Solutions to the Special K Problems, 2013

1: Let a, n and k be positive integers. Suppose $m \geq 3$ and $\gcd(a,m)=1$. Show that $a^k+(m-a)^k \equiv 0 \bmod m^2$ if and only if m is odd and $k \equiv m \bmod 2m$.

Solution: In order to have $a^k+(m-a)^k \equiv 0 \bmod m^2$, we must have $a^k+(m-a)^k \equiv 0 \bmod m$. Working modulo m we have

$$\begin{aligned} a^k+(m-a)^k \equiv 0 &\iff a^k+(-a)^k \equiv 0 \iff a^k\big(1+(-1)^k\big) \equiv 0 \\ &\iff 1+(-1)^k \equiv 0 \iff (-1)^k \equiv -1 \mod m \end{aligned}$$

where, at one step in the above calculation, we divided by a^k which we can do since $\gcd(a,m)=1$. Since $m \geq 3$, in order to have $(-1)^k \equiv -1 \bmod m$, we see that k must be odd. When k is odd, working modulo m^2 we have

$$\begin{aligned} a^k+(m-a)^k \equiv 0 &\iff a^k+\big(m^k-km^{k-1}a+\cdots+kma^{k-1}-a^k\big) \equiv 0 \\ &\iff a^k+kma^{k-1}-a^k \equiv 0 \iff kma^{k-1} \equiv 0 \iff km \equiv 0 \mod m^2. \end{aligned}$$

Note that $km \equiv 0 \bmod m^2 \iff k \equiv 0 \bmod m$ and so we have

$$a^k+(m-a)^k \equiv 0 \bmod m^2 \iff k \text{ is odd with } k \equiv 0 \bmod m \iff m \text{ is odd and } k \equiv m \bmod 2m.$$

2: Find the number of positive integers k such that k^2+2013 is a square.

Solution: For $k,l \in \mathbf{Z}^+$ we have

$$k^2+2013=l^2 \iff l^2-k^2=2013 \iff (l-k)(l+k)=2013.$$

Given $k,l \in \mathbf{Z}^+$ with $k<l$ and $(l-k)(l+k)=2013$, let $a=l-k$ and $b=l+k$ to obtain $a,b \in \mathbf{Z}^+$ with $a<b$ and $ab=2013$. Conversely, given $a,b \in \mathbf{Z}^+$ with $a<b$ and $ab=2013$, note that a and b are both odd (since 2013 is odd) and let $k=\frac{b+a}{2}$ and $l=\frac{b-a}{2}$ to obtain $k,l \in \mathbf{Z}^+$ with $k<l$ and $(l-k)(l+k)=2013$. Thus the number of pairs $k,l \in \mathbf{Z}^+$ with $k<l$ and $(l-k)(l+k)=2013$ is equal to the number of pairs $a,b \in \mathbf{Z}^+$ with $a<b$ and $ab=2013$. Since 2013 factors into primes as $2013=3\cdot 11\cdot 61$, it has eight positive divisors, namely $1,3,11,33,61,183,671,2013$. Thus we have four possible pairs $a,b \in \mathbf{Z}^+$, namely $(a,b)=(1,2013),(3,671),(11,183),(33,61)$, and hence four possible pairs $k,l \in \mathbf{Z}^+$, namely $(k,l)=(1006,1007),(334,337),(86,97),(14,47)$. Thus there are exactly 4 positive integers k for which k^2+2013 is a perfect square, namely $k=1006,334,86,14$.

3: For each positive integer n, let a_n be the first digit in the decimal representation of 2^n, let b_n be the number of indices $k \le n$ for which $a_k = 1$, and let c_n be the number of indices $k \le n$ for which $a_k = 2$. Show that there exists a positive integer N such that for all $n \ge N$ we have $b_n > c_n$.

