Here are the answers I had to the Number THeory questions.

1. Find all integers n for which $n(n+1)$ is a perfect square.

If $n^2+n=k^2$ then $(2n+1)^2=4n^2+4n+1=(2k)^2+1$ so that $2k$ and $2n+1$ are numbers whose squares differ by just 1. That can only happen if $2n+1=\pm 1$ which requires $n=-1$ or $n=0$.

Alternatively since n and $n+1$ are coprime (unless one of them is zero), their product will be a square iff each of them separately is a square (just look at the prime factorizations); but no two positive squares are ever consecutive.

2. Prove that there is no integer n for which n^5 can be written as a product of six consecutive positive integers.

Quite a few of you worked this problem but it's a little tricky. Jeffrey had the right idea; I can make it a little more detailed.

The first step is to show one of those six integers is itself already a perfect fifth power. The six integers must represent all six congruence classes modulo six; in particular three of them are even and one more is a multiple of 3, but there remain two that are coprime to both 2 and 3, and those two must differ by either 2 or 4. So at most one of those two is a multiple of 5. The other one will then share no common factors with any of the other five integers. In view of the Fundamental Theorem of Arithmetic all the primes dividing this one integer have exponents which are multiples of 5, and so this integer is a perfect fifth power.

It follows that the other five integers multiply out to be a fifth power as well. Since the numbers are so close together, this product will be almost the same as the fifth power of the middle number. Let's make this precise. Let x be the third smallest of the six integers, so the integers are now $x-2, x-1, x, x+1, x+2$, and $x+3$. We know one of those six is a fifth power, and the product of the other five is also a fifth power. That product is at least as big as

$$P=(x-2)(x-1)(x)(x+1)(x+2)=x^5-5x^3+4x$$

and no larger than

$$Q=(x-1)(x)(x+1)(x+2)(x+3)=x^5+5x^4+5x^3-5x^2-6x$$

depending on which of the six integers is the fifth power. But $Q<(x+1)^5$ (it's equal to $(x+1)^5-(x+1)(5x^2+10x+1)$ and that last term is obviously positive since $x>0$) and $P>(x-1)^5$ (it's equal to $(x-1)^5+(x-1)(5(x-3)^3+35(x-3)^2+75(x-3)+44)$ and I write it using that Taylor expansion at 3 so you can see the difference will be positive since $x\geq 3$) and so there are no fifth powers between P and Q except x^5 itself.

So the product of five numbers so close to x has to equal exactly x^5. This is clearly impossible; for example at least one of $x-1$ and $x+1$ has to be among those five numbers and this number is coprime to x (and cannot equal 1).

3. Let $n \geq 3$ be an odd integer. Prove that every positive integer less than n can be written as a sum or difference of two other (positive) integers, each of which is less than n and coprime to n.

For each (odd) prime p dividing n let a_p be an integer which is congruent to neither k nor 0 modulo p. Use the Chinese Remainder Theorem to find an integer a which is congruent to a_p mod p for each such p. We can choose a to be positive and less than the product of these p (in particular we will have $a < n$). I wanted $a_p \not\equiv 0 \pmod{p}$ precisely to ensure that a is coprime to n; since $a_p \not\equiv k \pmod{p}$ we also get that $b = k - a$ is coprime to n, and of course $k = a + b$. If $b < 0$ we have simply written $k = a - |b|$.

4. Let p be a prime of the form $3k + 2$. Suppose that there are integers a and b such that p divides $a^2 + ab + b^2$. Prove that p already divides a and b.

If $a^2 + ab + b^2 \equiv 0 \pmod{p}$ then multiply the first congruence by $a - b$ to conclude that $a^3 \equiv b^3$. But here's the thing: for such primes p, the act of cubing is a one-to-one function on the residues modulo p, that is, from $a^3 \equiv b^3$ we can conclude $a \equiv b$; and then $a^2 + ab + b^2 \equiv 3a^2$, which can only be a multiple of p if $p|a$ (and then we also get $p|b$ since $b \equiv a$ modulo p) so we are done.

That business about cubing is proved like this: since $p - 1 = 3k + 1$ is coprime to 3, 3 has an inverse — call it r, say — modulo $p - 1$. In other words $3r = (p - 1)s + 1$ for some integer s. Then from the premise that $a^3 \equiv b^3$ mod p we deduce that

$$a = a\,(1)^s \equiv a^1(a^{p-1})^s = a^{1+(p-1)s} = a^{3r} = (a^3)^r$$

thanks to Fermat's theorem (that $a^p \equiv a$ modulo p). But likewise $b \equiv (b^3)^r$, so if a^3 and b^3 are congruent, then so are a and b.

