Math 341 Homework 2 Solutions

1. Let m and n be integers and let a be a positive integer. We say $m \equiv n \pmod a$ if there is an integer t so that $m-n = ta$ (i.e. $m-n$ is divisible by a). If the statement "$m \equiv n \pmod a$" is false, we write $m \not\equiv n \pmod a$. HW1 problem 4 implies that if p is prime, then $(1+n)^p \equiv 1+n^p \pmod p$ for every positive integer n. You may use this fact to solve the problem below.
a) Using induction, prove that if p is a prime, then $n^p \equiv n \pmod p$ for every positive integer n.

Solution. For each prime p, we will prove the result by induction on n. Let p be a prime. if $n = 1$ then $n^p = 1 = n$. Now suppose the result has been proved for some positive integer n. From HW1 problem 4, we have $(1+n)^p \equiv 1+n^p \pmod p$, i.e. $(1+n)^p - (1+n^p) = tp$ for some integer t. Using the induction hypothesis, we have $n^p \equiv n \pmod p$, i.e. $n^p - n = sp$ for some integer s. Thus

$$(1+n)^p = 1 + n^p + tp = 1 + n + sp + tp = 1 + n(s+t)p,$$

which is exactly the statement $(1+n)^p \equiv 1+n \pmod p$. This completes the induction step and finishes the proof.

b) Give an example of positive integers n and a so that $n^a \not\equiv n \pmod a$.

Solution. Let $n = 3,\ a = 4$. Then $n^a - n = 78$, which is not divisible by 4. Thus $3^4 \not\equiv 3 \pmod 4$.

2. Prove that

$$\binom{2n}{n} = \frac{2^{2n}}{\sqrt{\pi n}}\Big(1 + O(\frac{1}{n})\Big).$$

(Here $\pi = 3.141...$ is a real number, not a permutation!)

Solution. First, we should understand what we are being asked to prove. From lecture, the above statement is equivalent to the following: Prove that there exists a constant C and a number N so that

$$\Big|\binom{2n}{n} - \frac{2^{2n}}{\sqrt{\pi n}}\Big| \leq \frac{C}{n}\frac{2^{2n}}{\sqrt{\pi n}} \qquad \text{for all } n \geq N. \tag{1}$$

For each positive integer n, define $f(n) = n! - \sqrt{2\pi n}(n/e)^n$. By Stirling's approximation, we know that

$$\Big|\frac{f(n)}{\sqrt{2\pi n}(n/e)^n}\Big| \leq C_0/n$$

for some absolute constant C_0 (we are calling the constant C_0 rather than C since we don't want to confuse it with the constant C from Equation (1)). Thus if $n \geq 2C_0$, we have that

$$1/2 \leq \Big|1 - \frac{f(n)}{\sqrt{2\pi n}(n/e)^n}\Big| \leq 2. \tag{2}$$

We will set $N = 2C_0$, so that Equation (2) holds for all $n \geq N$. Now lets analyze the expression in

(1). We have that whenever $n \geq 2C_0$,

$$\begin{aligned}
\Big|\binom{2n}{n} - \frac{2^{2n}}{\sqrt{\pi n}}\Big| &= \Big|\frac{(2n)!}{(n!)^2} - \frac{2^{2n}}{\sqrt{\pi n}}\Big| \\
&= \Big|\frac{\sqrt{4\pi n}(2n/e)^{2n} + f(2n)}{\big(\sqrt{2\pi n}(n/e)^n + f(n)\big)^2} - \frac{2^{2n}}{\sqrt{\pi n}}\Big| \\
&= \Big|\frac{\sqrt{4\pi n}(2n/e)^{2n}\big(1 + \frac{f(2n)}{\sqrt{4\pi n}(2n/e)^{2n}}\big)}{\big(\sqrt{2\pi n}(n/e)^n\big)^2\big(1 + \frac{f(n)}{\sqrt{2\pi n}(n/e)^n}\big)^2} - \frac{2^{2n}}{\sqrt{\pi n}}\Big| \\
&= \Big|\frac{2^{2n}}{\sqrt{\pi n}}\frac{1 + \frac{f(2n)}{\sqrt{4\pi n}(2n/e)^{2n}}}{\big(1 + \frac{f(n)}{\sqrt{2\pi n}(n/e)^n}\big)^2} - \frac{2^{2n}}{\sqrt{\pi n}}\Big| \qquad (3) \\
&\leq \frac{2^{2n}}{\sqrt{\pi n}}\Big|\frac{1 + C_0/(2n)}{1 - C_0/n} - 1\Big| \\
&= \frac{2^{2n}}{\sqrt{\pi n}}\frac{3C_0/(2n)}{1 - C_0/n} \\
&\leq \frac{3C_0}{n}\frac{2^{2n}}{\sqrt{\pi n}}
\end{aligned}$$

