18.781 Problem Set 3

Due Monday, February 25 in class.

1(a). "Casting out nines" says that when the decimal number $a_k a_{k-1} \cdots a_0 a_1$ is divided by 9, the remainder is the same as when $a_0 + a_1 \cdots + a_k$ is divided by 9. Give an analogous rule to find the remainder when this decimal numeral 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). 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(c). 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 (that is, $ap + b$) for an inverse of 2 modulo 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 linear formulas similar to those in part (b) for the inverse of 3 modulo any prime except 3.

2(d). Write a single quadratic formula in p for the inverse of 3 modulo any prime p except 3.

3(a). Exercise 34, page 58.

3(b). Suppose you are interested in testing whether a large number is prime. You have a computer that can perform 4×10^{12} arithmetic operations (on 200 digit numbers) per second. What's the biggest m whose primality you could test in one year using (a)?

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

3(d). What's the biggest m whose primality you could test in one year using (c)? (Same computer as in (b).)