

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