MA357, Spring 2020 — Problem Set 4 Solutions

1. NTG, Exercise 4.7.5.

Notice first that it doesn't work for $n = 4$, because $3! = 6$ is not congruent to zero mod 4. A good proof will clarify what is special about 4.

Suppose first that $n = ab$ with $a \neq b$ and $1 < a < n$ and $1 < b < n$. Then both a and b will appear as factors in

$$(n-1)! = (n-1)(n-2)\cdots(2)(1),$$

so $n = ab$ will be a divisor of $(n-1)!$ (but if $a = b$ then that number appears only once). So we have shows that $(n-1)! \equiv 0 \pmod{n}$ whenever n can be written as a product of two distinct non-trivial factors.

The only non-prime n that cannot be written that way are squares of primes, so it remains to consider $n = p^2$ where p is a prime. But if $n = p^2$ and $p > 2$ then $1 < p < 2p < p^2$, so both p and $2p$ appear in the list

$$1, 2, 3, \ldots, n-1.$$

That shows that p^2 divides $(p^2-1)!$ when $p > 2$, which completes the proof. The result is false when $p = 4$ exactly because in that case $2p = p^2$ is not one of the factors.

2. NTG, Exercise 4.7.8.

One can just run to the computer and ask GP to compute things like `Mod(5,7)^18`. That leads us quickly to

$$5^{18} \equiv 1 \pmod{7}, \qquad 68^{105} \equiv 1 \pmod{13}, \qquad 6^{47} \equiv 0 \pmod{12}.$$

A slightly more intelligent approach might tells us more about *why* those are the answers.

For (a), we might start by noticing that $5 \equiv -2 \pmod{7}$ and then noticing that $2^3 \equiv 1 \pmod{7}$. Putting those together gives $5^3 \equiv -1 \pmod{7}$ and hence $5^6 \equiv 1 \pmod{7}$. Cubing both sides gives 5^{18}.

For (b), we start by noticing that $68 \equiv 3 \pmod{13}$, so we're really computing powers of 3. Successive squaring is the way to go (unless you know Fermat's little theorem).

$$\begin{aligned} 3^2 &\equiv 9 \pmod{13} \\ 3^4 \equiv 9^2 &\equiv 3 \pmod{13} \\ &\cdots \end{aligned}$$

But wait, that already tells us $3^4 \equiv 3 \pmod{13}$, so $3^3 \equiv 1 \pmod{13}$. Since 105 is a multiple of 3, we're done.

Finally, for (c) just notice that $6^2 \equiv 0 \pmod{12}$.

3. NTG, Exercise 4.7.11.

This is one of those darstardly tricks. Any three consecutive numbers look like $n-1$, n, $n+1$, whose sum is $3n$. So if you every triple $37k-1, 37, 37k+1$ will give an example.

If you don't think of the dastardly trick and write the numbers as $m, m+1, m+2$, then you're solving the congruence $3m+3 \equiv 0 \pmod{37}$, which just gives $m \equiv -1 \pmod{37}$.

In any case, the smallest example is $36, 37, 38$.

4. Show that if n is an integer, then so is $\dfrac{n^5}{5} + \dfrac{n^3}{3} + \dfrac{7n}{15}$.

Taking a common denominator gives

$$\frac{3n^5 + 5n^3 + 7n}{15},$$

so what we want need to show is that $3n^5 + 5n^3 + 7n \equiv 0 \pmod{15}$. It's enough to show that this expression is $0 \pmod 3$ and is also $0 \pmod 5$. So do each separately.

Working mod 3,

$$3n^5 + 5n^3 + 7n \equiv 2n^3 + n \pmod 3.$$

Now for n^3 we can climb every mountain to check that $n^3 \equiv n \pmod 3$ (it's pretty easy if you realize that the three elements of $\mathbb{Z}/3\mathbb{Z}$ are $\overline{0}$, $\overline{1}$, and $\overline{-1}$). So

$$2n^3 + n \equiv 2n + n \equiv 3n \equiv 0 \pmod 3,$$

in other words, $3n^5 + 5n^3 + 7n$ is always divisible by 3.

Now work mod 5:

$$3n^5 + 5n^3 + 7n \equiv 3n^5 + 2n.$$

Now climb mountains to see that $n^5 \equiv n \pmod 5$ and conclude that $3n^5 + 5n^3 + 7n \equiv 5n$ is divisible by 5.

In fact, $n^p \equiv n \pmod p$ is true for all primes p. This is one of the ways to state "Fermat's Little Theorem."

5. NTG, Exercise 4.7.25.

Remember that there are solutions to $ax \equiv b \pmod m$ if and only if $\gcd(a, m)$ divides b. The number of solutions (up to congruence) is exactly the gcd.

(a) $\gcd(6, 11) = 1$, so there is a unique solution, which is $x \equiv 7 \pmod{11}$.

(b) $\gcd(6, 9) = 3$ which does not divide 11, so there are no solutions.

