MA357, Spring 2020 — Problem Set 5 Solutions

1. NTG, Exercise 4.7.41.

The hint suggests looking at the equation mod 7. Indeed, if

$$x^2 - 7y^3 + 21z^5 = 3,$$

then we must have $x^2 \equiv 3 \pmod 7$. Squaring $0, \pm 1, \pm 2, \pm 3$ gives $0, 1, 4, 2$. It follows that 3 is not a square mod 7, and therefore no such x exists, so that the original equation has no solutions.

2. NTG, Exercise 4.7.42. (Experiment first!)

Trying the first four values of n (on a computer, I hope) shows that they are all divisible by 3.

```
gp > for(n=1,4,print(factor(2^(2^n)+5)))
  [3, 2]
  [3, 1; 7, 1]
  [3, 2; 29, 1]
  [3, 1; 7, 1; 3121, 1]
```

So let's work mod 3. Notice that $2^2 \equiv 1 \pmod 3$, and therefore $2^{2^n} \equiv 1 \pmod 3$ for all $n \geqslant 1$. Therefore

$$2^{2^n} + 5 \equiv 1 + 2 \equiv 0 \pmod 3.$$

Since $2^{2^n} + 5 \geqslant 5 > 3$, it follows that $2^{2^n} + 5$ is composite.

I found it hard to guess which modulus to work with just from looking at the formula.

3. Do any numbers satisfy the equation $\varphi(n) = 2n$?

No, because $\varphi(n)$ counts how many of the numbers between 1 and n are relatively prime to n, and there are certainly no more than n of them!

4. Do any numbers satisfy the equation $\varphi(n) = n/2$?

If n is odd, it is clearly not possible, since $n/2$ is not an integer. It's easy to see that any power of two does satisfy the equation, since $\gcd(n, 2^a) = 1$ if and only if n is odd.

For the general case, write $n = 2^a m$ with m odd and $a > 0$. Then m is one of the $n/2$ odd numbers that are less than n, and therefore $\varphi(n) < n/2$. So the upshot is that $\varphi(n) = n/2$ if and only if $n = 2^a$ for some $a \geqslant 1$.

Yes, one can also do this using more powerful results (multiplicativity, or even the formula for $\varphi(n)$ in terms of the factorization of n.)

5. NTG, Exercise 5.6.21.

If you read the text, you know that a is a zero divisor in $\mathbb{Z}/35\mathbb{Z}$ if and only if $\gcd(a,35) > 1$. So the zero divisors in $\mathbb{Z}/35\mathbb{Z}$ are the classes of

$$5, 7, 10, 14, 15, 20, 21, 25, 28, 30.$$

The units are all the others. The pairs (a, a^{-1}) are

$$(1,1), (2,18), (3,12), (4,9), (6,6), (8,22), (11,16), (13,27)$$
$$(17,33), (19,24), (23,32), (26,31), (29,29), (34,34).$$

Notice that we have four cases of $a = a^{-1}$.

For $\mathbb{Z}/11\mathbb{Z}$, it's easier: there are no zero divisors, and every nonzero element is a unit. The $(a, a^{-1}))$ pairs are

$$(1,1), (2,6), (3,4), (5,9), (7,8), (10,10).$$

Since 11 is prime $a = a^{-1}$ can only happen if $a = \pm 1$.

6. In the previous assignment you showed that if $n > 4$ is not prime then $(n-1)! \equiv 0 \pmod{n}$. This problem shows what happens when n is prime.

Let p be a prime. Use the fact that every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ has an inverse $\pmod{p}$ to show that

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

This is called *Wilson's Theorem*.

The first thing we need to show is that the only numbers that are their own inverses mod p are 1 and -1. In fact, if x is its own inverse, then $x^2 \equiv 1 \pmod{p}$, which means that $p \mid (x^2 - 1)$, and so that p divides the product $(x-1)(x+1)$. But if a prime divides a product it must divide one of the factors, so either $p \mid (x-1)$ or $p \mid (x+1)$. The first of these says $x \equiv 1 \pmod{p}$, and the second says $x \equiv -1 \pmod{p}$. So only 1 and -1 are their own inverses.

Once that has been established, we see that we can pair up all the numbers 2, 3, 4, ..., $(p-2)$ with their inverses. Since a number times its inverse is congruent to 1 $\pmod{p}$, the product of this part of the factorial is congruent to $1 \pmod{p}$. Multplying by 1 and by $(p-1)$ gives $(p-1)$, i.e., gives $-1 \pmod{p}$.

7. Suppose $m \in \mathbb{N}$ and let a be an integer such that $\gcd(a, m) = 1$. In the last problem set you showed that there exists an integer k such that $a^k \equiv 1 \pmod{m}$. Of course, then we also have $a^{2k} \equiv 1 \pmod{m}$, so there will be many such exponents.

Let $e \geqslant 1$ be the *smallest* exponent such that $a^e \equiv 1 \pmod{m}$. This is called the *order* of a mod m. Show that

a. If n is a multiple of e, then $a^n \equiv 1 \pmod{m}$.

If $n = ed$, then $a^n = a^{ed} = (a^e)^d \equiv 1^d = 1 \pmod{p}$.

b. Conversely, if $a^n \equiv 1 \pmod{p}$, then e is a divisor of n. (Consider the remainder when we divide n by e.)

We know $a^n \equiv 1 \pmod{p}$ and $a^e \equiv 1 \pmod{m}$. Write $n = eq + r$ with $0 \leqslant r < e$. We want to prove $r = 0$.

Since $a^e \equiv 1$, we get $a^{eq} \equiv 1$. Multiplying both sides by a^r gives $a^{eq+r} \equiv a^r \pmod{p}$. Since $eq + r = n$ we get $a^r \equiv 1 \pmod{p}$. But e is the smallest positive exponent with this property and $0 \leqslant r < e$. So $r = 0$ and e is a divisor of n.

This really has nothing to do with modular arithmetic per se. Rather, it is about the orders of elements of any finite group.