1 a) For example, let $q = 2n$,

$A = B = \{0, 2, 4, \dots, 2n-2\}$

Then $|A| = |B| = |A+B| = n$

$\min(q, |A|+|B|-1) = 2n-1$

(any other subgroups of $\mathbb{Z}/q\mathbb{Z}$ would work)

b) Assume wlog $B = B^* \cup \{0\}$.

(since $A + (B^* \cup \{0\}) \subset A+B$).

Follow outlines of proof of CΔ Thm.

Do induction on $|B|$.

$|B| = 1$ can be easily checked.

Can assume $2 \leq |A| \leq p-2$.

Let $\mathrm{Stab}(A) = \{g \in \mathbb{Z}/q\mathbb{Z} : g + A = A\}$.

So $\mathrm{Stab}(A) < (\mathbb{Z}/q\mathbb{Z})$, $|\mathrm{Stab}(A)| < q$.

Then we have that $\mathrm{Stab}(A) \cap B = \{0\}$.

(otherwise, for all $b \in B \setminus \{0\}$, since $(b, q) = 1$,

we have that $\mathbb{Z}/q\mathbb{Z} = \langle b \rangle < \mathrm{Stab}(A)$,

contradiction.)

Rest of proof follows the same as CΔ. $\square$

2 We follow the same steps as the polynomial method proof of CΔ.

We first show that if $|A|+|B|-3 \geq p$,
then $C=\{a+b \mid a\in A, b\in B, ab\neq 1\}=\mathbb{Z}/p\mathbb{Z}$.

Let $n\in \mathbb{Z}/p\mathbb{Z}$. Then
$$|(n-A)\cap B| = |(n-A)|+|B|-|(n-A)\cup B|$$
$$\geq 3.$$
So there exists distinct $a_1, a_2, a_3 \in A$
such that $b_1, b_2, b_3 \in B$
$$a_1+b_1 = a_2+b_2 = a_3+b_3 = n.$$
Note that if $a+b=n$ and $ab=1$, then a, b are solutions of the polynomial $X^2-nX+1\in\mathbb{F}_p[X]$, which has at most 2 solutions (since $\mathbb{F}_p$ field).
So there exists $i\in\{1,2,3\}$ s.t. $a_ib_i\neq 1$, so $n\in C$. ✓

Now assume $|A|+|B|-3<p$ and assume for contradiction $|C|\leq |A|+|B|-4$.
Let $m=|A|+|B|-4-|C|$, set
$$P(X,Y) = (X+Y)^m (XY-1)\prod_{c\in C}(X+Y-c).$$
This polynomial has degree $|A|+|B|-2$ and $P(a,b)=0$, $\forall (a,b)\in A\times B$.
The coefficient of $X^{|A|-2}Y^{|B|-2}$ is $\binom{|A|+|B|-4}{|A|-2}\not\equiv 0 \pmod p$.

Contradiction follows as in the course. $\square$

③ a) Squares are $\equiv 0, 1 \pmod 4$, so if $p \equiv 3 (4)$, then p cannot be sum of two squares.

b) If $p \equiv 1 \pmod 4$, note that -1 is a square modulo p.

(there are many ways to see this, for example from Euler criterion $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv \left((-1)^{\frac{p-1}{4}}\right)^2 \equiv 1 \ (p)$.

Also, since $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclic, $\exists g$ s.t. $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$ and $-1 = g^{\frac{p-1}{2}} = \left(g^{\frac{p-1}{4}}\right)^2$).

In particular, $\exists\, 0 < x < p$ s.t. $x^2 + 1 \equiv 0 \pmod p$.

So $x^2 + 1 = mp$, with $0 < m < p$.

Let $m > 0$ be minimal with property that $mp = x^2 + y^2$.

c) Suppose $m > 1$. Since $\exists x, y$ such that $x^2 + y^2 = mp$, pick a, b with $|a|, |b| \leq \frac{m}{2}$ such that

$x \equiv a \pmod m$, $y \equiv b \pmod m$.

