2019 SDHMC Part II #4

Tristan Shin

20 Apr 2019

Let $\{a_1, a_2, \ldots, a_n\}$ and $\{b_1, b_2, \ldots, b_n\}$ be distinct sets of positive integers. Assume that any integer m can be written as $a_i + a_j$ with $1 \le i < j \le n$ in exactly as many ways as it can be written as $b_i + b_j$ with $1 \le i < j \le n$. Show that n is a power of 2.

Define the polynomials $A(x) = \sum_{i=1}^{n} x^{a_i}$ and $B(x) = \sum_{i=1}^{n} x^{b_i}$. Write

$$A(x)^2 = \sum_{i=1}^{n} x^{a_i} \sum_{j=1}^{n} x^{a_j} = \sum_{1 \le i,j \le n} x^{a_i + a_j}.$$

This sum adds $x^{a_i+a_j}$ twice for each $1 \le i < j \le n$ and x^{2a_i} once for each $1 \le i \le n$. Since $\sum_{i=1}^{n} x^{2a_i} = A(x^2)$, we have that $\frac{A(x)^2 - A(x^2)}{2}$ is the sum of $x^{a_i+a_j}$ over $1 \le i < j \le n$. By the problem statement, this is the sum of $x^{b_i+b_j}$ over $1 \le i < j \le n$. But by symmetry, this sum is $\frac{B(x)^2 - B(x^2)}{2}$, so

$$A(x)^2 - A(x^2) = B(x)^2 - B(x^2)$$

as a polynomial identity. Rearrange this to

$$(A(x) - B(x))\,(A(x) + B(x)) = A(x^2) - B(x^2).$$

Now, let $A(x) - B(x) = P(x)(x-1)^k$ for a non-negative integer k and polynomial P where $x - 1$ does not divide P. This is possible because $A(x) - B(x)$ is not the zero polynomial (else the two sets are the same), so by the factor theorem we can repeatedly factor out $x-1$ from $A(x)-B(x)$ until we cannot any more. Then by the factor theorem, $P(1) \ne 0$. First note that $A(1) = B(1) = n$, so $k \ge 1$. Now, we have

$$P(x)(x-1)^k\,(A(x) + B(x)) = P(x^2)(x^2-1)^k = P(x^2)(x+1)^k(x-1)^k.$$

Since this is a polynomial identity, we can divide by $(x-1)^k$ to get

$$P(x)\,(A(x) + B(x)) = P(x^2)(x+1)^k.$$

Plug in $x = 1$ to get

$$P(1)\,(A(1) + B(1)) = P(1)2^k.$$

Since $P(1) \ne 0$ and $A(1) = B(1) = n$, we deduce that $n = 2^{k-1}$, a power of 2. ■

Remark. In fact, we can construct sets that work when n is a power of 2. First, when $n = 2$ we have that $\{1, 4\}$ and $\{2, 3\}$ work. Now, suppose A_k and B_k work when $n = 2^k$. Consider the sets

$$A_{k+1} = A_k \cup \{b + 2^{k+1} \mid b \in B_k\}$$
$$B_{k+1} = B_k \cup \{a + 2^{k+1} \mid a \in A_k\}$$

defined recursively. One can verify the polynomial identity inductively to show that this works.