Thus (1) holds with $N = 2C_0$ and $C = 3C_0$.

3. Let n be a positive integer. Prove that for every $\pi \in S_n$, there is a positive integer t so that $\pi^t = e$, where e is the identity permutation.

(Here π is a permutation, not the real number 3.141...!)

Food for thought: If n is fixed, what is the largest t can be? Can you come up with an interesting bound on the size of t?

Solution. Let $\pi \in S_n$. Consider the list of $n! + 1$ permutations $\pi, \pi^2, \pi^3, \ldots, \pi^{n!+1}$. We proved in class that $|S_n| = n!$. Thus by the pigeonhole principle, two of the permutations from the above list must be the same, i.e. there exist integers u and v, with $1 \leq u < v \leq n! + 1$ with $\pi^u = \pi^v$. Thus $e = \pi^u\pi^{-u} = \pi^v\pi^{-u} = \pi^{v-u}$. Define $t = v - u$. $u < v$, $t \geq 1$.

Vectors and the symmetric group

For the next set of questions, we will have the following setup.

Let n be a positive integer and let $v_1, \ldots, v_n$ be vectors in $\mathbb{R}^n$. We'll use the notation

$$\begin{aligned}
v_1 &= (v_{1,1}, v_{1,2}, \ldots, v_{1,n}), \\
v_2 &= (v_{2,1}, v_{2,2}, \ldots, v_{2,n}), \\
&\vdots \\
v_n &= (v_{n,1}, v_{n,2}, \ldots, v_{n,n}).
\end{aligned}$$

Consider the following function, whose input is n vectors and whose output is a real number:

$$f(v_1, \ldots, v_n) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{j=1}^{n} v_{j\pi,j}. \qquad (4)$$

(Recall our notation from class that if $\pi \in S_n$ and $j \in [n]$, then $j\pi$ is the integer obtained by applying the permutation π to the integer j. We will define $\mathrm{sgn}(\pi)$ in class on Jan 30.)

For example, if $n = 2$ then S_2 is the set containing the permutations $\pi_1 = e$ and $\pi_2 = (1,2)$. We have $\mathrm{sgn}(\pi_1) = 1$ and $\mathrm{sgn}(\pi_2) = -1$. Thus, if $v_1 = (v_{1,1}, v_{1,2})$ and $v_2 = (v_{2,1}, v_{2,2})$, then

$$f(v_1, v_2) = v_{1,1}v_{2,2} - v_{2,1}v_{1,2}. \tag{5}$$

4. Let $n = 3$ and let $v_1 = (v_{1,1}, v_{1,2}, v_{1,3})$ and similarly for v_2 and v_3. Write down $f(v_1, v_2, v_3)$ explicitly as a sum of products of the numbers $v_{i,j}$, in the same style as Equation (5) above. Compare this with the formula for the determinant

$$\begin{vmatrix} v_{1,1} & v_{1,2} & v_{1,3} \\ v_{2,1} & v_{2,2} & v_{2,3} \\ v_{3,1} & v_{3,2} & v_{3,3} \end{vmatrix}$$

Are the two expressions the same?

