Problems

Let p be a prime greater than 3. Prove that there exist integers $a_1, a_2, \ldots, a_n$ with

$$-\frac{p}{2} < a_1 < a_2 < \cdots < a_n < \frac{p}{2}$$

such that

$$\frac{(p - a_1)(p - a_2) \cdots (p - a_n)}{|a_1 a_2 \cdots a_n|}$$

is a perfect power of 3.

(**Source:** *2007 MOSP Tests Edited by Zuming Feng, Practice Test 8, Problem 1*)
10/23/2017

The ordering of the a_i is unimportant, as we can just re-label at the end, so drop this condition (we just need the a_i to be distinct and within the given range). Since $p > 3$ is prime, either $3 \mid p + 1$ or $3 \mid p - 1$. In the first case, set $b_1 = -1$ and in the second case set $b_1 = 1$. For $i \geq 1$, construct b_{i+1} as follows, having constructed b_i such that $3 \nmid b_i$, $3 \mid p - b_i$, and $-\frac{p}{2} < b_i < \frac{p}{2}$.

Let c_i be such that $3^{d_i} c_i = p - b_i$, where $v_3(p - b_i) = d_i$ (i.e. $3 \nmid c_i$). $d_i \geq 1$ and $\frac{p}{2} < p - b_i < \frac{3p}{2}$ so $0 < c_i < \frac{p}{2}$. As $3 \nmid c_i$, either $3 \mid p + c_i$ or $3 \mid p - c_i$ (like above). In the first case, set $b_{i+1} = -c_i$ and in the second case set $b_{i+1} = c_i$. (From the way b_1 was defined, $c_0 = 1$.)

Having constructed the b_i in this way, there will exist some smallest $j \geq 2$ such that $b_j = b_k$ for some $k < j$ (i.e. we will enter a cycle, possibly pure), since all b_i are drawn from the finite set $\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\}$. Set $a_1 = b_k, a_2 = b_{k+1}, \ldots, a_{j-k} = b_{j-1}$. By minimality of j, these a_i are distinct, lie in the range, and give the above product as:

$$
\begin{aligned}
\frac{(p - a_1)(p - a_2) \cdots (p - a_n)}{|a_1 a_2 \cdots a_n|} &= \frac{3^{d_k} c_k}{c_{k-1}} \cdot \frac{3^{d_{k+1}} c_{k+1}}{c_k} \cdot \;\cdots\; \cdot \frac{3^{d_{j-1}} c_{j-1}}{c_{j-2}} \\
&= \frac{3^{d_k + d_{k+1} + \cdots + d_{j-1}} c_{j-1}}{c_{k-1}} \\
&= \frac{3^{d_k + d_{k+1} + \cdots + d_{j-1}} c_{k-1}}{c_{k-1}} \\
&= 3^{d_k + d_{k+1} + \cdots + d_{j-1}}
\end{aligned}
$$

So this choice of a_is satisfies all conditions.

Let n and k be integers with $0 \leq k < \frac{n}{2}$. Initially, let A be the sequence of subsets of $\{1, 2, \ldots, n\}$ with exactly k elements, and B the sequence of subsets of $\{1, 2, \ldots, n\}$ with exactly $k+1$ elements, both arranged in lexicographic (dictionary) order. Now let S be the first element in A. If there is a T in B such that $S \subseteq T$, remove S from A and the first such T from B, and repeat this process as long as A is nonempty; otherwise, stop. Prove that this process terminates with A empty.

For $C \in \mathcal{P}([n])$ and $i \in [n]$, define $g_i(C)$ to be the number of elements of $[n]$ contained in C among $\{n-i+1, n-i+2, \ldots, n\}$ minus the number of elements of $[n]$ not contained in C among $\{n-i+1, n-i+2, \ldots, n\}$.

