Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in complete sentences. Be careful to explain what you are doing since your exam book is your only representative when your work is being graded.

The problems are worth 6 points each.

1. Show that \( \frac{(2n)!}{n!2^n} \) is an odd integer for \( n = 0, 1, 2, \ldots \).

For what it’s worth, the first values of \( \frac{(2n)!}{n!2^n} \) are

\[ 1, 1, 3, 15, 105, 945, 10395, 2027025, 34459425, 654729075, \ldots. \]

I encountered this problem while talking with a student in office hours; it came up in homework last week or the week before. The point is to think of \( (2n)! \) as the product of some odd numbers \( 1 \cdot 3 \cdot 5 \cdots (2n - 1) \) times the product of even numbers \( 2 \cdot 4 \cdots (2n) \). The latter product may be rewritten \( 2^n n! \) by factoring out a 2 from each element in the product.

2. Using the equation \( 1 = 32 \cdot 353 - 45 \cdot 251 \), find four distinct numbers mod \( 251 \cdot 353 \) whose squares are 1 mod \( 251 \cdot 353 \). (No need to calculate the four numbers exactly — just leave them as arithmetic expressions.)

The main point is that you can solve any pair of congruences \( x \equiv a \mod 251 \), \( x \equiv b \mod 353 \) once you realize that \( 32 \cdot 353 \) is 0 mod 353 and 1 mod 251 whereas \(-45 \cdot 251\) is 1 mod 353 and 0 mod 251. By taking \((a, b)\) to be, in turn, \((1, 1), (1, -1), (-1, 1)\) and \((-1, -1)\) you get four different numbers whose squares are 1. (I discussed this kind of thing briefly in class on September 18.)

3. Let \( n \) and \( k \) be positive integers. Show that \( \frac{(n+1)^k - 1}{n} \) is an integer congruent to \( k \) mod \( n \).

This was suggested by problem 32 of §1.2. Write the \( n \) in the denominator as \((n+1) - 1\) and use the fact that \( \frac{x^k - 1}{x - 1} \) is the sum \( 1 + x + x^2 + \cdots + x^{k-1} \). If you work mod \( n \), \( x = n + 1 \) is just 1. There are \( k \) terms in the sum that I just wrote down, each congruent to 1. Therefore the sum is \( k \) mod \( n \). (Of course you can do this also by expanding \((n + 1)^k \ldots\))
4. Let $p$ be a prime and let $n = kp + r$ with $k \geq 1$ and $0 \leq r \leq p - 1$. Establish the congruence $k \equiv \binom{n}{p} \mod p$.

The number $\binom{n}{p}$ may be written as a fraction: The numerator is the product

$$(kp + r)(kp + r - 1)(kp + r - 2) \cdots (kp + r - (p - 1))$$

of $p$ different factors, one of which is $kp + r - r = kp$. The denominator is the product $p(p - 1)!$. Cancelling the $p$s, we see that $\binom{n}{p} = k \frac{a}{b}$, where $b = (p - 1)!$ and $a$ is the product of $p - 1$ factors, which are all non-zero mod $p$. These factors are furthermore incongruent to each other mod $p$, so they must be the mod $p$ numbers $1, 2, \ldots, p - 1$ in a slightly scrambled order. In other words, $a \equiv b \mod p$.

We have $\binom{n}{p} = k \frac{a}{b}$, as remarked above, so $b \binom{n}{p} = ka$. Working mod $p$, we have $b \binom{n}{p} \equiv kb$ because $a$ and $b$ are the same mod $p$. Since $b$ is invertible mod $p$ (actually it’s $-1$ by Wilson’s theorem), we get the desired congruence $\binom{n}{p} \equiv k \mod p$. Note: As explained at the exam, you lose only one point by restricting to the case $p = 7$.

5. Prove that there are infinitely many primes of the form $4k + 1$ by considering expressions of the form $P^2 + 4$, where $P$ is a product of prime numbers of the form $4k + 1$.

This is something that we did in class. I said that I learned it from “Proofs from the Book,” but I think that it’s mentioned in our textbook as well. If you have a bunch of primes of the form $4k + 1$, let $P$ be their product. The expression $P^2 + 4$ is clearly odd, so it’s not divisible by 2. Also, it can’t be divisible by a $(4k + 3)$ prime because of the theorem (or lemma) in the book that says that if such a prime divides $a^2 + b^2$ it has to divide both $a$ and $b$. (In our context, it can’t divide either.) So let $p$ be a prime dividing $P^2 + 4$. It’s odd, as I said, and can’t be of the form $4k + 3$; thus it must be of the form $4k + 1$. On the other hand, it can’t be one of the original bunch of primes: if it were in the bunch, it would divide $P$ and therefore divide 4. So it’s a new prime of the form $4k + 1$. We can make as many as we like in this way, so we have an infinite number of such primes.