Problem 2. Find all positive integers n such that $n!$ divides $(2n+1)^{2n}-1$.
(Here $n! = 1 \cdot 2 \cdot \ldots \cdot n$ is the factorial of n).

Solution. We start by observing that $2n+1$ must be a prime number. Indeed, if $2n+1 = ab$ with $1 < a \leq b$ then $a = (2n+1)/b \leq (2n+1)/2 = n + 1/2$. Thus $a \leq n$ and therefore a divides $n!$ but a does not divide $(2n+1)^{2n} - 1 = a^{2n}b^{2n} - 1$. It follows that $n!$ cannot divide $(2n+1)^{2n}-1$ if $2n+1$ is composite.

Our solution is based on an analysis of the highest power of 2 which divides a number of the form $a^k - 1$ or $a^k + 1$, where a is an odd integer.

Let us assume first that k is odd. We will use the following simple observation: if k is odd then $1 + a + a^2 + \ldots + a^{k-1}$ is odd. In fact, we are adding an odd number of odd numbers, hence we get an odd number. Since

$$a^k - 1 = (a-1)(1 + a + \ldots + a^{k-1})$$

we see that the largest power of 2 which divides $a^k - 1$ is the same as the largest power of 2 which divides $a - 1$.
Similarly, since

$$a^k + 1 = (a+1)(1 + (-a) + (-a)^2 + \ldots + (-a)^{k-1}),$$

the largest power of 2 which divides $a^k + 1$ is the same as the largest power of 2 which divides $a + 1$.

Suppose now that $k = 2^s m$ is even, where m is odd and $s \geq 1$. We will use the following simple but very useful observation: if b is an odd integer then $b^2 + 1$ is even but not divisible by 4. Indeed, writing $b = 2c + 1$ we see that $b^2 + 1 = 2[2(c^2 + c) + 1]$ is twice an odd number. It follows that when a is odd and k is even then the highest power of 2 which divides $a^k + 1$ is 2.

In order to analyze the highest power of 2 dividing $a^k - 1$ note that

$$a^k - 1 = a^{2^s m} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \ldots (a^{2^{s-1}m} + 1).$$

Our previous discussion tells us for each factor on the right the highest power of 2 dividing it. Putting it together we see that if 2^u is the highest power of 2 which divides $a - 1$ and 2^w is the highest power of 2 which divides $a + 1$ then $2^{u+w+s-1}$ is the highest power of 2 which divides $a^k - 1$.

We are going to apply the above observation when $a = 2n + 1$ and $k = 2n$.

Case 1: n is odd. Then $s = 1$, $u = 1$, $w = t + 1$, where 2^t is the largest power of 2 which divides $n + 1$. Thus 2^{t+2} is the largest power of 2 which divides $(2n+1)^{2n} - 1$.

On the other hand, if $n > 7$ then $2 < (n+1)/2 < n - 3 < n - 1$ so $n!$ is divisible by $(n+1)(n-3)(n-1)$ and $(n+1)(n-3)(n-1)$ is divisible by 2^{t+3} (since $n - 3$, $n - 1$ are even and one of them is divisible by 4). It follows that $n!$ cannot divide $(2n+1)^{2n} - 1$ when $n > 7$. Thus $n \leq 7$. Since $2n + 1$ must be a prime, $n \in \{1, 3, 5\}$. A simple verification confirms that conversely, if $n \in \{1, 3, 5\}$ then $n!$ divides $(2n+1)^{2n} - 1$. Thus the only odd numbers which satisfy the conditions of the problem are $1, 3, 5$.

Case 2: n is even. Write $n = 2^t m$, where m is odd and $t \geq 1$. In this case $s = t + 1$, $u = t + 1$, $w = 1$. Thus 2^{2t+2} is the largest power of 2 which divides $(2n+1)^{2n} - 1$.

Suppose now that $n!$ divides $(2n+1)^{2n} - 1$. Then the highest power of 2 which divides $n!$ can not exceed 2^{2t+2}.