Now assume $C \in \binom{[n]}{k}$. Define $h : \binom{[n]}{k} \to \binom{[n]}{k+1}$ by setting $h(C)$ to the union of C and the largest $i' \in [n]$ such that $g_{i'}(C) = \min_{i \in [n]} g_i(C)$. This is well-defined (i.e. $i' \notin C$) since if the minimum is attained at $m = g_{i'}(C)$ where $i' \in C$ and $i' < n$, then $g_{i'+1}(C) = m - 1$, a contradiction. If the minimum is attained at $i' = n$ with $n \in C$, then the minimum is $m = g_n(C) = 1$, a contradiction since $g_1(C) \leq -1 < 1$.

Define $f : \binom{[n]}{k} \to \binom{[n]}{k+1}$ to be such that $f(C) = D$ where D is the set removed from $\binom{[n]}{k+1}$ in the operation from the problem, if possible. Otherwise, make $f(C)$ undefined. We claim that f is always defined and furthermore, we claim that $f(C) = h(C)$, which we prove by induction on C under the lexicographic ordering of $\binom{[n]}{k}$. As a base case, $f([k]) = [k+1]$ while the minimum of $g_i([k])$ is attained solely at $i = k+1$ with $g_{k+1}([k]) = -(n-k)$ so $h([k]) = [k+1]$.

Now consider arbitrary $C \in \binom{[n]}{k}$ and assume that for all $D \in \binom{[n]}{k}$ with $D < C$, $f(D)$ is well-defined and equal to $h(D)$. Assume that the largest index where the minimum value of $g_i(C)$ occurs is at r with $g_r(C) = m$. As proven above, $r \notin C$ so we claim that $f(C) = C \cup \{r\}$.

Lemma 1. *$C \cup \{r\}$ is available in sequence B under the operation described in the problem when we reach C in sequence A.*

Proof. If $C \cup \{r\}$ were not available at this point, then $f(D) = C \cup \{r\}$ for some $D < C$. Since $C \cup \{r\}$ must also be attained from D by adding some element, D is of the form $(C \cup \{r\}) \setminus \{j\}$ for some $j > r$ with $j \in C$. Notice that for $i \leq r$ and $i > j$, $g_i(C) = g_i((C \cup \{r\}) \setminus \{j\})$ while for $r < i \leq j$, $g_i((C \cup \{r\}) \setminus \{j\}) = g_i(C) - 2$.

Let $m = \min_{i \in [n]} g_i(C)$ and $m' = \min_{i \in [n]} g_i((C \cup \{r\}) \setminus \{j\})$. By definition of j, $m' = g_j((C \cup \{r\}) \setminus \{j\}) = g_j(C) - 2 \geq (m+1) - 2 = m - 1$. Meanwhile, $m' \leq g_{r+1}((C \cup \{r\}) \setminus \{j\}) = $

$g_r((C \cup \{r\}) \setminus \{j\}) - 1 = g_r(C) - 1 = m - 1$. Thus $m' = m - 1$.

Then $m - 1 = g_j((C \cup \{r\}) \setminus \{j\}) = g_j(C) - 2$. Since $j \in C$, if $j \neq n$, then $g_{j+1}(C) = g_j(C) - 1 = m$, contradicting the fact that the largest index for which m is attained by $g_i(C)$ is at $i = r < j$. Otherwise, $j = n$ and $m' = -1$, so that $m = 0$, again a contradiction since $g_1(C) \leq -1$.

$\square$

Lemma 2. *For all $s < r$ with $s \notin C$, $C \cup \{s\}$ is unavailable in sequence B under the operation described in the problem when we reach C in sequence A.*

Proof. We will show that for each such $C \cup \{s\}$, there exists $D < C$ such that $f(D) = C \cup \{s\}$. Let $m'' = min_{i \in [n]} g_i(C \cup \{s\})$ and let j be the smallest index at which m'' is attained. Since $s < r$, for $i > s$, $g_i(C) = g_i(C \cup \{s\})$. In particular, for $i > r$, $g_i(C \cup \{s\}) > m$ and $g_r(C \cup \{s\}) = m$. Thus $m'' \leq m$ and m'' is attained last at some $t \leq r$. Since $g_i(C) = g_i(C \cup \{s\})$ for $i > s$ and $s < r$, $max_{i \in \{s+1,\dots,n\}} g_i(C) = m$. Since $g_i(C \cup \{s\}) = g_i(C) + 2$ for $i \leq s$, it follows that $m'' = m$. Thus, since $g_i(C) \geq m$ always, $g_1(C \cup \{s\}) \geq m + 2 = m'' + 2 > m''$, i.e. $t > 1$.