Solution: Note that the sequences $\{b_n\}$ and $\{c_n\}$ are increasing with

$$b_n = \begin{cases} b_{n-1} & \text{if } a_n \ne 1 \\ b_{n-1}+1 & \text{if } a_n = 1 \end{cases} \quad \text{and} \quad c_n = \begin{cases} c_{n-1} & \text{if } a_n \ne 2 \\ c_{n-1}+1 & \text{if } a_n = 2. \end{cases}$$

We list some powers of 2 and find a few values of b_n and c_n.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2^n	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768
b_n	0	0	0	1	1	1	2	2	2	3	3	3	3	4	4
c_n	1	1	1	1	1	1	1	2	2	2	3	3	3	3	3

We claim that $b_n > c_n$ for all $n \ge 14$. From the above table, we see that $b_{14} > c_{14}$ and $b_{15} > c_{15}$. Let $n \ge 16$ and suppose, inductively, that $b_{n-1} > c_{n-1}$ and $b_{n-2} > c_{n-2}$. We must show that $b_n > c_n$. If $a_n \ne 2$ so that $c_n = c_{n-1}$, then we have $b_n \ge b_{n-1} > c_{n-1} = c_n$. Suppose that $a_n = 2$ so that $c_n = c_{n-1}+1$. Then, since 2^n begins with the digit 2, for some $k \in \mathbf{N}$ we have $2 \cdot 10^k \le 2^n < 3 \cdot 10^k$. Dividing by 2 gives $1 \cdot 10^k \le 2^{n-1} < 1.5 \cdot 10^k$ which implies that 2^{n-1} begins with the digit 1 so that $a_{n-1} = 1$. Since $a_n = 2$ and $a_{n-1} = 1$ we have $b_n = b_{n-1} = b_{n-2}+1$ and $c_n = c_{n-1}+1 = c_{n-2}+1$. Thus $b_n = b_{n-2}+1 > c_{n-2}+1 = c_n$.

4: Let $\{a_n\}_{n\ge1}$ be a sequence of positive real numbers such that $a_n \le \dfrac{a_{n-1}+a_{n-2}}{2}$ for all $n \ge 3$. Show that $\{a_n\}$ converges.

Solution: Let $b_n = \max\{a_n, a_{n-1}\}$ for $n \ge 2$. We claim that $\{b_n\}_{n\ge2}$ is decreasing. If $a_{n-1} \le a_n$ so that $b_n = a_n$, then we have $a_{n+1} \le \frac{a_n+a_{n-1}}{2} \le \frac{a_n+a_n}{2} = a_n$ so that $b_{n+1} = \max\{a_{n+1}, a_n\} = a_n$, and in this case $b_{n+1} = a_n = b_n$. If $a_{n-1} \ge a_n$ so that $b_n = a_{n-1}$, then we have $a_{n+1} \le \frac{a_n+a_{n-1}}{2} \le \frac{a_{n-1}+a_{n-1}}{2} = a_{n-1}$ so that $b_{n+1} = \max\{a_{n+1}, a_n\} \le a_{n-1}$, and in this case $b_{n+1} \le a_{n-1} = b_n$. In either case, we have $b_{n+1} \le b_n$ and so $\{b_n\}$ is decreasing, as claimed. Also note that $\{b_n\}$ is bounded below by 0 (since we have $a_n \ge 0$ and $a_{n-1} \ge 0$ so that $b_n = \max\{a_n, a_{n-1}\} \ge 0$). Since $\{b_n\}$ is decreasing and bounded below, it converges. Let $l = \lim\limits_{n\to\infty} b_n$. We claim that $\{a_n\}$ converges with $\lim\limits_{n\to\infty} a_n = l$. Let $\epsilon > 0$. Choose $N \in \mathbf{Z}^+$ so that for all $n \in \mathbf{Z}^+$, if $n \ge N$ then $b_n < l + \frac{1}{7}\epsilon$. Let $n \ge N$. We shall show that $|a_n - l| < \epsilon$. Since $b_n = \max\{a_n, a_{n-1}\}$ we have $a_n \le b_n < l + \frac{1}{7}\epsilon < l + \epsilon$. It remains to show that $a_n > l - \epsilon$. Suppose, for a contradiction, that $a_n \le l - \epsilon$. Since $a_n \le l - \epsilon$ and $a_{n+1} \le b_{n+1} < l + \frac{1}{7}\epsilon$, we have $a_{n+2} \le \frac{a_{n+1}+a_n}{2} < \frac{l+\frac{1}{7}\epsilon+l-\epsilon}{2} = l - \frac{3}{7}\epsilon$. Since $a_{n+1} < l + \frac{1}{7}\epsilon$ and $a_{n+2} < l - \frac{3}{7}\epsilon$ we have $a_{n+3} \le \frac{a_{n+2}+a_{n+1}}{2} < \frac{l-\frac{3}{7}\epsilon+l+\frac{1}{7}\epsilon}{2} = l - \frac{1}{7}\epsilon$. Since $a_{n+2} < l - \frac{3}{7}$ and $a_{n+3} < l - \frac{1}{7}\epsilon$ we have $b_{n+3} = \max\{a_{n+3}, a_{n+2}\} < l - \frac{1}{7}\epsilon$, which contradicts the choice of N.