Solution. S_3 contains 6 elements. The elements e, $(1\ 2\ 3)$, and $(1\ 3\ 2)$ have sign $+1$, while the elements $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ have sign -1. Thus

$$f(v_1, v_2, v_3) = v_{1,1}v_{2,2}v_{3,3} + v_{2,1}v_{3,2}v_{1,3} + v_{3,1}v_{1,2}v_{2,3} - v_{2,1}v_{1,2}v_{3,3} - v_{3,1}v_{2,2}v_{1,3} - v_{1,1}v_{3,2}v_{2,3}.$$

Using the co-factor expansion for the determinant, we have

$$\begin{aligned} \begin{vmatrix} v_{1,1} & v_{1,2} & v_{1,3} \\ v_{2,1} & v_{2,2} & v_{2,3} \\ v_{3,1} & v_{3,2} & v_{3,3} \end{vmatrix} &= v_{1,1} \begin{vmatrix} v_{2,2} & v_{2,3} \\ v_{3,2} & v_{3,3} \end{vmatrix} - v_{1,2} \begin{vmatrix} v_{2,1} & v_{2,3} \\ v_{3,1} & v_{3,3} \end{vmatrix} + v_{1,3} \begin{vmatrix} v_{2,1} & v_{2,2} \\ v_{3,1} & v_{3,2} \end{vmatrix} \\ &= v_{1,1}(v_{2,2}v_{3,3} - v_{2,3}v_{3,2}) - v_{1,2}(v_{2,1}v_{3,3} - v_{2,3}v_{3,1}) + v_{1,3}(v_{2,1}v_{3,2} - v_{2,2}v_{3,1}) \\ &= v_{1,1}v_{2,2}v_{3,3} - v_{1,1}v_{2,3}v_{3,2} - v_{1,2}v_{2,1}v_{3,3} + v_{1,2}v_{2,3}v_{3,1} + v_{1,3}v_{2,1}v_{3,2} - v_{1,3}v_{2,2}v_{3,1} \end{aligned}$$

These two expressions are the same.

5. Let $v_1 = (1, \ldots, 0)$, $v_2 = (0, 1, 0, \ldots, 0)$, $v_3 = (0, 0, 1, \ldots, 0)$, and in general let v_j be the vector that has a one in the j–th position and zeroes elsewhere. Prove that

$$f(v_1, \ldots, v_n) = 1.$$

Let $v_1, \ldots, v_n$ be as above. Observe that if $\pi = e$, then $\prod_{j=1}^n v_{j\pi,j} = 1 = \prod_{j=1}^n v_{j,j} = \prod_{j=1}^n 1 = 1$. If $\pi \neq e$, then there exists at least one index k with $k \neq k\pi$, and thus $v_{k\pi,k} = 0$, so $\prod_{j=1}^n v_{j\pi,j} = 0$. This means that

$$f(v_1, \ldots, v_n) = \sum_{\pi \in S_n} \mathrm{sgn}(\pi) \prod_{j=1}^n v_{j\pi,j} = 1 + \sum_{\pi \neq e} \mathrm{sgn}(\pi) \prod_{j=1}^n v_{j\pi,j} = 1 + 0 = 1.$$

6. Prove that if two of the vectors are interchanged, then the sign of f flips. More formally, prove that if $v_1, \ldots, v_n$ are vectors in $\mathbb{R}^n$, then

$$f(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -f(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n).$$

(in the above expression, each of the vectors $v_1, \ldots, v_n$ are in the same place, except the vectors v_i and v_j have switched places on the right hand side).

Hint: it might be helpful to recall the definition of $\operatorname{sgn}(\pi)$.

Let $\tilde{\pi} \in S_n$ be the transposition $\tilde{\pi} = (i\ j)$. Note that for each $\pi \in S_n$, $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\tilde{\pi}\pi)$.