Note that x & y are NOT both multiples of m (by assumption of $m > 1$ and minimality of m).

Then $x^2 + y^2 \equiv a^2 + b^2 \equiv 0 \pmod m$,

so $a^2 + b^2 = rm$.

Also $a^2+b^2 \le \frac{m^2}{2}$, so $0 < r \le \frac{m}{2}$.

d) Note that $xa+yb \equiv a^2+b^2 \equiv 0 \pmod{m}$

$xb-ya \equiv ab-ab \equiv 0 \pmod{m}$

so $x' = \frac{xa+yb}{m} \in \mathbb{Z}$, $y' = \frac{xb-ya}{m} \in \mathbb{Z}$.

$$rm^2p = (x^2+y^2)(a^2+b^2) = (xa+yb)^2 + (xb-ya)^2$$
$$= m^2((x')^2+(y')^2),$$

so $(x')^2+(y')^2 = rp$, with $0 < r \le \frac{m}{2}$.

Contradiction with definition of m.

4 Follows the same steps as previous exercise. Need to show that for each prime p, there exists $0 < m < p$ with $mp = x_1^2+x_2^2+x_3^2+x_4^2$.

If $p=2$, $2 = 1^2+1^2+0^2+0^2$.

If $p>2$, we saw in the course that every element in $\mathbb{Z}/p\mathbb{Z}$ is a sum of two squares (from CA).

So there exists $0 < \frac{|x_1|}{2}, \frac{|x_2|}{2}, \frac{|x_3|}{4}, \frac{|x_4|}{4} \le \frac{p}{2}$

$-1 \equiv x_1^2+x_2^2 \pmod{p}$

$1 \equiv x_3^2+x_4^2 \pmod{p}$.

Hence $x_1^2+x_2^2+x_3^2+x_4^2 = mp$ with $0 < m < p$.

Rest of proof follows as previous exercise.

⑤ a) If $h = p-1$, then $\sum_{x \in \mathbb{F}_p} x^{p-1} = p-1$.

Now assume $1 \leq h < p-1$.

Write $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$, where g primitive root of unity.

Let $d = \gcd(h, p-1)$, so $h = dk$, $\gcd(k, p-1) = 1$.

Then $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g^k \rangle$.

Now $\sum_{x \in \mathbb{F}_p} x^h = \sum_{x \in \mathbb{F}_p^\times} x^h = \sum_{1 \leq n \leq p-1} g^{nh}$

$= \sum_{1 \leq n \leq p-1} (g^k)^{nd} =$

$= d \cdot \sum_{1 \leq n \leq \frac{p-1}{d}} (g^k)^{nd}$ $\qquad \sum \alpha^i = x^n - 1$

$= d \cdot \left(g^k \cdot \frac{(g^k)^{p-1} - 1}{g^{kd} - 1} \right) = 0,$

Since $g^{kd} \neq 1$ as $d < p-1$.

b) Note that $P(\underline{x})^{p-1} = \begin{cases} 0, & \text{if } P(\underline{x}) = 0 \\ 1, & \text{else.} \end{cases}$

Conclusion follows.

c) Note that $\sum_{\underline{x} \in \mathbb{F}_p^n} x_1^{j_1} \cdots x_n^{j_n} = \prod_{k=1}^{n} \left(\sum_{x_k \in \mathbb{F}_p} x_k^{j_k} \right)$

Now, if $\sum_{k=1}^{n} j_k < n(p-1)$, then $\exists\, k \in \{1, \dots, n\}$ such that $j_k < p-1$, so $\sum_{x_k \in \mathbb{F}_p} x_k^{j_k} = 0$.

This also shows that if $\deg(Q) < n(p-1)$, then $S(Q) = 0$

(Q is a sum of monomials).

d) Conclusion follows by choosing $Q = 1 - P(\underline{x})^{p-1}$.

e) If $P(\underline{x})$ homogeneous of degree $0 < d < n$, then the number of solutions to $P(\underline{x}) = 0$ is a multiple of p. Since $(0, \dots 0)$ is a solution, there are at least $p-1$ other solutions.

