Problem 11538
(American Mathematical Monthly, Vol.117, December 2010)

Proposed by M. Tetiva (Romania).

Prove that a finite commutative ring in which every element can be written as a product of two (not necessarily distinct) elements has a multiplicative identity.

Solution proposed by Roberto Tauraso, Dipartimento di Matematica, Università di Roma "Tor Vergata", via della Ricerca Scientifica, 00133 Roma, Italy.

We will prove the statement by induction with respect to the number of elements r of R. If $r = 0$ then $R = \{0\}$ and we can take 0 as multiplicative identity.
Let $R = \{a_1, a_2, \ldots, a_r\}$ with $r > 1$. Since every element can be written as a product of two elements, by applying this property a suitable number of times, we have that for any positive integer n and for any $a_j \in R$ there exist a non-empty subset $S \subset \{1, 2, \ldots n\}$, and positive integers $\{m_i\}_{i\in S}$ such that

$$a_j = \prod_{i\in S} a_i^{m_i} \quad \text{with } \max\{m_i\}_{i\in S} \geq n \tag{1}$$

Moreover, there is an element $\overline{a} \in R$ such that no power of $\overline{a}$ is equal zero. Otherwise, for any $a_j \in R$ there is a positive integer c_j such that $a_j^{c_j} = 0$ and by taking $n > \max\{c_j\}_{1\leq j\leq n}$, by (1) we find that $a_j = 0$ for any $a_j \in R$ which is a contradiction.
Since R is finite, the powers of $\overline{a}$ are not all different and there are two positive integers j and k such that $\overline{a}^j = \overline{a}^{j+nk}$ for all $n \geq 1$. Let n be sufficiently large such that $nk > j$, then

$$(\overline{a}^{nk})^2 = \overline{a}^{j+nk} \cdot \overline{a}^{nk-j} = \overline{a}^j \cdot \overline{a}^{nk-j} = \overline{a}^{nk},$$

and $e := \overline{a}^{nk}$ is a nonzero idempotent of R.
Let $I = eR$ and $I' = R - eR$, then I, I' are ideals of R such that

$$ae = (re)e = re^2 = re = a \quad \forall a \in I \quad , \quad ae = (r - re)e = re - re^2 = re - re = 0 \quad \forall a \in I'$$

Since $a = ae + (a - ae)$ for any $a \in R$ and $I \cap I' = \{0\}$, it follows that we can write R as a direct sum of I and I'. If $I' = \{0\}$ then $R = I$ and e is a multiplicative identity. On the other hand, if $I' \neq \{0\}$ then $|I'| < r$. Moreover, every element a of I' can be written as a product of two elements $c', d' \in I'$: by hypothesis $a = cd$ for some $c, d \in R$ then $0 = ae = cde = cde^2$ and

$$a = cd = cd - cde - dce + cde^2 = (c - ce)(d - de) = c'd'.$$

Therefore, by the induction hypothesis applied to the finite commutative ring I', there is a multiplicative identity $e' \in I'$ and $e + e'$ is a multiplicative identity of R:

$$(e+e')a = (e+e')(ae+(a-ae)) = ae^2+e'ae+e(a-ae)+e'(a-ae) = ae^2+(e'a)e+ea-ae^2+a-ae = a.$$

$\square$

Remark. Note that this problem is similar to this other one which appeared in 1965 Miklos Schweitzer Competition:

Let R be a finite commutative ring. Prove that R has a multiplicative identity element if and only if the annihilator of R is 0 (that is, $aR = 0$, $a \in R$ imply $a = 0$).