5: Let $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbf{Z}$. Suppose that $1 < f(1) < f\big(f(1)\big) < f\big(f\big(f(1)\big)\big)$. Show that $a \geq 0$.

Solution: Let
$$g(x) = f(x+1) - 1 = a(x+1)^2 + b(x+1) + c - 1 = ax^2 + dx + e$$
where $d = 2a + b$ and $e = a + b + c - 1$. Note that $g(0) = f(1) - 1$, $g(g(0)) = g(f(1) - 1) = f(f(1)) - 1$ and $g\big(g\big(g(1)\big)\big)g\big(f(f(1)) - 1\big) = f\big(f\big(f(1)\big)\big) - 1$, and so $1 < f(1) < f\big(f(1)\big) < f\big(f\big(f(1)\big)\big)$ is equivalent to
$$0 < g(0) < g\big(g(0)\big) < g\big(g\big(g(0)\big)\big).$$
Since $g(x) = ax^2 + dx + e$, we have $g(0) = e$, $g\big(g(0)\big) = g(e) = ae^2 + de + e$ and $g\big(g\big(g(0)\big)\big) = g(ae^2 + de + e) = a(ae^2 + de + e)^2 + d(ae + de + e) + e$. Thus

$$\begin{aligned}
&g(0) > 0 \implies e > 0 \\
&g(g(0)) > g(0) \implies ae^2 + de + e > e \implies e(ae + d) > 0 \implies ae + d > 0 \\
&g\big(g(g(0))\big) > g(g(0)) \implies a(ae^2 + de + e)^2 + d(ae + de + e) + e > ae^2 + de + e \\
&\quad \implies a\big(e(ae + d) + e\big)^2 + d\big(e(ae + d) + e\big) + e > ae^2 + de + e \\
&\quad \implies ae^2(ae + d)^2 + 2ae^2(ae + d) + ae^2 + de(ae + d) + de + e > ae^2 + de + e \\
&\quad \implies ae^2(ae + d)^2 + 2ae^2(ae + d) + de(ae + d) > 0 \implies e(ae + d)\big(ae(ae + d) + 2ae + d\big) > 0 \\
&\quad \implies ae(ae + d) + 2ae + d > 0 \implies ae(ae + d) + ae + (ae + d) > 0 \implies a\big(e(ae + d) + 1\big) > -(ae + d) \\
&\quad \implies a > \frac{-(ae + d)}{e\big((ae + d) + 1\big)} \implies a > -1 \ \text{ , since } \frac{1}{e} \leq 1 \text{ and } \frac{(ae + d)}{(ae + d) + 1} < 1.
\end{aligned}$$

6: Let E be the ellipse in $\mathbf{R}^2$ centred at the point O. Let A and B be two points on E such that the line OA is perpendicular to the line OB. Show that the distance from O to the line through A and B does not depend on the choice of A and B.