(c) $\gcd(6, 15) = 3$ does divide 9, so there are three solutions. To find them, we first divide through by 3 to get $2x \equiv 3 \pmod 5$, which gives $x \equiv 4 \pmod 5$. To get the solutions mod 15 we just add multiples of 5. So the solutions are $x \equiv 4, 9, 14 \pmod{15}$.

6. NTG, Exercise 4.7.34.

This one is just work. The answers are $x \equiv 156 \pmod{504}$, $x \equiv 267 \pmod{504}$, and $x \equiv 82 \pmod{504}$. Since the moduli are $7, 8, 9$ in all three cases, one could use Sage to find the CRT basis, which Sage gives as $[-216, -63, -224]$.

7. A band of 17 pirates, upon dividing their gold coins, found that three coins remained after the coins had been apportioned evenly. In the ensuing brawl, one of the pirates was killed. The wealth was again redistributed equally, and this time ten coins remained. Again an argument broke out and one of the pirates was killed. This time the fortune was distributed evenly among the survivors. What is the least possible value for the number of coins the pirates had initially?

If x is the number of coins, the problem says that $x \equiv 3 \pmod{17}$, $x \equiv 10 \pmod{16}$, and $x \equiv 0 \pmod{15}$. So this is a standard Chinese Remainder Theorem problem, and it can be solved the usual way. The number of coins must be congruent to $3930 \pmod{4080}$, so the smallest possible number of coins is 3930.

I tend to use GP to do quick computations. Here is how that looks:

```
gp > ?chinese
chinese(x,{y}): x,y being both intmods (or polmods) computes z in the same
residue classes as x and y.

gp > chinese(Mod(3,17),Mod(10,16))
%1 = Mod(122, 272)
gp > chinese(%,Mod(0,15))
%2 = Mod(3930, 4080)
```

You can do this in the Sage Cell Server if you put it into GP mode, or you can use `gp.chinese` in a Sage Notebook.

8. Let k and s be two positive integers. Show that there exists a sequence of k consecutive integers each of which is divisible by an s-th power. (For example, if $k = 3$ and $s = 2$, we are asking for three consecutive integers which are each divisible by a square. Then 48, 49, and 50 are an example, since they are divisible by 4^2, 7^2, and 5^2, respectively. You want to prove that such sequences always exist.)

Take $m_i = p_i^s$ where p_i is the ith prime number, and apply the Chinese remainder theorem to $x \equiv -(i-1) \pmod{m_i}$ for $i = 1, 2, \ldots k$. Then $x, x+1, \ldots, x+(k-1)$ are divisible, respectively, by $2^s, 3^s, \ldots, p_k^s$.

9. In this problem we want to explore the multiplicative structure of $\mathbb{Z}/m\mathbb{Z}$. Remember that we already know that a will have an inverse mod m if and only if $\gcd(a, m) = 1$.

a. How many congruence classes are invertible mod 4? How about mod 12?

We checked in class that $\varphi(4) = 2$, so two congruence classes are invertible. For 12, a direct count shows $\varphi(12) = 4$. Or you can ask Sage: `euler_phi(12)`.

b. Suppose m is prime. Show that any $a \not\equiv 0 \pmod{m}$ is invertible mod m.

If $a \not\equiv 0 \pmod{m}$ then a is not divisible by m. Since m is prime, that gives $\gcd(a, m) = 1$ and a is invertible mod m.

c. Suppose a is invertible mod m. Show that there must exist an integer $k \geqslant 1$ such that $a^k \equiv 1 \pmod{m}$.

This was the hard one. Consider the list

$$a, a^2, a^3, a^4, \cdots \in \mathbb{Z}/m\mathbb{Z}.$$

Since $\mathbb{Z}/m\mathbb{Z}$ is a finite set, that list can only contain finitely many different elements. So there must exist $r > s$ such that $a^r \equiv a^s \pmod{m}$. If we multiply both sides s times by the inverse of a, we get $a^{r-s} \equiv 1 \pmod{m}$. Since $r > s$, $k = r - s \geqslant 1$ does what we want.

d. Let $m = 7$. For each $a \equiv 1, 2, 3, 4, 5, 6 \pmod{7}$, find the least $k \geqslant 1$ such that $a^k \equiv 1 \pmod{7}$.

Here's a little table

a	1	2	3	4	5	6
smallest k	1	3	6	3	6	2

In GP the command `znorder(Mod(4,7))` gives the least k such that $4^k \equiv 1 \pmod{7}$. In Sage you first create $\mathbb{Z}/7\mathbb{Z}$ with `IntegerModRing(7)` and then use `R(4).multiplicative_order()`.

10. NTG, Exercise 4.7.27.

The binomial theorem says that

$$(a + b)^p = \sum_{n=0}^{p} \binom{p}{n} a^{p-n} b^n.$$

Remember that

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}.$$

If $n = 0$, we get $p!/p! = 1$. If $n = p$ we get $p!/p! = 1$ as well. If $0 < n < p$, there is a p in the numerator but there is no p in the denominator (because both n and $p - n$ are less than p). So $\binom{p}{n} \equiv 0 \pmod{p}$ when $n = 1, 2, \ldots, p - 1$. Plugging everything in,

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$