Problem 1276 Solution.

Solution. The problem posed had 2p numbers given. That is the form in Winkler's book. But in fact it is true even if one has only 2p-1 numbers. (And one need not assume primality, but for that extension I refer you to the papers. In short, the general case reduces to the prime case.) This is an old result of Erdos, Ginzburg, and Ziv ("Theorem in the additive number theory", Bull. of the Research Council of Isreal, 10F (1961) 41-43) and is tricky. I received no solutions. The paper "Zero-sum sets of prescribed size", by Noga Alon and Moshe Dubiner (COMBINATORICS, PAUL ERDŐS IS EIGHTY, 1 (1993) 33-50 <https://www.tau.ac.il/~nogaa/PDFS/egz1.pdf>) contains several proofs and I will present a very elegant one here. It makes use of Fermat's little theorem (a^(p-1) === 1 (mod p) when p is prime and p does not divide a).

Best to start with an example of the method.

Suppose $p = 3$. Form S, the sum of all the $(p-1)$th powers of sums of p-subsets of $2p-1$:

$$S = (a(1) + a(2) + a(3))^2 + (a(1) + a(2) + a(4))^2 + (a(1) + a(3) + a(4))^2 + (a(2) + a(3) + a(4))^2 + (a(1) + a(2) + a(5))^2 + (a(1) + a(3) + a(5))^2 + (a(2) + a(3) + a(5))^2 + (a(1) + a(4) + a(5))^2 + (a(2) + a(4) + a(5))^2 + (a(3) + a(4) + a(5))^2$$

Expand:

$$S = 6\,a(1)^2 + 6\,a(2)\,a(1) + 6\,a(3)\,a(1) + 6\,a(4)\,a(1) + 6\,a(5)\,a(1) + 6\,a(2)^2 + 6\,a(3)^2 + 6\,a(4)^2 + 6\,a(5)^2 + 6\,a(2)\,a(3) + 6\,a(2)\,a(4) + 6\,a(3)\,a(4) + 6\,a(2)\,a(5) + 6\,a(3)\,a(5) + 6\,a(4)\,a(5)$$

Note that each coefficient is divisible by p. There is a reason for that: Consider, the term $6\,a_2\,a_5$. Why is the 6 there? It arises from the three unexpanded terms

$(a(1) + a(2) + a(5))^2$ and $(a(2) + a(3) + a(5))^2$ and $(a(2) + a(4) + a(5))^2$.

Each of these terms contributes 2 to the product. But the number of these terms is 3, which in this case arises from $\binom{5-2}{3-2} = \binom{3}{1} = 3$. The "−2" is because two entries are fixed (a(4) and a(5)).

Now move to the general case. The sum S uses $(p-1)$th powers. The coefficient of any particular monomial with j positive exponents will arise from $\binom{2p-1-j}{p-j}$ subsets of size p. They each contribute the same amount (the binomial coefficient in the expansion), so the coefficient will be 0 (mod p) if $\binom{2p-1-j}{p-j} \equiv 0$ (mod p). But the binomial coefficient is clearly divisible by p, because p will divide the numberator but not the denominator. So we have that p divides S.

Now, if there is some p-subset whose sum is divisible by p, we are done, so assume there is no such set.

So in the sum that defines S, each summand is a $(p-1)$th power of a nonzero number (mod p). By Fermat's little theorem, every such power is 1, and that means $S \equiv \binom{2p-1}{p}$ (mod p). But this binomial coefficient is

$$\frac{(2p-1)\cdot(2p-2)\cdots p}{1\cdot 2\cdot 3\cdots p} = \frac{(2p-1)\cdot(2p-2)\cdots(p+1)}{(p-1)\,(p-2)\cdots 1} = \frac{(p-1)\cdot(p-2)\cdots 1}{(p-1)\,(p-2)\cdots 1} \equiv 1 \pmod{p}$$, contradicting S≡0 (mod p).

This proof is due to several people independently. Details are in the Alon and Dubiner paper.