This assignment is also computational in nature, but everything here can be done easily with Wolfram alpha, I think.

1. Find a 100-digit probable prime. I will give an extra credit point if your prime is different from those of the rest of the class, and different from the answers from any previous class. (Note: $10^{100}$ is a number with 101 digits.)

**Solution:** In addition to the standard $10^{99} + 289$ (given by two people), one person gave $10^{99} + 4381$, the 10th smallest prime larger than $10^{99}$, another gave $[\pi \times 10^{99}] + 70$. The rest of the class used Mathematica to produce a random 100-digit number and took the next larger prime.

If you are curious, past classes have done the following: It is common for people to do something like $10^{99} + 101101$, that is, not the smallest, but down the list of smallest 100-digit primes. Others have gotten away from $10^{99}$ in various ways, like $10^{99} \times 31$, $3^{10} \times 10^{99}$, and one I enjoyed, $10^{100} - 797$, the largest 100-digit prime. Actually, the person was more careful and gave me $10^{100} - 40659$, just in case anyone else in the class tried this idea.

2. Let $n = 10^{100} + 39$. Use Fermat’s Little Theorem to prove that $n$ is not a prime.

**Solution:** If we calculate $2^{n-1} \pmod{n}$, we get the 100 digit number $6923\ldots334$. Since we did not get 1, $n$ is not prime.

3. Use Fermat’s Little Theorem to verify that 561 is a Carmichael number. Hint: Show that for any $a$, $a^{561} \equiv a \pmod{3}$, $a^{561} \equiv a \pmod{11}$ and $a^{561} \equiv a \pmod{17}$. Conclude (with reasons) that $a^{561} \equiv a \pmod{561}$.

**Solution:** Many people said that by Fermat’s Little Theorem, $a^2 \equiv 1 \pmod{3}$, but this isn’t correct. What is true is that unconditionally, $a^3 \equiv a \pmod{3}$ but $a^2 \equiv 1 \pmod{3}$ only for those $a$ not divisible by 3. One approach to the problem is to do two cases: If $3 \nmid a$ then $a^2 \equiv 1 \pmod{3}$, so $a^{560} = (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod{3}$. Multiplying by $a$, $a^{561} \equiv a \pmod{3}$. If $3 \mid a$ then $a$ and $a^{561}$ are both 0 modulo 3, so we still have $a^{561} \equiv a \pmod{3}$. Similarly, if $11 \mid a$ then $a^{561} \equiv 0 \equiv a \pmod{11}$, and if $11 \nmid a$ then $a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}$, so $a^{561} \equiv a \pmod{11}$. Finally, if
5. (a) Find the smallest base 2 pseudoprime $n$. If $17 \nmid a$ then $a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$, so $a^{561} \equiv a \pmod{17}$, and if $17 \mid a$ then $a^{561} \equiv 0 \equiv a \pmod{17}$. Thus, $a^{561} - a$ is divisible by 3, 11 and 17, and since these are relatively prime, $a^{561} - a$ is divisible by their product, 561. Hence, $a^{561} \equiv a \pmod{561}$, so 561 is a Carmichael number.

One can also try the following, to avoid special cases: $x^{17} \equiv x \pmod{17}$ for all $x$ so $a^{561} = (a^{33})^{17} \equiv a^{33} \pmod{17}$. Next, $a^{33} = a^{17}a^{16} \equiv a \cdot a^{16} = a^{17} \equiv a \pmod{17}$. This kind of approach works better with larger primes. With 3, the chain would go like this: $a^{561} = (a^{187})^3 \equiv a^{187} \pmod{3}$. Next, divide 187 by 3 to get a quotient and remainder: $a^{187} = a^{62\cdot3+1} = a \cdot (a^{62})^3 \equiv a \cdot a^{62} = a^{63} \pmod{3}$. Now we can iterate this idea: $a^{63} = (a^{21})^3 \equiv a^{21} \pmod{3} = (a^7)^3 \equiv a^7 \pmod{3} = a \cdot (a^2)^3 \equiv a \cdot a^2 = a^3 \equiv a \pmod{3}$.

4. If $n > 2$, prove that $\phi(n)$ is even. Do this without using the formula for $\phi(n)$.

**Solution:** There is a tricky proof, which is a modification of an abstract algebra idea: use Euler’s theorem. Since -1 is relatively prime to every integer $n$, $(-1)^{\phi(n)} \equiv 1 \pmod{n}$. Also, if $n > 2$, then $-1 \not\equiv 1 \pmod{n}$, so it must be that $(-1)^{\phi(n)} = 1$, meaning that $\phi(n)$ is even.

A counting proof is to show that the things relatively prime to $n$ but less than $n$ pair up, so there must be an even number. The pairing is $x \leftrightarrow n - x$. That is, $x$ is relatively prime to $n$ if and only if $n - x$ is. To see this, if $d \mid n$ and $d \mid (n - x)$, then $d \mid (n - (n - x))$, so $d \mid x$. If gcd$(n, x) = 1$, this forces gcd$(n, n - x)$ to be 1 as well. Also, we can’t have something paired with itself: If $x = n - x$, then $n = 2x$, so gcd$(n, x) = x$, and this can’t be 1 unless $x = 1, n = 2$. So for $n > 2$, we do get a pairing, proving that $\phi(n)$ is even.

