

Solutions for Exercise Set 3.**Due in Class on Monday, April 2**

Write as if this were part of your resume for a high-paying job you really want!

1. Let n be a positive integer.

(a) Does n have a multiplicative inverse in $Z/(3n+1)$? If so, find it.

$$-3 = 3n - 2\%(3n+1)$$

(b) Does n have a multiplicative inverse in $Z/(n^2+1)$? If so, find it.

$$n^2 + 1 = n \cdot n + 1$$

So

$$n^{-1} = -n = n^2 + 1 - n\%(n^2 + 1)$$

2. Find all the primitive roots of $Z/18$, and use one of them as a base b to compute the discrete logarithm of those elements of $Z/18$ that have them.

We know there are $\phi(18) = 6$ integers relatively prime to 18: 1, 5, 7, 11, 13, 17. One primitive root is 5, and the discrete logs of 1, 5, 7, 11, 13, 17 are, respectively, 6, 1, 2, 5, 4, 3, respectively.

3. Construct a field F of $2^3 = 8$ elements using the irreducible polynomial $x^3 + x^2 + 1$ in $Z/2[x]$ (check that it is irreducible!), that is $Z/2[x]/(x^3 + x^2 + 1)$. Find a primitive element in this field (i.e. an element g such that every nonzero element in F is a power of g), and compute the discrete logs for this base g .

The polynomial is irreducible because it is degree 3 and has no root in $Z/2$. The element x is a primitive root with

$$x^1 = x, x^2 = x^2, x^3 = x^2 + 1, x^4 = x^2 + x + 1$$

$$x^5 = x + 1, x^6 = x^2 + x, x^7 = 1,$$

from which the discrete logs can be read off.

4. Consider a Hill cipher with block size $N = 2$ in which *guns* is encrypted as *YGJC*. What can you say about the possible keys for this Hill cipher?

Let

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Doing the conversion to integers, we see that the given information is

$$\begin{aligned} 6a + 20b &= 24 \\ 13a + 18b &= 9 \end{aligned}$$

Analysing these equations modulo 26 of course, we see that $a = 11$ and $b = 7$ or 20 , and $c = 4$ and $d = 3$ or 16 . Forming the matrices and checking for invertibility we see that there are two possible keys:

$$K = \begin{bmatrix} 11 & 7 \\ 4 & 3 \end{bmatrix}.$$

and

$$K = \begin{bmatrix} 11 & 20 \\ 4 & 3 \end{bmatrix}.$$