If $m \geq 3$ then $n!$ is divisible by $2^t \cdot (2 \cdot 2^t) \cdot (3 \cdot 2^t)$ so 2^{3t+1} divides $n!$. It follows that $3t + 1 \leq 2t + 2$ i.e. $t \leq 1$. Thus $t = 1$ and $n! = (2m)!$ is not divisible by $2^{2t+3} = 2^5$. Only $m = 3$ works since 2^5 divides $(2m)!$ for $m > 3$. Conversely, straightforward verification shows that $n = 6$ works since $6!$ divides $13^{12} - 1$.

If $m = 1$ then $n = 2^t$ and $n!$ is divisible by $2 \cdot 2^2 \cdot \ldots \cdot 2^t = 2^{t(t+1)/2}$. Thus $t(t+1)/2 \leq 2t + 2$, i.e. $t^2 - 3t - 4 = (t-4)(t+1) \leq 0$. This yields $t \leq 4$, i.e. $n \in \{2, 4, 8, 16\}$. A simple direct verification shows that only $n = 2$ works (as $2 \cdot 4 + 1 = 9$, $2 \cdot 16 + 1 = 33$ are not primes and $(2 \cdot 8 + 1)^{2 \cdot 8} - 1 = 17^{16} - 1$ is not divisible by 7).

Putting all the above discussion together we see that $n!$ divides $(2n+1)^{2n}-1$ if and only if n is one of $1, 2, 3, 5, 6$

Exercise. Use the binomial formula to justify the value of the highest power of 2 which divides $(2n+1)^{2n}-1$ in case 1 and case 2 of the above solution (this was the method used in the solution submitted by Prof. Kargin.)

A slightly more challenging than Problem 2 is the following problem.

Problem. Find all positive integers n such that $n!$ divides $(n+1^2)(n+2^2)\dots(n+n^2)$.

I do not know the answer to the following question:

Question. Is the set of prime numbers p such that every prime q smaller than $p/2$ divides $p^{p-1}-1$ finite?

We end our discussion with two exercises which expand on the technique used in our solution and which are very useful in many problems in elementary number theory.

Exercise. Recall thal $\lfloor x \rfloor$ denotes the largest integer not exceeding x. Prove that if $n > 1$ and $p \leq n$ is a prime then the highest power of p which divides $n!$ is p^e, where

$$e = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

(note that the sum is actually finite since $\lfloor n/p^k \rfloor = 0$ when $p^k > n$).

Hint. There are several ways to prove this, but I suggest a proof by induction on n. First show that if n, k are positive integers then

$$\left\lfloor \frac{n+1}{k} \right\rfloor = \begin{cases} \lfloor \frac{n}{k} \rfloor & \text{if } k \text{ does not divide } n+1 \\ 1 + \lfloor \frac{n}{k} \rfloor & \text{if } k \text{ divides } n+1 \end{cases}.$$

The goal of the next exercise is to study the highest power of an odd prime p which divides a number of the form $a^k \pm 1$. The case $p = 2$ was done in the solution to our original problem.

Exercise. Let p be an odd prime number and let a be an integer not divisible by p.

1. Show that the smallest positive integer d such p divides $a^d - 1$ exists and that d divides $p-1$. d is called **the order of** a **modulo** p. Hint: Use Fermat's Little Theorem.

2. Prove that p divides $a^k - 1$ if and only if d divides k.

3. Prove that if d is odd then p does not divide $a^k + 1$ for any k. Show that if $d = 2l$ is even then p divides $a^k + 1$ if and only if k/l is an odd integer.

4. Suppose that p^u is the highest power of p which divides $a^d - 1$. Prove that if d divides k and p^s is the highest power of p dividing k then p^{u+s} is the highest power of p dividing $a^k - 1$.

3. Show that if $d = 2l$ is even then p^u (defined in part 4.) is the highest power of p dividing $a^l + 1$. Show that if k/l is an odd integer and p^s is the highest power of p dividing k then p^{u+s} is the highest power of p dividing $a^k + 1$.