6 a) Since $S_b \subset A+B$, $\forall b \in B$, then $\bigcup_{b \in S_b} S_b \subset A+B$.

$\forall\, a \in A, b \in B$, $\quad a+b \in A+b \subset A_b + B_b = S_b$

So $A+B \subset \bigcup_b S_b$.

b) Let $t \in A_b - b$.

This implies $b \in A_b - t$, so $b \in B_b \cap (A_b - t) = \sigma_t(B_t)$.

$A \subset A_b \subset \sigma_t(A_b)$.

Also $A_b + B_b = \sigma_t(A_b) + \sigma_t(B_b)$ with

$$|A_b| + |B_b| = |\sigma_t(A_b)| + |\sigma_t(B_b)| \quad \checkmark$$

c) Minimality of B_b implies $B_b \subset A_b - t, \ \forall t \in A_b - b$

This implies $A_b \supset \bigcup_{t \in A_b - b} (B_b + t) = A_b + B_b + t$,

equivalently $B_b - b \subset \mathrm{Stab}(A_b)$.

d) Since $\mathrm{Stab}\, S_b \supset \mathrm{Stab}(A_b)$,

$$|S_b| + |\mathrm{Stab}\, S_b| \geq |S_b| + |\mathrm{Stab}\, A_b| \geq |S_b| + |B_b|$$
$$\geq |A_b| + |B_b| = |A| + |B|$$

e) Since $\bigcup_b S_b = A + B$, we have

$$\circledast \ |A+B| + |\mathrm{Stab}(A+B)| \geq \min_b (|S_b| + |\mathrm{Stab}(S_b)|) \geq |A| + |B|$$

Note that $A+H+B+H = A+B$

and $\mathrm{Stab}(A+H+B+H) = H$.

Apply $\circledast$ to $A' = A+H$, $B' = B+H$.

7 a) Assume we know for union of $k-1$ sets.

$$|S_2 \cup .. \cup S_k| + |\mathrm{Stab}(S_2 \cup .. \cup S_k)| \geq$$
$$\geq \min \{ |S_2| + |\mathrm{Stab}\, S_2|, \ |S_2 \cup .. \cup S_k| + |\mathrm{Stab}(S_2 \cup .. \cup S_k)| \}$$

$\geq \min_j \{ |S_j| + |\mathrm{Stab}\, S_j| \}$ by induction hypothesis

b) Let $H_i = \mathrm{Stab}(S_i)$, $H_0 = H_1 \cap H_2$.

Note that $S_i = \bigcup_{s \in S_i} (s + H_i)$, so S_i is a union of cosets of H_i.

This shows all sets S_1, S_2, $S_1 \cup S_2$, $\mathrm{Stab}(S_1 \cup S_2)$, $\mathrm{Stab}\, S_1$, $\mathrm{Stab}\, S_2$ are unions of cosets of H_0.

Can assume $H_0 = \{0\}$.

c) If $\exists h_1, h_1' \in H_1$, $h_2, h_2' \in H_2$ with

$h_1 + h_2 = h_1' + h_2' \Rightarrow \underbrace{h_1 - h_1'}_{\in H_1} = \underbrace{h_2' - h_2}_{\in H_2}$

$\to h_1 = h_1'$ & $h_2 = h_2'$

$\to |H_1 + H_2| = |H_1||H_2|$.

d) Let $h_1 \in H_1$, $h_2 \in H_2$.

$|(x + h_1 + h_2 + H_2) \cap S_1| = |(x + h_1 + H_2) \cap S_1|$

$= |(x + H_2) \cap (S_1 - h_1)| = |(x + H_2) \cap S_1|$.

Similarly for $k_2(x)$.

For all $x \in S$, $|(S \setminus S_2) \cup (x + H_1)| = h_1 - k_2$.

