Inlämningsuppgift 3 : Lösningar

2. Let's think modulo 7. If $a \in \mathbf{Z}$ is not a multiple of 7 then, by Fermat's theorem, $a^6 \equiv 1 \pmod 7$. If a IS a multiple of 7, then obviously $a^6 \equiv 0 \pmod 7$. Hence, the sixth power of an integer is always congruent to either 0 or 1, modulo 7. Let's now check all the possibilities, modulo 7, for the given polynomial expression :

$x^6 \pmod 7$	$y^6 \pmod 7$	$z^6 \pmod 7$	$x^6 + y^6 - z^6 \pmod 7$
0	0	0	0
0	0	1	6
1	0	0	1
1	0	1	0
0	1	0	1
0	1	1	0
1	1	0	2
1	1	1	1

Hence we see that, for any choice of x, y and z, the quantity $x^6 + y^6 - z^6$ is always congruent to 0,1,2 or 6 (modulo 7). So this quantity can only attain values in four of the seven congruence classes mod 7, and the desired result follows immediately.

3 (i) Modulo 13 we have

$$(\pm 1)^2 \equiv 1, \quad (\pm 2)^2 \equiv 4, \quad (\pm 3)^2 \equiv 9, \quad (\pm 4)^2 \equiv 3, \quad (\pm 5)^2 \equiv 12, \quad (\pm 6)^2 \equiv 10,$$

so that $\mathcal{R}_{13} = \{1, 3, 4, 9, 10, 12\}$. Similarly, modulo 17,

$$\begin{gathered}(\pm 1)^2 \equiv 1, \quad (\pm 2)^2 \equiv 4, \quad (\pm 3)^2 \equiv 9, \quad (\pm 4)^2 \equiv 16, \\ (\pm 5)^2 \equiv 8, \quad (\pm 6)^2 \equiv 2, \quad (\pm 7)^2 \equiv 15, \quad (\pm 8)^2 \equiv 13,\end{gathered}$$

so that $\mathcal{R}_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\}$.

(ii) $\Leftarrow$ is trivial.
$\Rightarrow$ Suppose $x^2 \equiv y^2 \pmod p$. Then p divides $x^2 - y^2$, in other words p divides $(x-y)(x+y)$. But, since p is prime, this implies that either p divides $x - y$ or p divides $x + y$. The former means that $x \equiv y \pmod p$, the latter that $x \equiv -y \pmod p$. This proves the claim.

It follows from the $\Rightarrow$ direction of the claim that, for odd p, all of the numbers $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ are mutually incongruent modulo p, hence that $|\mathcal{R}_p| \geq \frac{p-1}{2}$. But the reverse inequality is a consequence of the $\Leftarrow$ direction.

(iii) By part **(ii)** we have that

$$\sum_{x \in \mathcal{R}_p} x \equiv \sum_{k=1}^{\frac{p-1}{2}} k^2 \pmod{p}.$$

Recall the formula for the sum of the first n integer squares (which I assume you've seen before)

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Hence, taking $n = \frac{p-1}{2}$ we find that

$$\sum_{x \in \mathcal{R}_p} x \equiv \frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}\right)p}{6} = p\left[\frac{p^2-1}{24}\right] \pmod{p}.$$

But since $p > 3$ it does not appear in the denominator of the right-hand side, hence the right-hand side is a multiple of p, since p is prime, as desired.