CS 812
Spring 2024
Homework #3

Due in class Monday, April 29, 2024

Rules for Homework. See Homework 1.

1. For this problem you are to use the number field sieve to factor $n = 65$.

   The form of n suggests using the field $\mathbf{Q}(i)$, where $i = \sqrt{-1}$. The algebraic integers in this field are the *Gaussian integers* $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$. It can be shown that $\mathbf{Z}[i]$ is a unique factorization domain in which every ideal is principal (has a single generator). Furthermore, the primes of $\mathbf{Z}[i]$ have an explicit description: $(1+i)$ is the unique prime ideal containing 2; if $p \equiv 1 \bmod 4$, then $a^2 + b^2 = p$ and $(a+bi)$, $(a-bi)$ are the prime ideals containing p; if $p \equiv 3 \bmod 4$, (p) is a prime ideal.

   a) Show by direct calculation that the units of $\mathbf{Z}[i]$ are $\pm 1, \pm i$. [Hint: multiply the equation $uv = 1$ by its conjugate, to get a constraint on the real and imaginary parts of u.]

   b) There is an "obvious" solution x to $x^2 + 1 = 65$. What is it? Note that $X^2 + 1$ is the defining polynomial for the extension $\mathbf{Q}(i)/\mathbf{Q}$. Show that ϕ, which sends i to x, is a ring homomorphism mapping $\mathbf{Z}[i]$ onto $\mathbf{Z}_n$.

   The idea of the number field sieve, in this case, is to find pairs $(a+bi, a+bx)$ for which both components factor into "small" primes (in $\mathbf{Z}[i]$ and $\mathbf{Z}$, respectively). Combine these pairs by multiplication, to get a new pair $((A + Bi)^2, C^2)$. Applying ϕ to the first component gives $(A + Bx)^2 \equiv C^2 \bmod n$, which we can exploit to split n.

   c) Try this, using the three pairs given by $(a, b) = (-7, 1), (-1, 1), (4, 3)$. [These were found by computer search.]

   Food for thought: Along with the two integer solutions to $x^2 + 1 = 65$, there are two other x for which $x^2 + 1 \equiv 0 \bmod 65$. Could we use one of these?

2. Along with the link to this assignment, our web page has a link to a note by the American cryptographer Howard Campaigne. Please read this. Campaigne was director of research for NSA, and also acquired some notoriety among UFOlogists for an article on decoding extraterrestrial messages. (Unfortunately, communication with little green men is outside the scope of our course.)

   a) How was the sequence on page 1 of the note generated?

   b) Describe what would happen if the sequence (generated using the recipe you found for a)) was continued forever. In particular, how long is the ultimate period, and how long is the "tail" (if any) that one would observe before entering the cycle?

   c) Describe a method that could be used to determine the rule for any similarly generated sequence. (What "similarly generated" means should be explained.)

3. Here is an old programmer's trick for swapping x and y without using any extra space:

$$\begin{aligned} x &:= x \oplus y; \\ y &:= x \oplus y; \\ x &:= x \oplus y. \end{aligned}$$

Here $\oplus$ denotes bitwise exclusive or (vector addition mod 2).

a) Explain why this works.

b) Suppose we try to do the same thing for $x, y \in \mathbf{Z}_n$, and replace $x \oplus y$ by a linear function $\alpha x + \beta y$. For which pairs (α, β) will this work? Explain why a) is accounted for by your answer.

c) Now, imagine using three arbitrary linear functions:

$$\begin{aligned} x &:= \alpha x + \beta y; \\ y &:= \gamma x + \delta y; \\ x &:= \epsilon x + \zeta y. \end{aligned}$$

Characterize the tuples $(\alpha, \ldots, \zeta) \in \mathbf{Z}_n^6$ for which the above code swaps $x, y \in \mathbf{Z}_n$. How many of them are there? Give an efficient algorithm for choosing a uniformly distributed "swapping tuple." (Hint: Look for a nice geometric description.)

d) (*) Extend the above theory to include nonlinear functions. It also might be interesting to explore generalizations to other kinds of structures, beyond abelian groups.

4. Consider the following scheme for generating a random point in projective n-space over $\mathbf{Z}_p$. (Here p is prime.) Choose an index i uniformly from $\{0, \ldots, n\}$, so that the point will be

$$(x_0 : \cdots x_{i-1} : 1 : x_{i+1} \cdots x_n).$$

Then, choose $x_0, \ldots, x_{i-1}, x_{i+1}, \ldots x_n$ independently and uniformly from $\mathbf{Z}_p$. The rationale for this scheme is that projective space is symmetric, so we should not care where the 1 goes. After that, the set of all points with 1 in the i-th component is just affine (i.e. ordinary) n-space over $\mathbf{Z}_p$. Discuss this scheme, considering number of random bits needed, output distribution, etc.