Solution: Let E be the ellipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, where $a, b > 0$, with centre $O = (0, 0)$. Let A be the point $A = (r\cos\theta, r\sin\theta)$. Since OA is perpendicular to OB, the point B is of the form $B = (-s\sin\theta, s\cos\theta)$ for some $s \neq 0$. Let C be the point on the line AB nearest to O. Since ΔACO is similar to ΔAOB we have $\dfrac{|OC|}{|OA|} = \dfrac{|OB|}{|AB|}$ and so the distance from O to the line AB is
$$d = |OC| = \frac{|OA|\,|OB|}{|AB|} = \frac{|r|\,|s|}{\sqrt{r^2 + s^2}} = \frac{1}{\sqrt{\frac{1}{r^2} + \frac{1}{s^2}}}.$$
Since A and B lie on the ellipse E we have
$$\frac{r^2\cos^2\theta}{a^2} + \frac{r^2\sin^2\theta}{b^2} = 1 \quad \text{and} \quad \frac{s^2\sin^2\theta}{a^2} + \frac{s^2\cos^2\theta}{b^2} = 1$$
so that
$$\frac{1}{r^2} = \frac{\cos^2\theta}{a^2} + \frac{\sin^2\theta}{b^2} \quad \text{and} \quad \frac{1}{s^2} = \frac{\sin^2\theta}{a^2} + \frac{\cos^2\theta}{b^2}$$
hence
$$\frac{1}{r^2} + \frac{1}{s^2} = \frac{\cos^2\theta + \sin^2\theta}{a^2} + \frac{\sin^2\theta + \cos^2\theta}{b^2} = \frac{1}{a^2} + \frac{1}{b^2}.$$
Thus
$$d = \frac{|r|\,|s|}{\sqrt{r^2 + s^2}} = \frac{1}{\sqrt{\frac{1}{r^2} + \frac{1}{s^2}}} = \frac{1}{\sqrt{\frac{1}{a^2} + \frac{1}{b^2}}} = \frac{ab}{\sqrt{a^2 + b^2}},$$
which does not depend on A and B.

Solutions to the Big E Problems, 2013

1: Find the number of positive integers k such that $k^2 + 10!$ is a perfect square.

Solution: For $k, l \in \mathbf{Z}^+$ we have

$$k^2 + 10! = l^2 \iff l^2 - k^2 = 10! \iff (l-k)(l+k) = 10!.$$

Given $k, l \in \mathbf{Z}^+$ with $k < l$ and $(l-k)(l+k) = 10!$, let $a = l - k$ and $b = l + k$ to obtain $a, b \in \mathbf{Z}^+$ with $a < b$ and $ab = 10!$. Note that $a = b + 2l$ so that a and b have the same parity, and since $ab = 10!$, which is even, it follows that a and b must both be even. Let $u = \frac{a}{2}$ and $v = \frac{b}{2}$ to get $u, v \in \mathbf{Z}^+$ with $u < v$ and $uv = \frac{10!}{4}$. Conversely, given $u, v \in \mathbf{Z}^+$ with $u < v$ and $uv = \frac{10!}{4}$, let $a = 2u$ and $b = 2v$ and then let $k = \frac{b+a}{2}$ and $l = \frac{b-a}{2}$ to obtain $k, l \in \mathbf{Z}^+$ with $k < l$ and $(l-k)(l+k) = 10!$. Thus the number of positive integers k for which $k^2 + 10!$ is a square is equal to the number of pairs $k, l \in \mathbf{Z}^+$ with $k < l$ and $(l-k)(l+k) = 10!$, which is equal to the number of pairs $u, v \in \mathbf{Z}^+$ with $u < v$ and $uv = \frac{10!}{4}$, which, in turn, is equal to $\frac{1}{2}\tau\left(\frac{10!}{4}\right)$ where for $n \in \mathbf{Z}^+$, $\tau(n)$ denotes the number of positive divisors of n. Since $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$ so that $\frac{10!}{4} = 2^6 \cdot 3^4 \cdot 5^2 \cdot 7^1$, we have

$$\tfrac{1}{2}\,\tau\left(\tfrac{10!}{4}\right) = \tfrac{1}{2} \cdot 7 \cdot 5 \cdot 3 \cdot 2 = 105.$$

2: Let $f : [0,1] \to \mathbf{R}$ be continuous. Suppose that $\displaystyle\int_0^x f(t)\,dt \geq f(x) \geq 0$ for all $x \in [0,1]$. Show that $f(x) = 0$ for all $x \in [0,1]$.

