Due Monday, September 26 in class. In each of these problems, the last part is meant to be somewhat harder than the others.

**1(a).** Give a rule analogous to “casting out nines” to find the remainder when the decimal numeral $a_k a_{k-1} \cdots a_1 a_0$ is divided by seven. (Hint: for three-digit numbers, the rule is that the remainder is the same as when dividing $a_0 + 3a_1 + 2a_2$ by seven. So the remainder when dividing 365 by seven is the same as dividing $5 + 3 \cdot 6 + 2 \cdot 3$, or 29. Applying the rule again, the remainder on dividing 29 by 7 is the same as dividing $9 + 3 \cdot 2$, or 15. Applying the rule again, this is the same as dividing $5 + 3 \cdot 1 = 8$ by 7. The remainder is therefore 1.)

**Ans:** A number $n$ is divisible by 7 if and only if $n \equiv 0 \pmod{7}$. Written in the decimal notation above, we need to calculate $a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \pmod{7}$.

To calculate $a + b \pmod{7}$ and $ab \pmod{7}$, we can replace $a$ and/or $b$ with another number equivalent to it (mod 7). So, if we were working (mod 9) rather than (mod 7), we could replace all of the 10’s with 1’s, because $10 \equiv 1 \pmod{9}$. In our case, things are a little more complicated.

$$
\begin{align*}
1 &\equiv 1 \pmod{7} \\
10 &\equiv 3 \pmod{7} \\
10^2 &\equiv 3^2 \equiv 2 \pmod{7} \\
10^3 &\equiv 2 \cdot 3 \equiv 6 \pmod{7} \\
10^4 &\equiv 6 \cdot 3 \equiv 4 \pmod{7} \\
10^5 &\equiv 4 \cdot 3 \equiv 5 \pmod{7} \\
10^6 &\equiv 5 \cdot 3 \equiv 1 \pmod{7}
\end{align*}
$$

From here the pattern repeats, for example $10^9 = 10^6 \cdot 10^3 \equiv 1 \cdot 6 \pmod{7}$. So, division of a number $a_k a_{k-1} \cdots a_1 a_0$ by seven yields the same remainder as division of the number $a_0 + 3a_1 + 2a_2 + \cdots + 5a_5 + a_6 + 3a_7 + \cdots$ by seven.

**1(b).** What does the fact that 365 $\equiv 1 \pmod{7}$ tell you about calendars?

**Ans:** There are probably a few reasonable answers. One, for instance, is that (ignoring leap years) if September 26 is a Monday this year, then it will be a Tuesday next year.

**1(c).** Show that the remainder when the decimal numeral $a_k a_{k-1} \cdots a_1 a_2$ is divided by 37 is equal to

$$
a_0 + 10a_1 + 26a_2 + a_3 + 10a_4 + 26a_5 + a_6 + \cdots,
$$

the pattern being cyclic with period three.
2 SOLUTIONS TO HOMEWORK 3

Ans: Given the method in part (a) above, we need to calculate powers of 10 (mod 37).

\[ 1 \equiv 1 \pmod{37} \]
\[ 10 \equiv 10 \pmod{37} \]
\[ 10^2 \equiv 26 \pmod{37} \]
\[ 10^3 \equiv 26 \cdot 10 \equiv 1 \pmod{37}. \]

The reasoning is now the same as in part (a), and it’s clear that the proposed property holds.

1(d). The rule you found in (a) for remainders mod 7 is more complicated than the rule in (c) for remainders mod 37. What’s the next “surprisingly simple” rule like the one for 37?

Ans: The rule for 37 is simple because 37 divides 999, and thus \( 10^3 \equiv 1 \pmod{37} \).

So, we need to find a prime divisor of 9999 bigger than 37 (this will yield a pattern with period 4), or, if that doesn’t work, a prime divisor of 99999 bigger than 37 (yielding a pattern with period 5), etc. It turns out we don’t have to proceed past 9999, because 101 divides 9999. Here the surprisingly simple rule is that 101 divides \( a_k a_{k-1} \cdots a_1 a_0 \) if and only if it divides

\[ a_0 + 10a_1 + 100a_2 + 91a_3 + a_4 + 10a_5 + 100a_6 + 91a_7 + \cdots. \]

If you prefer, this can be rewritten as

\[ a_0 + 10a_1 - a_2 - 10a_3 + a_4 + 10a_5 - a_6 - 10a_7 + \cdots. \]

Another possible answer would be the rule for dividing by 41. It divides 99999, and so it also has a simple rule, but with period 5 rather than period 4.

2(a). Find a multiplicative inverse of 17 modulo 101.

Ans: We can see that 17 and 101 are relatively prime. (The same is true for any two distinct prime numbers.) Nevertheless, let’s use the Euclidean algorithm as if we were seeking their greatest common divisor:

\[ 101 = 5 \cdot 17 + 16 \]
\[ 17 = 1 \cdot 16 + 1 \]

So, we have 16 = 101 - 5 \cdot 17 and 17 - 16 = 1, and plugging in the first to the second, we get 17 - (101 - 5 \cdot 17) = -101 + 6 \cdot 17 = 1, and hence

\[ 6 \cdot 17 \equiv 1 \pmod{101}, \]

so 6 is a multiplicative inverse of 17 (mod 101).

2(b). The integer 2 is invertible modulo any odd prime \( p \). Write a formula that’s linear in \( p \) for an inverse of 2 modulo \( p \). (I’m not looking for the formula \( 2^{p-2} \) from the text; that is not linear in \( p \). Here’s a hint: if \( p \) is odd, then \( p + 1 \) is even, so you can divide it by two.)

