Задача 1

$g \in H(A) \Rightarrow g + A = A \Rightarrow g + A + B = A + B \Rightarrow g \in H(A + B)$.

Задача 2

Пусть $A < G$. Тогда если $g \in H(A) \Rightarrow g + A = A \Rightarrow g + 0 \in A \Rightarrow g \in A$.

Пусть $H(A) = A$. Рассмотрим $a \in H(A) = A, b \in A \Rightarrow a + A = A \Rightarrow a + b \in A$. Теперь рассмотрим $-a$. В силу того, что множество A замкнуто по сложению и конечно, приходим к выводу, что a имеет конечный порядок, то есть $k \cdot a = 0 \Rightarrow -a = a + \ldots + a \in A$.

Задача 3

По теореме Кнезера: $|A_1 + \ldots + A_h| \geqslant |A_1 + \ldots + A_{h-1}| + |A_h| - |H(A_1 + \ldots + A_h)| \geqslant \ldots \geqslant |A_1| + \ldots + |A_h| - |H(A_1 + A_2)| - \ldots - |H(A_1 + \ldots + A_h)|$. Так как $H(A_1 + A_2) < \ldots < H(A_1 + \ldots + A_h)$, можем оценить последнее выражение как $\sum\limits_{i=1}^{h} |A_i| - (h-1)|H(A_1 + \ldots + A_h)|$.

Задача 4

Очевидно, что $|(A+B)/H| = |A/H| + |B/H| - 1 \Leftrightarrow |A + B + H| = |A + H| + |B + H| + |H|$. С другой стороны $|A/H| = \frac{|A+H|}{|H|}$, значит $|(A+B)/H| = \frac{|A+H+B+H|}{|H|} = \frac{|A+B|}{|H|}$, стало быть $|A + B|$ делится на $|H|$.

Пусть $|A + B| \leqslant |A| + |B| - 1 \Rightarrow |A + B| \leqslant |A + H| + |B + H| - 1$. По теореме Кнезера $|A+B| \geqslant |A+H| + |B+H| - |H|$ и, так как $|A+B|$ кратно H, то $|A+B| = |A+H| + |B+H| - |H| \Rightarrow |(A+B)/H| = |A/H| + |B/H| - 1$.

Задача 5

Если $H = \{0\}$, то всё получаем требуемое по теореме Кнезера. Иначе H — циклическая подгруппа, порожденная элементом x, притом x делит m. Рассмотрим множество $B + H \supset B$. В нём содержатся также элементы $x, 2x, \ldots, m - x$, которые не содержатся в B, так как каждый элемент B, кроме 0 взаимнопрост с m. Отсюда $|B + H| \geqslant |B| + |H| - 1$. Применяя теорему Кнезера, получаем: $|A + B| \geqslant |A + H| + |B + H| - |H| \geqslant |A + H| + |B| + |H| - 1 - |H| \geqslant |A| + |B| - 1$.

Задача 6

Возьмём любые два множества A, B и рассмотрим $H = H(A + B)$. Применим неравенство к $A + H, B + H : |A + H + B + H| \geqslant |A + H| + |B + H| - |H(A + H + B + H)|$. Так как $A + B + H + H = A + B + H = A + B$, то получаем $|A + B| \geqslant |A + H| + |B + H| - |H(A + B)|$.

Задача 7

Выведем из каждого следующее:

- $|A+B| = |A||B| \Rightarrow \forall a_1 \neq a_2, b_1 \neq b_2 \to a_1 + b_1 \neq a_2 + b_2 \Rightarrow a_1 - b_2 \neq a_2 - b_1 \Rightarrow |A - B| = |A||B|$.
- $|A-B| = |A||B| \Rightarrow \forall a_1 \neq a_2, b_1 \neq b_2 \to a_1 - b_1 \neq a_2 - b_2 \Rightarrow a_1 + b_2 \neq a_2 + b_1 \Rightarrow$ для пары (a_1, b_2) существует только одна пара $(x, y) = (a_1, b_2)$, такая что $a_1 + b_2 = x + y$, если $x \in A, y \in B$. Значит размер указанного множества равен $|A||B|$.
- Заметим, что $a_1 + b_1 = a_2 + b_2 \Leftrightarrow a_1 - b_2 = a_2 - b_1$, что даёт биекцию между множествами.
- Рассмотрим какой-то элемент $x = a_1 + b_1$. Если $a_2 = x - b_2$, то $a_2 = a_1 + b_1 - b_2 \Rightarrow a_2 - b_1 = a_1 - b_2$. Так как существует ровно одна такая четвёрка, то $a_2 = a_1, b_2 = b_1$, то элемент в пересечении $|A \cap (x - B)|$ ровно один.
- Пусть для какого-то $y = a_1 - b_1 \in A - B$ это не так, то есть $|A \cap (B + a_1 - b_1)| > 1$, то есть существует $a_2, b_2 : a_2 \neq a_1, b_2 \neq b_1, a_2 = b_2 + a_1 - b_1 \Rightarrow a_1 = a_2 - b_2 + b_1$, то есть $|A \cap (B + y)| > 2$ для $y = a_2 - b_2$, противоречие.
- Пусть $0 \neq x \in (A - A) \cap (B - B), x = a_1 - a_2 = b_1 - b_2, a_1 \neq a_2, b_1 \neq b_2$. Тогда $|A \cap (B + y)| > 2$ для $y = a_2 - b_2$.
- Пусть $|A + B| < |A||B|$. Тогда $\exists (a_1, b_1) \neq (a_2, b_2) : a_1 + b_1 = a_2 + b_2 \Rightarrow a_1 - a_2 = b_2 - b_1 = x$, притом $x \neq 0$. Значит $0 \neq x \in (A - A) \cap (B - B)$, противоречие.

Задача 8

Если $|A + cB| < |A||B|$, то найдутся $(a_1, b_1) \neq (a_2, b_2) : a_1 + cb_1 = a_2 + cb_2 \Rightarrow c = \frac{a_1 - a_2}{b_2 - b_1}$.

Задача 9

$|(c + dP)(c + dP)| = |c^2 + cdP + cdP + d^2 P| = |c^2 + cdP + d^2 P| = |cdP + d^2 P|$. С другой стороны это по условию $|c + dP|$. По задаче 8, c представимо как $c = d\frac{p_1 - p_2}{p_3 - p_4} \in dP$.

Задача 10

Достаточность очевидна. Положим $|\mathbb{F}| = p^k$. Положим $A' = A - a_0, a_0 \in A$. Тогда $|A'| = |A| = |A + A| = |2a_0 + A' + A'| = |A' + A'|$. Однако $A' \subset A' + A' \Rightarrow A' = A' + A'$, то есть A' есть смежный класс по H. Так как он содержит 0, то A' есть подгруппа $\mathbb{F}$ по сложению.

Если $0 \notin A$, то аналогичными рассуждениями получаем, что $A = cA''$, где A'' подгруппа $\mathbb{F}^*$ по умножению. Но тогда по теореме Лагранжа $|A|$ делит $|\mathbb{F}| = p^k$ и $|\mathbb{F}^*| = p^k - 1$. Так как эти числа взаимнопросты, то $|A| = 1$, тогда все тривиально.

Итак, $0 \in A$, значит $A \setminus \{0\}$ — (возможно мультипликативно сдвинутая) подгруппа по умножению. То есть $A = cP$, где P — подкольцо с единицей. Так как порядок всех элементов конечный, то если $a \in P$, то $\exists q : a^q = 1$. Так как $P \cdot P = P$, то $a^{-1} = a^{q-1} \in P$, то есть P — подполе, ч.т.д.

Задача 11

Рассмотрим двоичные записи чисел из $A + A$. Все числа вида $2^i + 2^j$ имеют две единицы в двоичной записи (на позициях до n-й) за исключением тех, что имеют вид $2^i + 2^i = 2^{i+1}$. С другой стороны каждое такое число легко получить, сложив нужные степени двойки. Стало быть $|A+A| \geqslant C_{n+1}^2$, значит и $|A + A| = C_{n+1}^2$.