We then claim that $t - 1 \in C \cup \{s\}$, $t - 1 \neq s$, $(C \cup \{s\}) \setminus \{t - 1\} < C$ and that $f((C \cup \{s\}) \setminus \{t - 1\}) = C \cup \{s\}$.

First, since $m'' = m$ is minimal and attained at $i = t$, $g_{t-1}(C \cup \{s\}) = 1 + g_t(C \cup \{s\})$, implying that $t - 1 \in C \cup \{s\}$ (since g_i increases by 1 from t to $t - 1$ rather than decreasing by 1). Since $m'' = m$, $t > s$. Furthermore, since $g_i(C \cup \{s\}) \geq m + 2$ for $i \leq s$ and $g_t(C \cup \{s\}) = t$, then $t - 1 > s$ since g_i only ever increases or decreases by 1 between consecutive values of i. Since $t - 1 > s$, $(C \cup \{s\}) \setminus \{t - 1\} < C$.

Further, $g_i((C \cup \{s\}) \setminus \{t - 1\}) = g_i(C) \geq m$ for $i > t$. Then $g_{t-1}((C \cup \{s\}) \setminus \{t - 1\}) = m - 1$ and $g_i((C \cup \{s\}) \setminus \{t - 1\}) = g_i(C) - 2 \geq (m + 1) - 2 = m - 1$ for $s < i \leq t - 1$. For $i \leq s$, $g_i((C \cup \{s\}) \setminus \{t - 1\}) = g_i(C) \geq m$. Thus, $min_{i \in [n]} g_i((C \cup \{s\}) \setminus \{t - 1\}) = m - 1$ and the largest index at which it is attained is $t - 1$. Thus, by the induction hypothesis, $f((C \cup \{s\}) \setminus \{t - 1\}) = h((C \cup \{s\}) \setminus \{t - 1\}) = C \cup \{s\}$.

Meanwhile, $g_t((C \cup \{s\}) \setminus \{t\}) = g_i(C) - 2$ for using the induction hypothesis, $f((C \cup \{s\}) \setminus \{t\})$.

$\square$

Lemmas 1 and 2 together imply that $f(C) = C \cup \{r\}$, completing the induction.

Steve is piling $m \geq 1$ indistinguishable stones on the squares of an $n \times n$ grid. Each square can have an arbitrarily high pile of stones. After he finishes piling his stones in some manner, he can then perform stone moves, defined as follows. Consider any four grid squares which are corners of a rectangle, i.e. in positions $(i,k), (i,l), (j,k), (j,l)$ for some $1 \leq i, j, k, l \leq n$, such that $i < j$ and $k < l$. A stone move consists of either removing one stone from each of (i,k) and (j,l) and moving them to (i,l) and (j,k) respectively, or removing one stone from each of (i,l) and (j,k) and moving them to (i,k) and (j,l) respectively.

Two ways of piling the stones are equivalent if they can be obtained from one another by a sequence of stone moves.

How many different non-equivalent ways can Steve pile the stones on the grid?

(Source: *2015 USAMO, Problem 4*) 1/7/2018

For a rectangular grid, let R_i denote the i-th row and C_j denote the j-th column. Furthermore, for a stone piling on a grid, let $s(R_i)$ denote the sum of the number of stones in all cells in R_i and let $s(C_j)$ denote the sum of the number of stones in all cells in C_j.

Lemma 3. *For any set of operations on an $a \times b$ grid G with some initial distribution of m stones, each row sum and each column sum remains invariant.*

Proof. Consider moving a stone from each of (i,k) and (j,l) to (i,l) and (j,k). It is clear that $s(R_t)$ and $s(C_u)$ are unchanged for $t \neq i, j$ and $u \neq k, l$. Since one stone is removed from (i,k) and given to (i,l), $s(R_i)$ remains the same. A similar analysis shows that $s(R_j)$, $s(C_k)$ and $s(C_l)$ remain the same.