Also $(x + H)$ is a union of h_2 cosets of H_1, and k_1 of them are inside S_1.

e) If $\exists x$ s.t. $0 < k_2(x) < h_2$ & $0 < k_2(x) < h_1$, then $|S \setminus S_2||S \setminus S_2| \geq k_2 k_2 (h_1 - k_2)(h_2 - k_1)$

$$\geq (h_1 - 1)(h_2 - 1)$$

$\Rightarrow$ at least one of $|S \setminus S_i| \geq h_i - 2$ is true.

But then $|S \setminus S_i| \geq h_i - |H|$.

$$\underset{|S_1 \cup S_2| - |S_i|}{\overset{\shortparallel}{|S \setminus S_i|}}$$

✓

f) if $k_1(x) = 0 < k_2(x)$, $\quad k_2(y) = 0 < k_1(y)$

$$|S \setminus S_2||S \setminus S_2| \geq |(S \setminus S_2) \cap (x + H)| \, |(S \setminus S_2) \cap (y + H)|$$

$$= k_1(y) h_1 \cdot k_1(x) h_2 \geq h_1 h_2.$$

Conclusion follows as above.

g) Note that if $x \in S_1$, then $k_1(x) > 0$

Similarly, for $x \in S_2$, $k_2(x) > 0$.

Note that if $k_1(x) = h_2$ and $k_2(x) = h_1$, then

$x + H_2 \subset S_1$ & $x + H_1 \subset S_2$

$\Rightarrow x + H \subset S_1$ & $x + H \subset S_2$.

Conclusion follows.

So we must have $k_2(x) = h_2$, $\forall x \in S_2$.

$\Rightarrow H_2 + x \subset S_2$, $\forall x \in S_2$

$\Rightarrow H_1 < \mathrm{Stab}(S_2)$

$\Rightarrow H_1 < \mathrm{Stab}(S_1 \cup S_2)$, conclusion follows.

(8) Check any number theory book for (possibly many different) proofs of quadratic reciprocity.

8 a) Quadratic reciprocity states that if p, q are odd primes, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

"$\Rightarrow$" Assume QR holds.

- If $p \equiv q \pmod{4a}$, in particular $p \equiv q\ (4)$,
  so $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}}$.

If $k \geq 1$, then $p \equiv q \pmod 8$

$$\Rightarrow \left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = \begin{cases} 1, & p \equiv 1, 7\ (8) \\ -1, & p \equiv 3, 5\ (8) \end{cases}$$

If r / a prime $\Rightarrow \left(\frac{r}{p}\right) = \left(\frac{p}{r}\right)(-1)^{\frac{p-1}{2}\frac{r-1}{2}}$
$r > 2$.

$$= \left(\frac{q}{r}\right)(-1)^{\frac{q-1}{2}\frac{r-1}{2}} = \left(\frac{r}{q}\right).$$

Since $r \mid p - q$, $p \equiv q\ (4)$.

- If $p \equiv -q \pmod{4a}$
  If $2 / a \Rightarrow p \equiv -q \pmod 8 \Rightarrow \left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$.

If $r / a, r > 2$: $\left(\frac{r}{p}\right) = \left(\frac{p}{r}\right)(-1)^{\frac{p-1}{2}\frac{r-1}{2}}$

$$= \left(\frac{-q}{r}\right)(-1)^{\frac{p-1}{2}\frac{r-1}{2}}$$

$$= \left(\frac{q}{r}\right)(-1)^{\frac{r-1}{2}}(-1)^{\frac{r-1}{2}\frac{p-1}{2}}$$

$$= \left(\frac{r}{q}\right)(-1)^{\frac{r-1}{2}}(-1)^{\frac{r-1}{2}\frac{p-1}{2}}(-1)^{\frac{r-1}{2}\frac{q-1}{2}}$$

$$= \left(\frac{r}{q}\right) \text{ since } (-1)^{\frac{p-1}{2}+\frac{q-1}{2}} = 1.$$

"$\Leftarrow$" Select $a = \pm p \pm q$ depending on congruences mod 4. . . .

b) Evaluate $Z = a \cdot (2a) \cdots \left(\frac{p-1}{2}\right) a \mod p$ in two different ways.

c)