On the differences of elements in a finite set

Othman SLASSI

January 2, 2018

In this article we well state some elementary results in combinatorics and we will discuss some applications as well as some genaralisations.

1 A classical example

Considere a subset X of $\{1, 2, \ldots, 2018\}$ with 1100 elements, then we can always find two integers in X with difference equal to 181.

Proof

Considere the set $Y = X \cup (X + 181)$
where $(X + 181) := \{x + 181 \mid x \in X\}$, $\textbf{card}(Y) \leq 2.1100 = 2200$ (*)
with equality if and only if $X \cap (X + 181) = \emptyset$
we also have $Y \subseteq \{1, 2, \ldots, 2018 + 181\} = \{1, 2, \ldots, 2199\}$
so equality in (*) cannot hold witch means
$\exists x \in X \cap (X + 181) \Rightarrow \exists x, y \in X, x = y + 181$ □

Using exactly the same method we can proof this more general result:

T1: **Let $2 \leq n \leq m$ and p be three integers such that $2n \geq m+p+1$ and X a subset of $\{1, 2, \ldots, m\}$ of cardinality n. Then p can be expressed as the difference of two integers in X.**

Many olympiad problems are variants of this result or require the same kind of methods, we will see an other example wich cannot be solved using the direct approach.

2 Same kind of problem, different approach

Here is an other problem, you can try to solve it the same way as above, you will find out that it's simply can't be done:

$a \in \{152, 133\}$ ***and*** X ***is a set of*** 1065 ***integers are chosen randomly between*** 1 ***and*** 2018 ***proof that there exist two integers in*** X ***with difference equal to*** a***.***

The general result discussed in section 1 states a pretty strong assumtion on the number p. Here I will state an other result in which the assumptions on p seem to vanish, in some cases this result is much stronger than T1.

T2: Let n and m be two integers strictly greater than 1 such that $\lfloor \frac{m-1}{n-1} \rfloor = 1$ and X a subset of $\{1, 2, \ldots, m\}$ of cardinality n. Then every divisor of $n-1$ can be expressed as the difference of two integers in X.

Proof
Considere p a divisor of $n-1$, we can write $n = kp + 1$ where k is a positive integer.
According to the pigeonhole principle there is a least $\lceil \frac{n}{p} \rceil = k + 1$ integers in X witch have the same residue r modulo p.
Denote $pq_1 + r < pq_2 + r < \ldots < pq_{k+1} + r$ those elements.
Let $\delta = \min\limits_{1 \leq i \leq k} (q_{i+1} - q_i)$.
We have:
$k\delta \leq \sum\limits_{i=1}^{k} (q_{i+1} - q_i) = q_{k+1} - q_1 = \frac{1}{p}((pq_{k+1} + r) - (pq_1 + r)) \leq \frac{1}{p}(m-1)$.
Wich means: $\delta \leq \frac{1}{kp}(m-1) = \frac{m-1}{n-1}$ hence $\delta \leq \lfloor \frac{m-1}{n-1} \rfloor = 1$ but δ is a positive integer so $\delta = 1 \Rightarrow \exists l \in \{1, 2, \ldots, k\}; 1 = q_{l+1} - q_l$.
Now considere the numbers $a = pq_{l+1} + r$ and $b = pq_l + r$.
We have clearly $a - b = p$. $\square$

3 Quadratic residues

$p \geq 5$ is a prime number, Q_p the set of quadratic residues mod p in $\{1, 2, \ldots, p\}$ we will proof the following result: **Any divisor d of $\frac{p-1}{2}$ can be represented ans the difference of two elements of Q_p.**

Proof

We write $kd = \frac{p-1}{2}$ then $\mathbf{card}(Q_p) = kd+1$ so there is a least $\lceil \frac{p}{d} \rceil = k+1$ integers in Q_p witch have the same residue r modulo d.
Denote $x_1 < x_2 < \ldots < x_{k+1}$ those elements.
Where $\forall i \in \{1, \ldots, k+1\} : x_i = dq_i + r$ and let $\delta = \min\limits_{1 \le i \le k} (q_{i+1} - q_i)$.
We have:
$k\delta \le \sum\limits_{i=1}^{k} (q_{i+1} - q_i) = q_{k+1} - q_1 = \frac{1}{d}(x_{k+1} - x_1) \le \frac{p-1}{d} = 2k$ (*).
So $\delta = 1$ or $= 2$
Case 1: $\delta = 2$
All inequalities in (*) are equalities witch means that:
$\forall i \in \{1, \ldots, k+1\} : q_i = q_1 + 2(i-1)$
$\Rightarrow \forall i \in \{1, \ldots, k+1\} : x_i = 1 + 2d(i-1)$
Now we considere the sequence $(y_i)_{i \in \mathbb{N}}$ in $\mathbb{Z}_p$ such that :
$\forall i \in \mathbb{N} : y_i = \overline{1 + id}$
$(z_i)_{i \in \mathbb{N}} = (y_{2i})_{i \in \mathbb{N}}$ is a $k-$periodic sequence, more over by the Fermat's Little Theoreme we have: $y_{2^{p-1}} = \overline{1+d} = z_{2^{p-2}}$.
Since all the elements of $(z_i)_{i \in \mathbb{N}}$ are quadratic residues $1+d$ is quadratic residue, but we have also $1+2d$ is quadratic residue, so we've done.
Case 2: $\delta = 1$
In this case $\exists i_0 \in \{1, 2, \ldots, k\} : q_{i_0+1} - q_{i_0} = 1$
Then $x_{i_0+1} - x_{i_0} = d$. $\square$