Solution: Suppose, for a contradiction that $f(x) > 0$ for some $x \in [0,1]$. Choose $c \in [0,1]$ so that $f(c) > 0$. Since f is continuous, we have $f(x) > 0$ in a neighbourhood of c so we can choose a point $b \in [0,1)$ with $f(b) > 0$. By the Extreme Value Theorem, we can choose $a \in [0,b]$ so that $f(x) \leq f(a)$ for all $x \in [0,b]$. Then we have

$$f(a) \leq \int_0^a f(t)\,dt \leq \int_0^a f(a)\,dt = a\,f(a) < f(a)$$

giving the desired contradiction.

3: For each positive integer n, let a_n be the first digit in the decimal representation of 2^n, let b_n be the number of indices $k \leq n$ for which $a_k = 1$, and let c_n be the number of indices $k \leq n$ for which $a_k = 2$. Show that there exists a positive integer N such that for all $n \geq N$ we have $b_n > c_n$.

Solution: Note that the sequences $\{b_n\}$ and $\{c_n\}$ are increasing with

$$b_n = \begin{cases} b_{n-1} & \text{if } a_n \neq 1 \\ b_{n-1} + 1 & \text{if } a_n = 1 \end{cases} \qquad \text{and} \qquad c_n = \begin{cases} c_{n-1} & \text{if } a_n \neq 2 \\ c_{n-1} + 1 & \text{if } a_n = 2. \end{cases}$$

We list some powers of 2 and find a few values of b_n and c_n.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2^n	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768
b_n	0	0	0	1	1	1	2	2	2	3	3	3	3	4	4
c_n	1	1	1	1	1	1	1	2	2	2	3	3	3	3	3

We claim that $b_n > c_n$ for all $n \geq 14$. From the above table, we see that $b_{14} > c_{14}$ and $b_{15} > c_{15}$. Let $n \geq 16$ and suppose, inductively, that $b_{n-1} > c_{n-1}$ and $b_{n-2} > c_{n-2}$. We must show that $b_n > c_n$. If $a_n \neq 2$ so that $c_n = c_{n-1}$, then we have $b_n \geq b_{n-1} > c_{n-1} = c_n$. Suppose that $a_n = 2$ so that $c_n = c_{n-1} + 1$. Then, since 2^n begins with the digit 2, for some $k \in \mathbf{N}$ we have $2 \cdot 10^k \leq 2^n < 3 \cdot 10^k$. Dividing by 2 gives $1 \cdot 10^k \leq 2^{n-1} < 1.5 \cdot 10^k$ which implies that 2^{n-1} begins with the digit 1 so that $a_{n-1} = 1$. Since $a_n = 2$ and $a_{n-1} = 1$ we have $b_n = b_{n-1} = b_{n-2} + 1$ and $c_n = c_{n-1} + 1 = c_{n-2} + 1$. Thus $b_n = b_{n-2} + 1 > c_{n-2} + 1 = c_n$.

4: Let p be an odd prime. Show that $\binom{2p}{p} \equiv 2 \bmod p^2$.

Solution: We have

$$\binom{2p}{p} = \frac{(2p)!}{p!\cdot p!} = \frac{2p^2\cdot\prod_{k=1}^{p-1}(p-k)\cdot\prod_{k=1}^{p-1}(p+k)}{p^2\cdot(p-1)!^2} = 2\cdot\frac{\prod_{k=1}^{p-1}(p^2-k^2)}{(p-1)!^2}$$

and so modulo p^2 we have

$$\binom{2p}{p} \equiv 2\cdot\frac{\prod_{k=1}^{p-1}(-k^2)}{(p-1)!^2} \equiv 2\cdot\frac{(-1)^{p-1}(p-1)!^2}{(p-1)!^2} \equiv 2 \bmod p^2.$$

5: Let V be a vector space over $\mathbf{R}$. Let V^* be the space of linear maps $g : V \to \mathbf{R}$. Let F be a finite subset of V^*. Let $U = \{x \in V \big| f(x) = 0 \text{ for all } f \in F\}$. Show that for all $g \in V^*$, if $g(x) = 0$ for all $x \in U$ then $g \in \operatorname{Span}(F)$.