$\square$

Lemma 4. *For any two rectangular $a \times b$ grids $G^{(1)}$ and $G^{(2)}$ each distributing m stones such that $\forall i, 1 \leq i \leq a, s(R_i^{(1)}) = s(R_i^{(2)})$ and $\forall j, 1 \leq j \leq b, s(C_j^{(1)}) = s(C_j^{(2)})$, then $G^{(1)}$ and $G^{(2)}$ are equivalent.*

Proof. Induct on $a + b$. When $a = b = 1$ (and whenever one of a or b is 1), there is only one grid matching given constraints on all row and column sums. Assume the claim holds for $a + b = k$ with $k \geq 2$ and consider an instance when $a + b = k + 1$. We will transform $G^{(1)}$ into $G^{(2)}$. Let the number of stones at (i,j) in $G^{(1)}$ currently be $c_{i,j}$ and in $G^{(2)}$ currently be $d_{i,j}$. Consider R_a. If there exists j such that $c_{a,j} < d_{a,j}$, then since $\sum_{p=1}^{b} c_{a,p} = \sum_{p=1}^{b} d_{a,p}$, there exists k such that $c_{a,k} > d_{a,k}$. Similarly, there exists q such that $c_{q,j} > d_{q,j}$. Thus, we can move stones from (q,j) and (a,k) to (q,k) and (a,j) in $G^{(1)}$. We proceed likewise for when $c_{a,j} > d_{a,j}$.

This process can be continued while there exists j such that $c_{a,j} \neq d_{a,j}$. Thus, when it terminates, $\forall j, c_{a,j} = d_{a,j}$ in grid $G^{(1)}$. By induction, we can then transform the grid composed of the first $a-1$ rows of $G^{(1)}$ into the first $a-1$ rows of $G^{(2)}$ without disturbing the identical a-th row.

$\square$

Lemma 5. *For an $n \times n$ grid G and any choice of $s(R_1), s(R_2), \ldots, s(R_n), s(C_1), s(C_2), \ldots, s(C_n)$ such that $\sum_{i=1}^{n} s(R_i) = \sum_{i=j}^{n} s(C_j) = m$, there exists a distribution of stones on the grid matching these row and column sums.*

Proof. Begin at the upper left corner of the grid. If $s(R_1) > s(C_1)$, place $s(C_1)$ stones at $(1,1)$ and move to $(2,1)$ while decrementing $s(R_1)$ by $s(C_1)$. If $s(R_1) < s(C_1)$, place $s(R_1)$ stones at $(1,1)$ and move to $(2,1)$ while decrementing $s(C_1)$ by $s(R_1)$. If $s(R_1) = s(C_1)$, then place $s(R_1)$ stones at $(1,1)$ and move to $(2,2)$. Continue this process until reaching the final row or column, at which point the algorithm will end naturally and meet the given conditions on row and column sums.

$\square$

The above three lemmas together imply that the number of non-equivalent arrangements is given by the number of ways to distribute m items among n rows times the same number of distributions for columns, which is then $\binom{m+n-1}{m}^2$.

Note: The algorithm used in the third lemma is based on the idea of the "Northwest Corner" rule for the "Transportation Problem" in Operations Research.

Let $X_1, X_2, \ldots, X_{100}$ be a sequence of mutually distinct nonempty subsets of a set S. Any two sets X_i and X_{i+1} are disjoint and their union is not the whole set S, that is, $X_i \cap X_{i+1} = \varnothing$ and $X_i \cup X_{i+1} \neq S$, for all $i \in \{1, \ldots, 99\}$. Find the smallest possible number of elements in S.

