18.781 Problem Set 3

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 $a_k a_{k-1} \cdots a_0 a_1$ 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.)

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

1(c). Show that the remainder when the decimal numeral $a_k a_{k-1} \cdots a_0 a_1$ 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.

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?

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

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.

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

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

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.

3(c). Use the method of (b) to find a proper divisor of 143. (Hint: $11! = 3,991,680$.)

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)?

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

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 $a^{18} \equiv 1 \pmod{37}$.

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?