Ans: As explained in the hint, \( \frac{p+1}{2} \) is an integer, and clearly \( 2 \cdot \frac{p+1}{2} = p + 1 \equiv 1 \pmod{p} \). Hence, \( \frac{p+1}{2} \) is a formula for the inverse which is linear in \( p \).

2(c). The integer 3 is invertible modulo \( p \) for any prime \( p \) except 3. By breaking the problem into two cases, write formulas similar to those in part (b) for the inverse of 3 modulo any prime except 3.
Ans: If \( p \equiv 2 \pmod{3} \), then 3 divides \( p + 1 \), and so, as above, we have a multiplicative inverse \( \frac{p+1}{3} \). If \( p \equiv 1 \pmod{3} \), then 3 divides \( 2p + 1 \), and so \( 2^{p+1} \) is a multiplicative inverse of three \( \pmod{p} \). These two cases cover all primes distinct from 3.

3. This problem is about the exercises for section 3.5.

3(a). Find a counterexample to exercise 3.5.1.

Ans: Four is not prime, yet it doesn’t divide 3!. This should be the only counterexample.

3(b). Suppose that \( n > 1 \) is a natural number. Let \( m \) be the largest integer less than or equal to the square root of \( n \). Prove that \( \gcd(n, m!) \) is equal to 1 if \( n \) is prime, and strictly greater than 1 if \( n \) is not prime.

Ans: Assume first \( n \) is prime. Then \( n \) has only two divisors, 1 and \( n \). As \( m \) is strictly less than \( n \) and \( n \) is prime, we see that \( m! \) cannot have \( n \) among its divisors. So, the greatest common divisor has to be 1.

Now we assume \( n \) is composite. Then we can write \( n = ab \) as the product of two natural numbers, where neither \( a \) nor \( b \) equals 1. One of \( a \) and \( b \) must be less than or equal to the square root of \( n \), lest the product \( ab \) be greater than \( \sqrt{n^2} = n \). Without loss of generality, we can assume that \( a \) is this element. Then \( a \) divides \( m! \), and so \( \gcd(n, m!) > 1 \).

3(c). Use the method of (b) to find a proper divisor of 143. (Hint: \( 11! = 39,916,800 \).)

Ans: With part (b) above in mind, because \( \sqrt{143} = 11.958 \ldots \) we consider \( 11! \) and apply the Euclidean algorithm to find a proper divisor of 143.

\[
39,916,800 = 279138 \times 143 + 66 \\
143 = 2 \times 66 + 11 \\
66 = 6 \times 11
\]

Hence 11 is a proper factor of 143.

3(d). The Euclidean algorithm is very fast even for large numbers. Does this exercise fix the “impracticality” objection for Wilson’s Theorem as a test for prime numbers (text, top of page 55)?

Ans: No. It improves the speed, because now we have to calculate the factorial of a number on the order of \( \sqrt{n} \) rather than on the order of \( n \), but this can still require an impractical number of calculations (about \( \sqrt{n} \) of them).

4(a). Find a primitive root for 37. (If you do part (b) first, then you have a little less calculating to do.)

Ans: By part (b), if we have a number \( a \), with \( 1 \leq a < 37 \) such that \( a^{18} \not\equiv 1 \pmod{37} \) and \( a^{12} \not\equiv 1 \pmod{37} \), then \( a \) is a primitive root.

\[
2^{12} \equiv 26 \pmod{37} \\
2^{18} \equiv -1 \pmod{37}
\]

So, 2 is a primitive root for 37.

4(b). Suppose that \( a \) is not divisible by 37, but is not a primitive root for 37. Show that either \( a^{12} \equiv 1 \pmod{37} \), or \( a^{18} \equiv 1 \pmod{37} \).
Ans: We know that \( a^{36} \equiv 1 \pmod{37} \) by Fermat’s Little Theorem. Not being a primitive root implies the order is strictly less than 36. The order must be a divisor of 36 (sketch of proof: if \( b \) is the order and \( b \) does not divide 36, then by division with remainder we get some \( 0 < r < b \) such that \( a^r = a^{36-r} b = 1 \cdot 1 \), which contradicts our assumption that the order was \( b \)). By prime factorization, a proper divisor of 36 = \( 2^2 \cdot 3^2 \) must be a (not necessarily proper) divisor of \( 2^2 \cdot 3 \) or \( 2 \cdot 3^2 \). Hence the claim.

4(c). Part (b) gives a test for being a primitive root for 37 that involves calculating only two exponentials modulo 37. How many exponentials do you need to test for being a primitive root for some prime \( p \)?

Ans: Again, from the reasoning in part (b), we know \( a \) has order dividing \( p - 1 \). So we first calculate the prime factorization of \( p - 1 \). Say \( p - 1 = p_1^{n_1} \cdots p_k^{n_k} \), where the \( p_i \)’s are all distinct. A proper divisor of \( p - 1 \) will be a (not necessarily proper) divisor of \( p_1^{n_1} \cdots p_i^{n_i - 1} \cdots p_k^{n_k} = \frac{p - 1}{p_i} \) for some \( i \). We thus calculate \( a^{(p-1)/p_i} \) for the \( k \) distinct \( i \)’s, and if any of them is equal to one, \( a \) is not a primitive root. If none of them is equal to one, then \( a \) is a primitive root. The fact that both of the \( n_i \)’s in our example were greater than 1 was just a coincidence.