(Source: *2016 USAMO, Problem 1*) 1/11/2018

The smallest possible size of S is 8. If $|S| \leq 6$ then there could only be at most 63 nonempty subsets of S, which is not enough. If $|S| = 7$, then no subsets of S of size 6 could be used because any consecutive set would have to either intersect such a subset or be a singleton whose union with the subset is all of S. Similarly, any neighbors of a subset T of size 5 must have only one element so at most 8 subsets of size 5 can appear. Likewise, any subset T of size 4 can only have neighbors of size 1 or 2 so at most $1 + \binom{7}{1} + \binom{7}{2} = 29$ subsets of size 4 can appear. So together there are at most $29 + 8 = 37$ subsets of size 4 or 5.

However, the first upper bound assumes that $|X_1| = |X_{100}| = 5$ and the second upper bound assumes that $|X_1| = |X_{100}| = 4$, which cannot both happen so there are really only at most 36 subsets of size 4 or 5. Together with subsets of size $1, 2,$ and 3, this gives at most $\binom{7}{1} + \binom{7}{2} + \binom{7}{3} + 36 = 99$ subsets, a contradiction.

So $|S| \geq 8$. We give a recursive construction for a sequence Y_n consisting of $2^{n-1} + 1$ subsets of $[n]$ which meet the adjacency conditions given. With $n = 8$, this gives more than enough subsets.

Given a construction for Y_n, we construct Y_{n+1} as follows. Let $Y_n^{(1)}$ be the result of adding $n + 1$ to each odd indexed subset in Y_n, then remove the final set. Let $Y_n^{(2)}$ be the result of adding $n + 1$ to each even indexed subset in Y_n. Since Y_n met the adjacency conditions, it follows that $Y_n^{(1)}$ and $Y_n^{(2)}$ do as well since each adjacent pair remains disjoint and with union missing some element from $[n+1]$. Now take Y_{n+1} as $Y_n^{(1)}$ with $\{n+1\}$ appended to the end of the sequence and then followed by $Y_n^{(2)}$ appended to the end of that sequence. Since $[n]$ could not have appeared in Y_n, $\{n+1\}$ is disjoint from its neighbors and does not form a union of $[n+1]$.

Run this approach recursively, beginning with:

$$Y_4 = \{\{1, 2\}, \{4\}, \{1, 3\}, \{2\}, \{1, 4\}, \{3\}, \{2, 4\}, \{1\}, \{3, 4\}\}$$

Prove that there exists an infinite set of points

$$\ldots, P_{-3}, P_{-2}, P_{-1}, P_0, P_1, P_2, P_3, \ldots$$

in the plane with the following property: For any three distinct integers, a, b, and c, points P_a, P_b, and P_c are collinear if and only if $a + b + c = 2014$.

(Source: *2014 USAMO, Problem 3*) 1/14/2018

For $n \in \mathbb{Z}$, set $P_n = (n, n^3 - 2014n^2)$.

($\Leftarrow$): If $a + b + c = 2014$, then $(x - a)(x - b)(x - c) = x^3 - 2014x^2 + (ab + bc + ca)x - abc$. So at $x = a, b, c$:

$$0 = x^3 - 2014x^2 + (ab + bc + ca)x - abc$$
$$\implies x^3 - 2014x^2 = (-ab - bc - ca)x + abc$$

Thus, P_a, P_b, P_c all lie on the line $f(x) = (-ab - bc - ca)x + abc$.

($\Rightarrow$): If three points P_a, P_b, and P_c all lie on a line $f(x) = dx + e$, then $x = a, b, c$ all satisfy the equation: $x^3 - 2014x^2 = dx + e$ meaning that a, b, c are the three solutions to $x^3 - 2014x^2 - dx - e = 0$ and $a + b + c = 2014$ by Vieta's theorem.

Let a, b, c, d, e be distinct positive integers such that $a^4 + b^4 = c^4 + d^4 = e^5$. Show that $ac + bd$ is a composite number.