Next we will make a crucial observation: if $\pi_1, \pi_2 \in S_n$, then $\pi_1 = \pi_2$ if and only if $\tilde{\pi}\pi_1 = \tilde{\pi}\pi_2$. This means that if we enumerate the elements of S_n as $S_n = \{\pi_1, \dots, \pi_{n!}\}$. Then we also have $S_n = \{\tilde{\pi}\pi_1, \dots, \tilde{\pi}\pi_{n!}\}$. In particular, this means that

$$\sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{k=1}^{n} v_{k\pi,k} = \sum_{\pi \in S_n} \operatorname{sgn}(\tilde{\pi}\pi) \prod_{k=1}^{n} v_{k\tilde{\pi}\pi,k}$$

But this is great! We have $\operatorname{sgn}(\tilde{\pi}\pi) = -\operatorname{sgn}(\pi)$, and we have $v_{k\tilde{\pi}\pi,k} = v_{k\pi,k}$, unless $k = i$ (in which case $k\tilde{\pi}\pi = j\pi$), or $k = j$ (in which case $k\tilde{\pi}\pi = i\pi$), i.e.

$$\sum_{\pi \in S_n} \operatorname{sgn}(\tilde{\pi}\pi) \prod_{k=1}^{n} v_{k\tilde{\pi}\pi,k} = -\sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{k=1}^{n} v_{k\tilde{\pi}\pi,k} = -f(v_1, \dots, v_j \dots, v_i, \dots, v_n),$$

i.e.

$$f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -f(v_1, \dots, v_j \dots, v_i, \dots, v_n),$$

as desired.

7. Let $v_1, \dots, v_n$ be vectors in $\mathbb{R}^n$. Suppose that two of the vectors are the same, i.e. $v_i = v_j$ for some $i \neq j$. Prove that

$$f(v_1, \dots, v_n) = 0.$$

Solution. This follows quickly from problem 6: we have

$$f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -f(v_1, \dots, v_j, \dots, v_i, \dots, v_n).$$

But since $v_i = v_j$, we also have

$$f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = f(v_1, \dots, v_j, \dots, v_i, \dots, v_n),$$

i.e.

$$f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -f(v_1, \dots, v_i, \dots, v_j, \dots, v_n),$$

from which it follows that $f(v_1, \dots, v_n) = 0$.

8. Let $v_1, \dots, v_n$ be vectors in $\mathbb{R}^n$, let $1 \leq j \leq n$ and let v'_j be a vector in $\mathbb{R}^n$. Prove that

$$f(v_1, \dots, v_j + v'_j, \dots, v_n) = f(v_1, \dots, v_j, \dots, v_n) + f(v_1, \dots, v'_j, \dots, v_n).$$

Solution. The main issue with this problem is that the notation is a bit tricky. In the formula (4), we need to figure out which terms of the form $v_{\pi i,i}$ are entries of v_j, i.e. for which value of i is it the case that $i\pi = j$. But we can apply π^{-1} to both sides to see that $i = j\pi^{-1}$, i.e. one of the terms in the product $v_{\pi 1,1} v_{\pi 2,2} \cdots v_{\pi n,n}$ will be of the form $v_{j,\pi^{-1}j}$, and this is the only term containing an entry from the vector v_j.

One other note on notation: We'll write the vector $v_j + v'_j$ as $(v_{j,1} + v'_{j,1},\ v_{j,2} + v'_{j,2},\ \dots,\ v_{j,n} + v'_{j,n})$. We're now ready to solve the problem. We have

$$
\begin{aligned}
&f(v_1, \ldots, v_j + v'_j, \ldots, v_n) \\
&= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) v_{1\pi,1} v_{2\pi,2} \cdots (v_{j,\pi^{-1}j} + v'_{j,\pi^{-1}j}) \cdots v_{n\pi,n} \\
&= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) v_{1\pi,1} v_{2\pi,2} \cdots v_{j,\pi^{-1}j} \cdots v_{n\pi,n} + \sum_{\pi \in S_n} \operatorname{sgn}(\pi) v_{1\pi,1} v_{2\pi,2} \cdots v'_{j,\pi^{-1}j} \cdots v_{n\pi,n} \\
&= f(v_1, \ldots, v_j, \ldots, v_n) + f(v_1, \ldots, v'_j, \ldots, v_n).
\end{aligned}
$$