Solution: If $F = \emptyset$ or $F = \{0\}$ then we have $U = V$, and so if $g(x) = 0$ for all $x \in U$ then $g = 0 \in \operatorname{Span} F$. Suppose that $F \neq \emptyset$ and $F \neq \{0\}$. Choose a maximal linearly independent set $\{f_1, f_2, \cdots, f_n\} \subseteq F$ so that $\{f_1, f_2, \cdots, f_n\}$ is a basis for $\operatorname{Span} F$. Note that $U = \{x \in V \big| f_1(x) = f_2(x) = \cdots = f_n(x)\}$ because for $x \in V$, if $f_1(x) = f_2(x) = \cdots = f_n(x) = 0$ then for any $f \in F$ we can write $f = \sum_{i=1}^{n} t_i f_i$ for some $t_i \in \mathbf{R}$ and then we have $f(x) = \sum_{i=1}^{n} t_i f_i(x) = 0$.

We claim that there exist vectors $v_1, v_2, \cdots, v_n \in V$ for which $f_i(v_j) = \delta_{i,j}$ for all indices i and j. Define $\phi : V \to \mathbf{R}^n$ by $\phi(x) = \big(f_1(x), f_2(x), \cdots, f_n(x)\big)^T$. Note that for $t \in \mathbf{R}^n$, we have

$$t \in \phi(V)^\perp \iff \phi(x) \bullet t = 0 \text{ for all } x \in V \iff \sum_{i=1}^{n} t_i f_i(x) = 0 \text{ for all } x \in V \iff \sum_{i=1}^{n} t_i f_i = 0 \iff t = 0.$$

Thus we have $\phi(V)^\perp = \{0\}$ and so $\phi(V) = \mathbf{R}^n$, hence ϕ is surjective. Since ϕ is surjective, for each index $j = 1, 2, \cdots, n$ we can choose $v_j \in V$ so that $\phi(v_j) = e_j$ where e_j is the j^{th} standard basis vector in $\mathbf{R}^n$. Since $e_j = \phi(v_j) = \big(f_1(v_j), f_2(v_j), \cdots, f_n(v_j)\big)^T$, we see that $f_i(v_j) = \delta_{i,j}$ for all indices i and j, as claimed.

Let $g \in V^*$ with $g(x) = 0$ for all $x \in U$. We claim that $g = \sum_{i=1}^{n} g(v_i) f_i$ so that $g \in \operatorname{Span} F$. Let $x \in V$. Let $v = \sum_{i=1}^{n} f_i(x) v_i$ and let $u = x - v$. Notice that $u \in U$ because for all indices j we have

$$f_j(u) = f_j(x-v) = f_j\big(x - \sum_{i=1}^{n} f_i(x) v_i\big) = f_j(x) - \sum_{i=1}^{n} f_i(x) f_j(v_i) = f_j(x) - \sum_{i=1}^{n} f_i(x)\delta_{i,j} = f_j(x) - f_j(x) = 0.$$

Since $u \in U$ we have $g(u) = 0$ and so

$$g(x) = g(u+v) = g(u) + g(v) = g(v) = g\big(\sum_{i=1}^{n} f_i(x) v_i\big) = \sum_{i=1}^{n} f_i(x) g(v_i) = \big(\sum_{i=1}^{n} g(v_i) f_i\big)(x).$$

Since $g(x) = \big(\sum_{i=1}^{n} g(v_i) f_i\big)(x)$ for all $x \in V$ it follows that $g = \sum_{i=1}^{n} g(v_i) f_i$, as claimed.

6: Let a, b and c be positive real numbers. Let E be the ellipsoid $\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1$ in $\mathbf{R}^3$. Let $u,v,w\in E$ be such that the set $\{u,v,w\}$ is orthogonal. Show that the distance from the origin to the plane through u, v and w does not depend on the choice of u, v and w.