(Source: *2015 USAMO, Problem 5*) 1/19/2018

$$a^4 c^4 - b^4 d^4 = (e^5 - b^4)c^4 - b^4(e^5 - c^4) \tag{1}$$
$$= e^5 c^4 - b^4 c^4 - b^4 e^5 + b^4 c^4 \tag{2}$$
$$= e^5(c^4 - b^4) \tag{3}$$
$$\implies (a^2 c^2 + b^2 d^2)(ac + bd)(ac - bd) = e^5(c^2 + b^2)(c + b)(c - b) \tag{4}$$

If $2 \mid ac, bd$ then since a, b, c, d are positive, $ac + bd$ is composite. If both of ac and bd are odd, then a, b, c, d are all odd and $e^5 \equiv a^4 + b^4 \equiv c^4 + d^4 \equiv 2 \pmod{16}$ since $(2k+1)^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1 \equiv 8k(k+1) + 1 \equiv 1 \pmod{16}$. However, if $e^5 \equiv 2 \pmod{16}$, then $2 \mid e$, so that $e^5 \equiv 0 \pmod{16}$, a contradiction. So 2 divides exactly one of ac and bd and in particular, $2 \nmid ac - bd, a^2 c^2 - b^2 d^2$.

Notice:

$$\gcd(a^2 c^2 + b^2 d^2, a^2 c^2 - b^2 d^2) = \gcd(2b^2 d^2, a^2 c^2 - b^2 d^2)$$
$$= \gcd(b^2 d^2, a^2 c^2 - b^2 d^2)$$
$$= \gcd(b^2 d^2, a^2 c^2)$$

where the second equality follows from the fact that $2 \nmid a^2 c^2 - b^2 d^2$. Any prime q divides each of $a^2 c^2$ and $b^2 d^2$, then it also divides $ac + bd$, which again implies that $ac + bd$ is composite since a, b, c, d are positive. Then we can assume that $\gcd(a^2 c^2 + b^2 d^2, a^2 c^2 - b^2 d^2) = \gcd(b^2 d^2, a^2 c^2) = 1$, i.e. $a^2 c^2 + b^2 d^2$ and $a^2 c^2 - b^2 d^2$ are relatively prime. Through a similar argument, $ac + bd$ and $ac - bd$ are relatively prime as well.

Now assume that $p = ac + bd$ is prime. From the last paragraph, $p \nmid a^2c^2 + b^2d^2, ac - bd$. Recall equation (4) above. If $p \mid e^5$, then $p \mid e^5$ so $p^5 \mid e^5$. Since the only factor on the LHS divisible by p is $ac+bd$ (itself p), then $p^5 \mid ac+bd = p$, a contradiction. Thus $p = ac+bd \mid (c^2+b^2)(c+b)(c-b)$.

If $p \mid c+b$, then $ac+bd \leq c+b < ac+bd$, a contradiction since a, b, c, d are distinct positive integers. Likewise, $p \nmid c - b$. Thus, $p \mid c^2 + b^2$.

Notice:

$$(b^2 + c^2)(a^2 + d^2) = (ac + bd)^2 + (ab - cd)^2$$

So $p \mid |ab - cd|$. If $ab = cd$, then $(b^2 + c^2)(a^2 + d^2) = p^2$ and since a, b, c, d are positive, then $b^2 + c^2 = a^2 + d^2 = p$. Then $\gcd(b, c) = \gcd(a, d) = 1$ and $c \mid a$ and $a \mid c$, implying that $a = c$, a contradiction.

So $|ab - cd| > 0$. WLOG, $ab > cd$ so $ac, bd < p = ac + bd \leq ab - cd < ab \Rightarrow c < b$ and $d < a$. Then $c^4 + d^4 < b^4 + a^4$, a final contradiction.

Notes: Very helpful first identity involving $a^4c^4 - b^4d^4$; involved a lot of difficult steps to get right; looks like e^5 could have been replaced by any integer exponent at least 2.

Integers n and k are given, with $n \geq k \geq 2$. You play the following game against an evil wizard.

The wizard has $2n$ cards; for each $i = 1, \ldots, n$, there are two cards labeled i. Initially, the wizard places all cards face down in a row, in unknown order.

