Show that $(pv) \cdot g = 0$. Similarly show that $(pu) \cdot h = 0$.

23.3 Using that m is the order of the element g, show that if an integer q has the property $q \cdot g = 0$, then m divides q. Conclude that m divides (pv). Similarly n divides (pu).

23.4 Show that u is relatively prime to n (otherwise we would have a non-trivial divisor of the sum $1 = um + vn$). Similarly v is relatively prime to m.

23.5 Conclude that m divides p, and n divides p, hence that mn divides p.

23.6 Conclude that the order of the element $g + h$ is mn.

23.7 Use induction to improve this result: suppose $h_1, \ldots, h_k$ are elements of a finite commutative group G, such that h_i is of order m_i. Suppose that the m_i are pairwise relatively prime. Then show that the element

$$h = h_1 + h_2 + \ldots + h_k$$

has order $m_1 m_2 \cdots m_k$.

Question 24. (*Finite commutative groups — II*)

Suppose G is a commutative group, that is finite, with order n (in other words, G has n elements). The notation of G will be additive, in other words $G = (G, +, 0)$.

We would like to show the following lemma:

Lemma: *Suppose G is a finite our finite commutative group of order n. Then either*

(a) G is cyclic, i.e. $G \cong \mathbb{Z}/n\mathbb{Z}$; or

(b) there is a number $m < n$ such that m divides n, such that every element of G has order dividing m.

Write the prime factor decomposition

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Let b_i be the maximum power of the prime p_i that occurs in the order of any element of g.

24.1 Show that $b_i \leq a_i$.

24.2 If $b_i < a_i$ for some $i = 1, \ldots, k$ then show that we can take $m := n/p_i$ and obtain the conclusion (b) of the Lemma.

24.3 Therefore we may now assume $b_i = a_i$. Let $g_i \in G$ be an element of order d_i such that $p_i^{a_i}$ divides d_i (point out that this exists by the definition of b_i). Show that if we set $e_i := d_i/p_i^{a_i}$ then $h_i = e_i \cdot g_i$ is an element of G of order $p_i^{a_i}$.

24.4 Let $h := h_1 + h_2 + \cdots + h_k \in G$ be the sum of all these elements. Remember that we are assuming G is commutative. Use the result of 23.7