This observation is used heavily in cryptography.

5. Suppose p is prime. Show that there are infinitely many positive integers n such that p divides $2^n - n$.

For any integer k let $l = 2^k$. Use the Chinese Remainder Theorem to find infinitely many integers n having both $n \equiv l \pmod{p}$ and $n \equiv k \pmod{p - 1}$. Then thanks again to Fermat's Theorem we will have $2^n \equiv 2^k$ modulo p, and thus $2^n - n \equiv 2^k - l = 0$, i.e. $p|(2^n - n)$.

6. Show that if k is odd then

$$(1 + 2 + \cdots + n) \mid (1^k + 2^k + \cdots + n^k)$$

for all positive integers n.

7. Prove that the sum of the squares of 3 consecutive integers is not a perfect square. What about the sum of the squares of 4 consecutuive integers?

If the integers are $x-1$, x, and $x+1$ then the sum is $3x^2+2$. But that's never a square: squares are always congruent to 0 or 1 modulo 3,

A similar analysis for 5, 7, ... squares asks whether there are integer solutions to Diophantine equations like

$$y^2 = 5x^2 + 10, \qquad y^2 = 7x^2 + 28, \qquad y^2 = 9x^2 + 60, \qquad \ldots$$

Look up "Pell's Equation" to learn about these.

The case of even numbers of summands is similar but a bit messier. For example $(x-1)^2 + x^2 + (x+1)^2 + (x+2)^2 = 4x^2 + 4x + 6$. You could either argue that no square is congruent to 6 modulo 4, or notice that the sum is $(2x+1)^2 + 5$ and the only squares that differ by 5 (namely 4 and 9) do not have an odd number for the smaller of the two.

FWIW:

$$18^2 + 19^2 + \ldots + 28^2 = 77^2.$$

Let me also remark that numbers of the form $1 + 4 + 9 + \ldots + n^2$ are known a *pyramid numbers* for obvious reasons; this sum can be expressed as $n(n+1)(2n+1)/6$. A well-known question asks which pyramid numbers are also squares. This leads to the Diophantine equation

$$y^2 = n(n+1)(2n+1)/6$$

which is now a *cubic* polynomial; that change of degree makes this a considerably harder problem. (We don't have easy ways to solve cubic Diophantine problems.)

8. Show that for all positive integers the number

$$S(m,n) = \frac{1}{m} + \frac{1}{m+1} + \cdots + \frac{1}{m+n}$$

is not an integer.

As noted on Monday, simply let N be the least common multiple of all the denominators on the right, so that $N \cdot S(m,n)$ is the sum of $n+1$ integers. I claim that precisely one of the summands is odd, making the sum of all of them be *odd*. On the other hand, since there are at least two summands, there are surely even denominators involved, so N is even, and so $N \cdot S(m,n)$ would be *even* if $S(m,n)$ were an integer. This contradiction shows $S(m,n)$ cannot b an integer after all.

To prove the claim, consider how many of the $n+1$ denominators is even. Obviously the answer is "about half"; more precisely every other denominator is even — $(n+1)/2$ if there is an even number of summands, and either $n/2$ or $(n/2)+1$ if there is an odd number of summands (depending on whether m is odd or even). So this the number of denominators divisible by 2^1. Similarly we can count the number of them which is divisible by 2^2: they will be every other one of the even denominators. In this way we can count the number of denominators divisible by 2^3, 2^4, etc.: we get a sequence of natural numbers,

each half as big as the one before (possibly rounding either up or down). The tail of such a sequence must be one of these:

$$\begin{aligned} \ldots 5 &\to 2 \to 1 \\ \ldots 4 &\to 2 \to 1 \\ \ldots 3 &\to 2 \to 1 \\ \ldots 3 &\to 1 \end{aligned}$$

(followed by any number of 1's, followed eventually by zeros). All this is a long-winded way of showing that there will be some value of k such that there is a unique denominator $m+i$ which is divisible by 2^k; if that one integer is divisible by 2^r but not 2^{r+1}, say, then N will also be divisible by 2^r but not 2^{r+1}, so when multiplying all the terms by N, that one summand will yield an odd integer $N/(m+i)$ and all the other summands will yield even integers $N/(m+j)$.

(I don't think I said that very well. Anyone else?)