ASO Number Theory question. Solution

(a) -3 is a quadratic residue modulo 2 and 3, so suppose $p \geqslant 5$. We have $(-3|p) = (-1|p)(3|p)$. Suppose $p \equiv 1 \mod 4$. Then $(-1|p) = 1$, and $(3|p) = (p|3)$ by quadratic reciprocity, and this is 1 iff $p \equiv 1 \mod 3$. If $p \equiv 3 \mod 4$ then $(-1|p) = -1$, and $(3|p) = -(p|3)$. This is -1 iff $p \equiv 1 \mod 3$. Thus in either case the condition is that $p \equiv 1 \mod 3$. **[B/S, 5 Marks]**

(b) Set $p = 673$. We have $x^3 - 1 = (x-1)(x^2+x+1)$. Thus we have the solution $x = 1$, and any other solutions must satisfy $x^2 + x + 1 \equiv 0 \mod p$. This may be rewritten as as $(2x+1)^2 \equiv -3 \mod p$. Since $p \equiv 1 \mod 3$, the equation $y^2 \equiv -3 \mod p$ has two solutions, and since p is odd we may then solve $y \equiv 2x + 1 \mod p$ for both of these solutions. **[S, 4 Marks]**

(c) The map $\pi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ given by $\pi(x) = x^3$ is a homomorphism whose image is H. Thus H is a subgroup. Its index is the size of $\ker \pi$ which, by part (b), is 3. **[B/S, 3 Marks]**

Parts (b) and (c) can also be done using primitive roots, and this is allowed, provided it is done carefully.

(d) $2H := (H+H) \setminus \{0\} \subset \mathbb{Z}/673\mathbb{Z}$ is a union of cosets of H, since if $a \in 2H$ is a sum $u^3 + v^3$ and if $x = y^3 \in H$ then $ax = (uy)^3 + (vy)^3$. We claim that $2H$ *strictly* contains H. If not then H is invariant under the map $x \mapsto x + 1$, provided $x \neq -1$. Starting with $x = 1$ and applying this map repeatedly, we obtain $H = (\mathbb{Z}/673\mathbb{Z})^*$, contrary to what we showed above. By an almost identical argument, $3H$ strictly contains $2H$. But $H, 2H, 3H$ are unions of cosets of H, which has index 3, and so $3H$ must be the whole group $(\mathbb{Z}/673\mathbb{Z})^*$. **[N, 6 Marks]**

(e) Observe that $2019 = 3 \times 673$. It is obvious that every integer is a sum of three cubes $\mod 3$. The result then follows from the Chinese remainder theorem and (d). **[S, 3 Marks]**

(f) No, this is not true. If $x = 3k + r$ then

$$(3k+r)^3 = 27k^3 + 27rk^2 + 9r^2k + r^3 \equiv r^3 \mod 9,$$

so all cubes are 0 or $\pm 1 \mod 9$. Clearly if $N \equiv \pm 4 \mod 9$ then it is not the sum of three cubes (this could also be done by a case analysis). **[S, 4 Marks]**