5. (a) Find the smallest base 2 pseudoprime $n > 1000$.

**Solution:** The smallest is $1105 = 5 \times 13 \times 17$. Many people were not careful enough and gave $n = 1009$ as their answer. But a pseudoprime is a composite number $n$ for which $2^{n-1} \equiv 1 \pmod{n}$.

(b) Use the binary squaring algorithm to show $2^{n-1} \equiv 1 \pmod{n}$.

**Solution:** We use $1104 = 1024 + 64 + 16 = 2^{10} + 2^6 + 2^4$, and form a table of $2^{2^k} \pmod{1105}$ for $0 \leq k \leq 10$. 

Page 2
Now
\[ 2^{1104} = 2^{2^4+2^6+2^{10}} = 2^{2^4} \times 2^{2^6} \times 2^{2^{10}} \equiv 341 \times 341 \times 341 \equiv 256 \times 341 \equiv 1 \pmod{1105}. \]

For people who mistakenly used \( n = 1009 \), the check that \( 2^{1008} \equiv 1 \pmod{1009} \) would go like follows.

\[ \begin{array}{cccccccccccc}
 k & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
 2^k \pmod{1009} & 2 & 4 & 16 & 256 & 383 & 384 & 142 & 993 & 256 \\
\end{array} \]

Now \( 1008 = 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 \) so \( 2^{1008} \equiv 960 \times 383 \times 384 \times 142 \times 993 \times 256 \equiv 404 \times 42 \times 949 \equiv 404 \times 507 \equiv 1 \pmod{1009} \).

(c) Prove (as in problem 3) that \( n \) is a Carmichael number.

**Solution:** I originally put this here, then decided to move it to extra credit, but forgot to delete it. I treated it like extra credit anyway.

This is almost identical to what was done in problem 3. I will give just a sketch. If \( p \) is one of the primes dividing 1105, then if \( p \mid a \), \( a^{1105} \equiv 0 \equiv a \pmod{p} \). If \( p \not\mid a \), then \( a^{p-1} \equiv 1 \pmod{p} \), and \( a^{k(p-1)} \equiv 1 \pmod{p} \) as well, for any integer \( k \). Since 1104 is divisible by 4, 12, and 16, we have the appropriate \( k \) values for each prime (they are \( k = 276, 92 \) and 69). Thus, for each prime \( p \), \( a^{1104} \equiv 1 \pmod{p} \), and multiplying by \( a \) gives \( a^{1105} \equiv a \pmod{p} \). This establishes \( a^{1105} \equiv a \pmod{p} \) for all \( a \) for each of the primes 5, 13, 17. Since these are distinct primes, \( a^{1105} - a \) will be divisible by their product, 1105, so \( a^{1105} \equiv a \pmod{1105} \) for all \( a \).

6. Prove that if \( p \) is prime, then \( \phi(p^n) = p^{n-1}(p-1) \). Do this without using the formula for \( \phi(p^n) \).

**Solution:** This is another counting argument. Since \( p \) is the only prime divisor of \( p^n \), of \( k \) is any integer with \( 1 \leq k \leq p^n \) which is NOT relatively prime to \( p^n \), then \( k \) must be divisible by \( p \). So to find out how many things are not relatively prime to \( p^n \), we just need to count the multiples of \( p \). These are \( 1 \cdot p, 2 \cdot p, \ldots, p^{n-1} \cdot p \), so there are exactly \( p^{n-1} \) numbers between 1 and \( p^n \) not relatively prime to \( p^n \). All the rest will be relatively prime to \( p^n \) so \( \phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) \).
For extra credit:

7. With regard to problem 5,

(a) Show that the smallest base 2 pseudoprime $n > 1000$ is actually a Carmichael number. Give a proof like the one called for in problem 3.

(b) Is the second smallest base 2 pseudoprime $n > 1000$ also a Carmichael number? If not, give a base $a$ for which $a^n \not\equiv a \pmod{n}$.

\begin{center}
\begin{tabular}{|l|}
\hline
\textbf{Solution:} The second smallest base 2 pseudoprime is 1387. It is not a Carmichael number: $3^{1386} \equiv 875 \pmod{1387}$. \\
\hline
\end{tabular}
\end{center}

(c) What about the smallest and second smallest base 3 pseudoprimes?

\begin{center}
\begin{tabular}{|l|}
\hline
\textbf{Solution:} The smallest base 3 pseudoprime is 1105 again, which is a Carmichael number. The second smallest is 1541, which is not a base 2 pseudoprime ($2^{1540} \equiv 1243 \pmod{1541}$) so it also is not a Carmichael number. However, the third smallest base 3 pseudoprime, 1729, is again a Carmichael number. \\
\hline
\end{tabular}
\end{center}