Solution: We generalize to $\mathbf{R}^n$. Let $a_1,a_2,\cdots,a_n>0$ and let E be the ellipsoid in $\mathbf{R}^n$ given by $\sum\limits_{i=1}^n\frac{{x_i}^2}{{a_i}^2}=1$. Let $\mathcal{U}=\{u_1,u_2,\cdots,u_n\}$ be an orthogonal set with each $u_i\in E$. Let P be the hyperplane through all of the points u_i. We have $P=u_1+U$ where $U=\text{Span}\{u_2-u_1,u_3-u_1,\cdots,u_n-u_1\}$, that is

$$P=\Big\{u_1+\sum_{k=2}^n t_k(u_k-u_1)\Big|t_k\in\mathbf{R}\Big\}=\Big\{\sum_{i=1}^n t_iu_i\Big|t_i\in\mathbf{R}\,,\ \sum_{i=1}^n t_i=1\Big\}.$$

Let x be the point in P nearest to the origin. Note that x is the (unique) point in $P\cap U^\perp$. Since $x\in U^\perp$ we have $x\bullet(u_k-u_1)=0$ so that $x\bullet u_k=x\bullet u_1$ for all $k\geq 2$. Let $c=x\bullet u_1$ so that we have $x\cdot u_k=c$ for all $k\geq 1$. Since $x\in P$, we can write $x=\sum\limits_{i=1}^n t_iu_i$ with $\sum\limits_{i=1}^n t_i=1$. Since $\mathcal{U}$ is orthogonal, the coefficients are given by $t_i=\frac{x\bullet u_i}{|u_i|^2}=\frac{c}{|u_i|^2}$. Since $\sum\limits_{i=1}^n t_i=1$, this gives $c=\Big(\sum\limits_{i=1}^n\frac{1}{|u_i|^2}\Big)^{-1}$. Thus the distance from the origin to P is

$$|x|=\Big|\sum_{i=1}^n t_iu_i\Big|=\sqrt{\sum_{i=1}^n {t_i}^2|u_i|^2}=\sqrt{\sum_{i=1}^n\frac{c^2}{|u_i|^2}}=\sqrt{c^2\cdot\frac{1}{c}}=\sqrt{c}=\Big(\sum_{i=1}^n\frac{1}{|u_i|^2}\Big)^{-1/2}.$$

Let A be the matrix with columns $\frac{u_i}{|u_i|}$, that is $A=\Big(\frac{u_1}{|u|_1},\frac{u_2}{|u_2|},\cdots,\frac{u_n}{|u_n|}\Big)\in M_n(\mathbf{R})$ and let D be the diagonal matrix $D=\text{diag}\Big(\frac{1}{{a_1}^2},\frac{1}{{a_2}^2},\cdots,\frac{1}{{a_n}^2}\Big)$. For each index k, since $u_k\in E$ we have ${u_k}^T D\,u_k=\sum\limits_{i=1}^n\frac{{u_{ki}}^2}{{a_i}^2}=1$ and so the diagonal entries of the matrix $A^TD\,A$ are given by

$$\big(A^TD\,A\big)_{k,k}=\Big(\frac{u_k}{|u_k|}\Big)^TD\Big(\frac{u_k}{|u_k|}\Big)=\frac{1}{|u_k|^2}.$$

Since the columns of A form an orthonormal basis for $\mathbf{R}^n$ we have $A^TA=I$ and so

$$\sum_{i=1}^n\frac{1}{|u_i|^2}=\text{trace}\big(A^TD\,A\big)=\text{trace}(D)=\sum_{i=1}^n\frac{1}{{a_i}^2}.$$

Thus the distance from the origin to P is

$$|x|=\Big(\sum_{i=1}^n\frac{1}{|u_i|^2}\Big)^{-1/2}=\Big(\sum_{i=1}^n\frac{1}{{a_i}^2}\Big)^{-1/2}$$

which is independent of the choice of $u_1,u_2,\cdots,u_n$.