Solutions 12

1. Prove the infinitude of primes. One approach is to suppose that there are only finitely many and try to arise at a contradiction.

   Solution. Suppose for a contradiction that there are only finitely many primes, call them $p_1 < p_2 < \ldots < p_k$. This means that p_k is the largest prime. Consider the number $n = p_1 p_2 \ldots p_k + 1$. Our n cannot be prime because it is larger than p_k, and yet it is clear that it is not divisible by any prime number since it leaves remainder 1 upon division by any p_j in our list of primes. This is a contradiction.

2. Find a cubic polynomial over $\mathbb{F}_{11}$ that passes through the points $(1,1), (4,2), (8,6)$.

   Solution. Let $f(t) = t^3 + bt^2 + ct + d$. Then we know that $f(1) = 1$ implies $b+c+d+1 = 1$, *i.e.* $b+c+d = 0$, from $f(4) = 2$ we know that $9+5b+4c+d = 2$, *i.e.* $5b + 4c + d = 4$, and from $f(8) = 6$ we know that $6 + 9b + 8c + d = 6$, *i.e.* $9b + 8c + d = 0$. Solving this linear system gives us the values of b, c, d, for example $b = 7, c = 3, d = 1$. A cubic which passes through the points is $f(t) = t^3 + 7t^2 + 3t + 1$.

3. Find the kernel of the given matrix A. Find all solutions to $Ax = (1, 2, 3)$.

$$A = \begin{bmatrix} 1 & 3 & 5 & 4 & 0 \\ 1 & -2 & 9 & 2 & 1 \\ 1 & 3 & 1 & 1 & 2 \end{bmatrix}$$

Solution. The RREF of this matrix is

$$\begin{bmatrix} 1 & 0 & 0 & -11/4 & 43/10 \\ 0 & 1 & 0 & 1 & -4/5 \\ 0 & 0 & 1 & 3/4 & -1/2 \end{bmatrix}.$$

If we take the variables to be x, y, z, u, v, the kernel is spanned by $z_1 := (11/4, -1, -3/4, 1, 0)$ and $z_2 := (-43/10, 4/5, 1/2, 0, 1)$. To find a particular solution, we could augment the system and solve, but I happen to notice that $(1, 2, 3)$ is the sum of the first and last columns. This means that $(1, 0, 0, 0, 1)$ is one solution to $Ax = (1, 2, 3)$. The complete solution is given by adding on the kernel; $(1, 0, 0, 0, 1) + c_1 z_1 + c_2 z_2$ for all real c_1, c_2.

4. The vector $(1, 4, 2, 0, 1, 0, 4, x, 5, 1)$ is an ISBN code for what value of x ?

Solution. We have to take the dot product of the given vector with the "blast-off" vector $(10, 9, \ldots, 2, 1)$. This gives us:

$$\begin{aligned} 10 \cdot 1 + 9 \cdot 4 + 8 \cdot 2 + 6 \cdot 1 + 4 \cdot 4 + 3 \cdot x + 2 \cdot 5 + 1 \cdot 1 \\ = 10 + 3 + 5 + 6 + 5 + 3x - 1 + 1 \\ = 7 + 3x \end{aligned}$$

We want the dot product to be zero, so we need to solve $3x + 7 = 0$, or $3x = 4$. To solve this, multiply both sides by 4, the inverse of 3, to obtain $x = 5$ in $\mathbb{F}_{11}$.

5. Compute 99! mod 101. For goodness sakes, use Wilson's Theorem to help you.

Solution. We know by Wilson's Theorem that 100! is -1 modulo 101, so 99! is $100! \cdot 100^{-1} = -1 \cdot -1 = 1$.

6. *Challenge.* Prove that for every prime $p > 2$ there is an element of $\mathbb{F}_p$ besides 1 that is its own inverse. (*e.g.* $2^{-1} = 2 \bmod 3$)

   Solution. This isn't the solution I had intended, but.. $p-1$ is its own inverse modulo p. This is because $(p-1)^2 = p^2 - 2p + 1 = 1$.