You may repeatedly make moves of the following form: you point to any k of the cards. The wizard then turns those cards face up. If any two of the cards match, the game is over and you win. Otherwise, you must look away, while the wizard arbitrarily permutes the k chosen cards and then turns them back face-down. Then, it is your turn again.

We say this game is winnable if there exist some positive integer m and some strategy that is guaranteed to win in at most m moves, no matter how the wizard responds.

For which values of n and k is the game winnable?

(Source: *2016 USAMO, Problem 6*) 1/23/2018

For $n \geq k+1$, the game is winnable. Call the card positions $P_1, P_2, \ldots, P_{2n}$. If we choose the cards initially in positions $P_1, P_2, \ldots, P_k$ and do not win, then select the cards in positions $P_2, P_3, \ldots, P_{k+1}$. We can then see from the cards which turn up at $P_2, P_3, \ldots, P_k$ which one is currently in P_1 by comparing to the set of cards turned up on the first turn. If we have not one, we can then select the cards at positions $P_3, P_4, \ldots, P_{k+2}$ and similarly learn the identity of the card at P_2. Continue in this way until after selecting the cards at $P_{2n-k+1}, \ldots, P_{2n}$ (or earlier if we coincidentally find a match).

We now know the identity of the cards at positions $P_1, P_2, \ldots, P_{2n-k}$. For $n \geq k+1$, $2n-k \geq n+1$ so by the pigeon hole principle we know the positions of two cards with the same numbering and can select a group of k containing them.

For $n = k$, the game is not winnable. After making a first move, it is possible that we get exactly one card each having $1, 2, \ldots, k$, so that the other k cards also have $1, 2, \ldots, k$. We can then identify k positions containing one each of cards labeled $1, 2, \ldots, k$ (so that the same is true of the other k cards) but we cannot tell anything more about the specific cards. Call this state of knowledge state S. We will show that after any move, it is possible that we remain in state S of knowledge.

Indeed, if at some point we have not won and we are in state S of knowledge, then assume that we choose $0 \leq m \leq k$ card positions from our last selection and $k - m$ card positions from among the other card positions. Since the last selection positions now have one each of $1, 2, \ldots, k$ as do the other k positions, it is possible that we choose $1, 2, \ldots, m$ from among positions in the last selection and $m+1, m+2, \ldots, k$ from among positions not in the last selection, so we are back in state S.

Note: Simple problem for a #6.

Find the least natural number n ($n \geq 3$) with the following property: for any coloring in 2 colors of n distinct collinear points $A_1, A_2, \ldots, A_n$ there exist three points A_i, A_j, A_{2j-i}, $1 \leq i < 2j - i \leq n$ which are colored in the same color.

(Source: *Bulgaria 1998, Problem 1*) 1/24/2018

The least such n is 9. This essentially asks for the smallest n with a monochromatic three-term arithmetic progression. For $n = 8$, color $[8]$ as follows. All values that are 1 or 2 (mod 4) are

colored red and all values that are 3 or 0 (mod 4) are colored blue. Any arithmetic progression with difference of 1, 2, or 3 cannot have all terms in $\{1, 2\}$ (mod 4) or in $\{3, 0\}$ (mod 4) since 1 and 3 are relatively prime to 4 and any two numbers two apart are differently colored. Furthermore, a common difference of 4 or more is impossible since the first and last term would have to have a difference of 8.

For $n < 8$, take the first n terms of the above described sequence.

It can be shown that all 2-colorings of [9] must contain an arithmetic progression by assuming WLOG that 1 is colored red and then taking the 8 cases for colorings of $4, 5, 6$, all of which fully and contradictorily determine the rest of the coloring.

Let $\mathbb{R}^+$ be the set of positive real numbers. Prove that there does not exist a function $f : \mathbb{R}^+ \to \mathbb{R}^+$ such that

$$(f(x))^2 \geq f(x + y)(f(x) + y)$$

for every $x, y \in \mathbb{R}^+$.

