Throughout this article we denote by $H = \langle -1, 2\rangle$ the subgroup generated by -1 and 2 in $\mathbb{F}_p^\times$ and set

$$\ell_0 = [\mathbb{F}_p^\times : H]$$

for the index of H in $\mathbb{F}_p^\times$. Notice that if $4 \nmid o_p(2)$ then by definition we have that $\mathscr{O}(p) = \ell_0$. Furthermore, Conjecture A is a non-empty statement if and only if $\mathscr{O}(p) = \ell_0 \geq 3$.

The idea behind Conjecture A is the following. Suppose that Conjecture A holds, then each triple (a_i, b_i, c_i) in the conjecture corresponds to a nonequi-difference codeword $\mathbf{x_i} = \{0, a_i, -c_i\}$ with difference set $\Delta(\mathbf{x_i}) = \{\pm a_i, \pm b_i, \pm c_i\}$. Hence, we have $\left\lfloor \frac{\mathscr{O}(p)}{3} \right\rfloor$ nonequi-difference codewords whose difference sets are disjoint. From the complement of $\cup_{i=1}\Delta(\mathbf{x_i})$ in $\mathbb{F}_p^\times$, their algorithm then produces $\frac{p-1-2\mathscr{O}(p)}{4}$ equi-difference codewords and hence gives a CAC of size matching the upper bound given in (1).

As an illustration, we briefly discuss the case treated in [FLS14, Example 3] where the length $p = 31$. Note that $o_{31}(2) = 5$ and hence $\mathscr{O}(31) = 3$. Then Conjecture A predicts that there are $3\left\lfloor \frac{\mathscr{O}(31)}{3} \right\rfloor = 3$ cosets and one element in each coset such that their sum is zero. One finds that the triple $(2, 3, -5)$ gives a solution and the corresponding codeword is $\{0, 2, 5\}$ whose difference set is just $\{\pm 2, \pm 3, \pm 5\}$ while 2, 3 and -5 lie exactly in three distinct cosets of H in $\mathbb{F}_p^\times$. Moreover, there are six equi-difference codewords $\{0, 4, 8\}$, $\{0, 6, 12\}$, $\{0, 7, 14\}$, $\{0, 9, 18\}$, $\{0, 10, 20\}$ and $\{0, 15, 30\}$ produced by their algorithm. In total, one concludes that the size of an optimal CAC of length 31 is $M(31) = 7$.

Independently, in [MZS14] the authors proposed a conjecture which provides solutions to the existence of the triples (A_i, B_i, C_i) in Conjecture A in terms of the group structure of $\mathbb{F}_p^\times / H$.

Conjecture B ([MZS14, Conjecture]). Let p be an odd prime. If $\ell_0 \geq 3$, then there exist $b \in gH$ and $c \in g^2H$ such that

$$1 + b + c = 0 \quad \text{in } \mathbb{F}_p$$

for some generator g of $\mathbb{F}_p^\times$.

Remark 1.1. We see that Conjecture B implies Conjecture A by setting $A_1 = H$, $B_1 = gH$, $C_1 = g^2H$, $A_2 = g^3H$, $B_2 = g^4H$, $C_2 = g^5H, \ldots, A_e = g^{3e-3}H$, $B_e = g^{3e-2}H$ and $C_e = g^{3e-1}H$ where $e = \left\lfloor \frac{\ell_0}{3} \right\rfloor$. Moreover, Conjecture B does not assume that $4 \nmid o_p(2)$.

Note that the subgroup $H = \langle -1, 2\rangle$ consists of all the ℓ_0-th power of elements of $\mathbb{F}_p^\times$. It follows that the elements b and c in Conjecture B are of the forms gy^{ℓ_0} and $g^2x^{\ell_0}$ respectively for some $x, y \in \mathbb{F}_p^\times$. Observe that if $\ell_0 \geq 3$ then any $\mathbb{F}_p$-rational solutions (x, y) to the the *diagonal equation* $g^2X^{\ell_0} + gY^{\ell_0} + 1 = 0$ must satisfy $xy \neq 0$ since $-1 \in H$ and g is a generator of $\mathbb{F}_p^\times$. Thus, any $\mathbb{F}_p$-rational solution gives a pair of elements b and c in Conjecture B. So Conjecture B is equivalent to the following statement.