$w_1, \dots, w_n$ be the projections of $e_1, \dots, e_n$. If the desired condition is not achieved, we can choose i, j such that

$$|w_i|^2 < \frac{1}{n}(|w_1|^2 + \cdots + |w_n|^2) < |w_j|^2.$$

By precomposing with a suitable rotation that fixes e_h for $h \neq i, j$, we can vary $|w_i|, |w_j|$ without varying $|w_i|^2 + |w_j|^2$ or $|w_h|$ for $h \neq i, j$. We can thus choose such a rotation to force one of $|w_i|^2, |w_j|^2$ to become equal to $\frac{1}{n}(|w_1|^2 + \cdots + |w_n|^2)$. Repeating at most $n-1$ times gives the desired configuration.

B–4 We use the identity given by Taylor's theorem:

$$h(x+y) = \sum_{i=0}^{\deg(h)} \frac{h^{(i)}(x)}{i!} y^i.$$

In this expression, $h^{(i)}(x)/i!$ is a polynomial in x with integer coefficients, so its value at an integer x is an integer.

For $x = 0, \dots, p-1$, we deduce that

$$h(x+p) \equiv h(x) + ph'(x) \pmod{p^2}.$$

(This can also be deduced more directly using the binomial theorem.) Since we assumed $h(x)$ and $h(x+p)$ are distinct modulo p^2, we conclude that $h'(x) \not\equiv 0 \pmod{p}$. Since h' is a polynomial with integer coefficients, we have $h'(x) \equiv h'(x+mp) \pmod{p}$ for any integer m, and so $h'(x) \not\equiv 0 \pmod{p}$ for all integers x.

Now for $x = 0, \dots, p^2-1$ and $y = 0, \dots, p-1$, we write

$$h(x+yp^2) \equiv h(x) + p^2 yh'(x) \pmod{p^3}.$$

Thus $h(x), h(x+p^2), \dots, h(x+(p-1)p^2)$ run over all of the residue classes modulo p^3 congruent to $h(x)$ modulo p^2. Since the $h(x)$ themselves cover all the residue classes modulo p^2, this proves that $h(0), \dots, h(p^3-1)$ are distinct modulo p^3.

Remark: More generally, the same proof shows that for any integers $d, e > 1$, h permutes the residue classes modulo p^d if and only if it permutes the residue classes modulo p^e. The argument used in the proof is related to a general result in number theory known as *Hensel's lemma*.

B–5 The functions $f(x) = x+n$ and $f(x) = -x+n$ for any integer n clearly satisfy the condition of the problem; we claim that these are the only possible f.

Let $q = a/b$ be any rational number with $\gcd(a,b) = 1$ and $b > 0$. For n any positive integer, we have

$$\frac{f(\frac{an+1}{bn}) - f(\frac{a}{b})}{\frac{1}{bn}} = bnf\left(\frac{an+1}{bn}\right) - nbf\left(\frac{a}{b}\right)$$

is an integer by the property of f. Since f is differentiable at a/b, the left hand side has a limit. It follows that for sufficiently large n, both sides must be equal to some integer $c = f'(\frac{a}{b})$: $f(\frac{an+1}{bn}) = f(\frac{a}{b}) + \frac{c}{bn}$. Now c cannot be 0, since otherwise $f(\frac{an+1}{bn}) = f(\frac{a}{b})$ for sufficiently large n has denominator b rather than bn. Similarly, $|c|$ cannot be greater than 1: otherwise if we take $n = k|c|$ for k a sufficiently large positive integer, then $f(\frac{a}{b}) + \frac{c}{bn}$ has denominator bk, contradicting the fact that $f(\frac{an+1}{bn})$ has denominator bn. It follows that $c = f'(\frac{a}{b}) = \pm 1$.

Thus the derivative of f at any rational number is ± 1. Since f is continuously differentiable, we conclude that $f'(x) = 1$ for all real x or $f'(x) = -1$ for all real x. Since $f(0)$ must be an integer (a rational number with denominator 1), $f(x) = x+n$ or $f(x) = -x+n$ for some integer n.

Remark: After showing that $f'(q)$ is an integer for each q, one can instead argue that f' is a continuous function from the rationals to the integers, so must be constant. One can then write $f(x) = ax+b$ and check that $b \in \mathbb{Z}$ by evaluation at $a = 0$, and that $a = \pm 1$ by evaluation at $x = 1/a$.

B–6 In all solutions, let $F_{n,k}$ be the number of k-limited permutations of $\{1, \dots, n\}$.

First solution: (by Jacob Tsimerman) Note that any permutation is k-limited if and only if its inverse is k-limited. Consequently, the number of k-limited permutations of $\{1, \dots, n\}$ is the same as the number of k-limited involutions (permutations equal to their inverses) of $\{1, \dots, n\}$.

We use the following fact several times: the number of involutions of $\{1, \dots, n\}$ is odd if $n = 0, 1$ and even otherwise. This follows from the fact that non-involutions come in pairs, so the number of involutions has the same parity as the number of permutations, namely $n!$.

For $n \leq k+1$, all involutions are k-limited. By the previous paragraph, $F_{n,k}$ is odd for $n = 0, 1$ and even for $n = 2, \dots, k+1$.

For $n > k+1$, group the k-limited involutions into classes based on their actions on $k+2, \dots, n$. Note that for C a class and $\sigma \in C$, the set of elements of $A = \{1, \dots, k+1\}$ which map into A under σ depends only on C, not on σ. Call this set $S(C)$; then the size of C is exactly the number of involutions of $S(C)$. Consequently, $|C|$ is even unless $S(C)$ has at most one element. However, the element 1 cannot map out of A because we are looking at k-limited involutions. Hence if $S(C)$ has one element and $\sigma \in C$, we must have $\sigma(1) = 1$. Since σ is k-limited and $\sigma(2)$ cannot belong to A, we must have $\sigma(2) = k+2$. By induction, for $i = 3, \dots, k+1$, we must have $\sigma(i) = k+i$.

If $n < 2k+1$, this shows that no class C of odd cardinality can exist, so $F_{n,k}$ must be even. If $n \geq 2k+1$, the classes of odd cardinality are in bijection with k-limited involutions of $\{2k+2, \dots, n\}$, so $F_{n,k}$ has the same parity as $F_{n-2k-1,k}$. By induction on n, we deduce the desired result.