18.781 Problem Set 3 solutions

1(a). "Casting out nines" says that when dividing the decimal number $a_k a_{k-1} \cdots a_0 a_1$ 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.)

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

$$a_k \cdot 10^k + a_{k1} \cdot 10^{k1} + \cdots + a_1 \cdot 10 + a_0 \pmod 7.$$

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

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

Now the pattern repeats with period 6; for example, $10^9 \equiv 10^3 \equiv 6 \pmod 7$. So division of $a_k a_{k-1} \cdots a_0 a_1$ by 7 yields the same remainder as division of

$$a_0 + 3a_1 + 2a_2 + \cdots + 5a_5 + a_6 + 3a_7 + \cdots$$

by 7.

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

The method in (a) says that we need to calculate

$$\begin{aligned}
1 &\equiv 1 \pmod{37} \\
10 &\equiv 10 \pmod{37} \\
10^2 \equiv 10 \cdot 10 &\equiv 26 \pmod{37} \\
10^3 \equiv 10 \cdot 26 &\equiv 1 \pmod{37}
\end{aligned}$$

The pattern repeats, so the same reasoning as in (a) applies. **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?**

The rule for 37 is simple because $37|999$, 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 doesnt work, a prime divisor of 99999 bigger than 37 (yielding a pattern with period 5), etc. It turns out that $101|9999$: the remainder on dividing $a_k a_{k-1} \cdots a_0 a_1$ by 101 is the same as on dividing

$$a_0 + 10a_1 + 100a_2 + 91a_3 + a_4 + 10a_5 + \cdots$$

If you prefer, this can be rewritten as

$$a_0 + 10a_1 - a_2 - 10a_3 + a_4 + 10a_5 + \cdots$$

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

This is exactly like Problem 1 on the second problem set:

$$\begin{aligned} 101/17 &= 5 \quad R\ 16 \\ 16 &= 101 - 5 \cdot 17 \\ 17/16 &= 1 \quad R\ 1 \\ 1 &= 17 - 16 = 17 - (101 - 5 \cdot 17) = -101 + 6 \cdot 17. \end{aligned}$$

The last equation $1 = -101 + 6 \cdot 17$ both says that the gcd of 101 and 17 is 1, and tells you that the multiplicative inverse of 17 modulo 101 is **6**.

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.)

So **(p+1)/2** is a formula (linear in the odd prime p) for an integer. I claim it's a multiplicative inverse of 2. The reason is

$$2 \cdot (p+1)/2 = p + 1 \equiv 1 \pmod{p}.$$

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.

If p is a prime not three, then $3 \nmid p$, so the remainder when p is divided by 3 must be 1 or 2. That is, *either* $p - 1$ is divisible by 3 *or* $p + 1$ is divisible by 3. Therefore an inverse z of 3 modulo any prime p not divisible by 3 is

$$z = \begin{cases} (1-p)/3 & (p-1 \text{ divisible by } 3) \\ (1+p)/3 & (p+1 \text{ divisible by } 3) \end{cases}$$

The reason is the same as in (b): in the first case, for example,

$$3 \cdot z = 1 - p \equiv 1 \pmod{p}$$

and in the second case

$$3 \cdot z = 1 + p \equiv 1 \pmod{p}.$$

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

There are several ways to proceed. One is that 2(c) shows that either $1 + p$ or $1 - p$ must be divisible by 3; so in either case their product $1 - p^2$ is divisible by 3. Therefore

$$z = (1 - p^2)/3$$

is a quadratic formula in p for a multiplicative inverse of 3 modulo p. The reason is

$$3 \cdot z = 1 - p^2 \equiv 1 \pmod{p}.$$

3(a). Exercise 34, page 58.

The exercise reads

an integer $m > 1$ is prime if and only if m divides $(m-1)! + 1$.

There are two statements you are asked to prove:

(ONLY IF) *If* m is prime, *then* $m | [(m-1)! + 1]$.

(IF) *If* $m | [(m-1)! + 1]$, *then* m is prime.

(You may think that I've labelled these backwards; think about it some more, or come to office hours and ask about it.) Wilson's theorem (text, page 53) is exactly ONLY IF. So you have to prove the second statement IF. In mathematics, the statement *if A then B* is exactly the same as *if not-B then not-A*. We'll prove that equivalent statement

(CONTRAPOSITIVE OF IF) *If* m is not prime, *then* $m \nmid [(m-1)! + 1]$.

So suppose m is not prime. This means (Theorem 1.14) that m has a prime divisor $p \leq m - 1$. Therefore p is one of the factors of $(m-1)!$, so $(m-1)! \equiv 0 \pmod{p}$. Therefore $(m-1)! + 1 \equiv 1 \pmod{p}$, and in particular $p \nmid [(m-1)! + 1]$. Since p is a divisor of m, it follows that

$$m \nmid [(m-1)! + 1],$$

and that's what we were supposed to show.

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)?

According to the exercise, m is prime if and only if

$$(m-1)! \equiv -1 \pmod{m}.$$

So to test m for primality, we have to compute

$$(m-1)! = 2 \cdot 3 \cdot \cdots \cdot (m-2) \cdot (m-1)$$

modulo m. That is, we need to perform $m-3$ multiplications modulo m. At the kth multiplication, we take the previous answer (which is between 0 and $m-1$), multiply it by $k+2$, divide by m with remainder, and then keep the remainder (which is again at most $m-1$). As long the old answer (which is $(k+1)!$ modulo m), $k+2$, and m have at most a hundred digits, then the two arithmetic operations involved will be done without overflow, and the new answer (which is $(k+2)!$ modulo m) will also have at most a hundred digits.

This description says that if m has at most a hundred digits, then the calculation of $(m-1)!$ modulo m requires $2(m-3)$ arithmetic operations. The time required is therefore approximately $2(m-3)/(4 \times 10^{12})$ seconds. We have a year, or 3×10^8 seconds. Therefore we can finish the calculation as long as

$$2(m-3)/(4 \times 10^{12}) < 3 \times 10^8, \qquad m - 3 < 6 \times 10^{20}.$$

That is, we can do this calculation on a **twenty digit number**.

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.

The product of two positive integers is at least as big as the square of the smaller one. Another way to say the same thing is that *the smallest prime factor of a non-prime $m > 1$ must be at most $\sqrt{m}$.* In the setting of the problem, this means that if m is not prime, then m has a prime factor at most n; so this prime factor must divide $n!$, and $\gcd(m, n!) > 1$. Conversely, if m is prime, then its only nontrivial divisor is m, which does not divide $n!$; so $(\gcd(m, n!) = 1$.

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

This time you need only $2(n-2) \approx 2\sqrt{m}$ calculations to compute the factorial. At the end you need to use the Euclidean algorithm to calculate the gcd. I discussed in class the fact that the number of steps in the Euclidean algorithm for $\gcd(a, b)$ (with $a > b$ is at worst about

$$\log_\gamma(a) = \text{five times the number of digits in } a.$$

(Here γ is the golden ratio $1.61803\ldots$.) So you can do the factorial calculation modulo m in a year as long as

$$\sqrt{(m)} \approx 6 \times 10^{20},$$

which is to say on a **forty-one digit** m. The gcd calculation at the end takes another couple of hundred operations, so is invisibly fast.

The point of these problems is that these primality tests *aren't good enough for modern practical purposes.* Moving money around the internet and keeping your email from your parents requires primes of about 200 digits. These are generated by writing a random 200 digit number and checking whether it's prime. (The odds are about one in 450, so you have to test quite a few random numbers to find a prime.)