Worksheet - Order in the Classroom

Recall that for \((a, m) = 1\), the order of \(a\) modulo \(m\) is the least positive value so that \(a^h \equiv 1 \pmod{m}\). The exponent is denoted by \(\text{ord}_m(a)\).

Let \(H(m)\) denote the set of orders of elements modulo \(m\). Let \(L(m)\) denote the largest element of the set \(H(m)\).

1 For \(2 \leq m \leq 13\) determine the following:
   i. The set \(H(m)\)
   ii. The value \(L(m)\).
   iii. A list of the reduced residues modulo \(m\) sorted by order.

2 For prime numbers \(p\) satisfying \(3 \leq p \leq 29\) determine the following:
   i. The set \(H(p)\)
   ii. A residue \(a\) modulo \(p\) so that \(\text{ord}_p(a) = L(p)\).

3 For \(p = 31\):
   Let \(G(p)\) denote the subset of reduced residues modulo \(p\) whose order is \(L(p)\).
   Let \(g = \) the smallest element of \(G(p)\).
   For all residues \(a \in G(p)\), write \(a \equiv g^k \pmod{p}\), where \(k\) is the least positive exponent that makes the congruence true. Let \(E(p)\) be the set of such exponents.
   What property do the elements of \(E(p)\) share? (if you’re not sure, repeat the computations for \(p = 47, 67, \text{etc} - \) the property is the same)