R}$ given by elements of the form $x + y\sqrt{5}$ with $x, y \in \mathbb{Z}$. Define a function $N : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}$ given by $N(x+y\sqrt{5}) = (x+y\sqrt{5})(x-y\sqrt{5}) = x^2 - 5y^2$. The definition immediately implies that if $r, s \in \mathbb{Z}[\sqrt{5}]$, then $N(rs) = N(r)N(s)$. In other words, for any $k \in \mathbb{N}$,

$$N((9 + 4\sqrt{5})^k) = 1$$

Thus if we write $x_k + y_k\sqrt{5} = (9 + 4\sqrt{5})^k$, we find that (x_k, y_k) is also a solution to the equation above. Note finally that if $x, y > 0$ then $(x + y\sqrt{5})^2 = x^2 + 5y^2 + 2xy\sqrt{5}$ and $x^2 + 5y^2 > x$. Thus the sequence $\{(x_k, y_k)\}_{k\in\mathbb{N}}$ contains infinitely many distinct elements. In other words $x^2 - 5y^2 = 1$ has infinitely many solutions in integers.

Problem 2. *Let P be a polynomial with integer coefficients such that $n \mid P(2^n)$ for every positive integer n. Prove that $P \equiv 0$.*

Solution. Let p and q be two odd primes. Note that $pq \mid P(2^{pq})$ implies that $P(2^{pq}) \equiv 0 \mod p$ for any prime q. By Fermat's little theorem, $2^{pq} \equiv (2^q)^p \equiv 2^q \mod p$. Hence

$$0 \equiv P(2^{pq}) \equiv P(2^q) \mod p$$

Thus $p \mid P(2^q)$ for all odd primes p, q. Taking p sufficiently large implies that $P(2^q) = 0$ for all odd primes q. Thus $P(x)$ has infinitely many roots and $P \equiv 0$.

Problem 3. *A set X consisting of n positive integers is called* good *if the following condition holds:*

($*$) *For any two distinct subsets $A, B \subset X$, the number $\sum_{a\in A} a - \sum_{b\in B} b$ is not divisible by 2^n.*

Given $n \in \mathbb{N}$, find the number of good sets of size n, all of whose elements are strictly less than 2^n.

Solution. Given a nonzero integer n, write $n = 2^k m$ where $\gcd(2, m) = 1$. Denote by $\nu_2(n) = k$. We claim that for any $n > 0$, the good sets are exactly sets $S = \{m_0, \dots, m_{n-1}\}$ such that $\nu_2(m_i) = i$. Indeed, if $A, B \subset S$ are distinct, then by properties $\nu_2(-)$ (namely the fact that if $\nu_2(a) \neq \nu_2(b)$ then $\nu_2(a + b) = \min\{\nu_2(a), \nu_2(b)\}$), we see that

$$\nu_2\left(\sum_{a\in A} a - \sum_{b\in B} b\right) = \min\{\nu_2(x) : x \in A \cup B\} \leq \nu_2(m_{n-1}) = n - 1$$

In particular, any set of this form is good. Conversely, call a set X n-good if it satisfies ($*$), even if it doesn't necessarily have n elements. we show by induction that any n-good set of size n must be of this form, and that there are no n-good sets of size $n + 1$. If $n = 1$, then evidently $S = \{x\}$ is a good set if and only if x is odd, i.e. $\nu_2(x) = 0$ and there are no good sets S of size 2. Now suppose that we have shown the result for $n = m - 1$. Let S

Date: April 19, 2024.

be a m-good set. If every element of S is even, then let $T = \{x/2 : x \in S\}$. Then T is a $m-1$-good set for of size m, which is a contradiction. Thus S contains an odd number r. Consider the collection $E = \{\sum_{a\in A} a : A \subset S\}$. Note that $|E| = 2^n$ and that by assumption, all of the remainders $\mod 2^n$ of elements of E are distinct. Hence we conclude that E forms a complete set of residues $\mod 2^n$. Let $F = \{\sum_{a\in A} : r \notin A \subset S\}$. By the earlier remark, the sets $\{\{f, f+r\} : f \in F\}$ partitions the set of residues $\mod 2^n$. But this implies that every element $f \in F$ must be even. Thus every element of $T = S \setminus \{r\}$ is even. In particular, $R = \{x/2 : x \in T\}$ is an $m-1$-good set of size $|S| - 1$. If $|S| - 1 = m - 1$, then we conclude by the induction hypothesis that every element of R has a different 2-adic valuation. If $|S| - 1 > m - 1$, then the induction hypothesis gives a contradiction.

Finally, note that the set of elements $m < 2^n$ such that $\nu_2(m) = k$ is precisely 2^{n-k-1}. Thus the number of good sets of size n all of whose elements are strictly less than 2^n is

$$\prod_{k=0}^{n-1} 2^{n-k-1} = \prod_{k=0}^{n-1} 2^k = 2^{n(n-1)/2} = 2^{\binom{n}{2}}$$