(Source: *Bulgaria 1998, Problem 3*) 1/24/2018

We assume for contradiction that such f exists. Since $f(x) + y > 0$, we can divide through by this on both sides as follows:

$$(f(x))^2 \geq f(x + y)(f(x) + y)$$
$$\implies f(x + y) \leq \frac{(f(x))^2}{f(x) + y}$$
$$= f(x) - y + \frac{y^2}{f(x) + y}$$

$f(x) + y > y \Rightarrow f(x) - y + \frac{y^2}{f(x)+y} < f(x) - y + y = f(x)$ so $f(x + y) < f(x)$ for any $y > 0$, i.e. f is a strictly decreasing function.

Take $y = f(x)$ in the original inequality:

$$((f(x))^2 \geq f(x + f(x))(2f(x)) \tag{5}$$

$$\implies f(x + f(x)) \leq \frac{1}{2}f(x) \tag{6}$$

where we were able to divide through by $f(x)$ to get (6) since $f(x) > 0$ for all $x \in \mathbb{R}^+$.

Let $f(1) = a$. Then $f(1 + a) \leq \frac{1}{2}a$. We claim that for all integers $n \geq 0$:

$$f\left(1 + \sum_{i=0}^{n} \frac{1}{2^i}a\right) \leq \frac{1}{2^{n+1}}a$$

We proceed by induction on n. The case of $n = 0$ was just show, following from (6). Now assume that $f(1 + \sum_{i=0}^{k} \frac{1}{2^i}a) \leq \frac{1}{2^{k+1}}a$ for some $k \geq 0$. Then from (6):

$$f\left(1 + \sum_{i=0}^{k} \frac{1}{2^i}a + f\left(1 + \sum_{i=0}^{k} \frac{1}{2^i}a\right)\right) \leq \frac{1}{2}f\left(1 + \sum_{i=0}^{k} \frac{1}{2^i}a\right) \tag{7}$$

$$\leq \frac{1}{2^{k+2}}a \tag{8}$$

Since f is decreasing and $1 + \sum_{i=0}^{k} \frac{1}{2^i}a + f(1 + \sum_{i=0}^{k} \frac{1}{2^i}a) \leq 1 + \sum_{i=0}^{k+1} \frac{1}{2^i}a$, it follows that $f(1 + \sum_{i=0}^{k+1} \frac{1}{2^i}a)$ is less than or equal to the LHS of (7) so $f(1 + \sum_{i=0}^{k+1} \frac{1}{2^i}a) \leq \frac{1}{2^{k+2}}a$, completing the induction.

Now assume that $f(1 + 2a) = b > 0$. Then there exists positive integral n such that $\frac{1}{2^{n+1}}a < b$, so that $f(1 + \sum_{i=0}^{n} \frac{1}{2^i}a) < b$. However, since f is decreasing, $b = f(1 + 2a) < f(1 + \sum_{i=0}^{n} \frac{1}{2^i}a)$, a contradiction.

Prove that there exists a positive integer $n < 10^6$ such that 5^n has six consecutive zeros in its decimal representation.

(Source: *2016 USAJMO, Problem 2*) 1/25/2018

Take $n = 2^{19} + 20$. $2^{10} = 1024 \Rightarrow 2^{20} = 1048576 \Rightarrow 2^{19} + 20 = 524308 < 10^6$. Notice:

$$5^n \equiv 0 \equiv 5^{20} \pmod{5^{20}} \tag{9}$$

$$5^n \equiv 5^{20} \pmod{2^{20}} \tag{10}$$

where (10) follows from Euler's Totient Theorem. It is then clear that $5^n \equiv 5^{20} \pmod{10^{20}}$. Furthermore:

$$5^{20} = \frac{10^{20}}{2^{20}} < \frac{10^{20}}{10^6} = 10^{14}$$

since $2^{10} = 1024 > 10^3$. Thus the last 20 digits of 5^n are the digits of 5^{20}, of which the leftmost 6 are 0s.

Notes: The key idea seems to have been to get the Chinese Remainder Theorem applications to work out correctly for mod 5^{20} and mod 2^{20} which worked most easily by having them both be 5^{20}, which is done for mod 2^{20} using the totient function and taking a power 5^m sufficiently smaller than 10^m.