Number Theory and Cryptography
Homework 7 (due 4/23)

1. Factor the complex integer $x = 36 - 3i$ as a product of prime elements of $\mathbf{Z}[i]$. (Hint: It might be helpful to look at the norm of x.)

2. According to the Chinese remainder theorem, there is a unique number $a \in \mathbf{Z}_{200}$ such that $a = 3 \bmod 8$ and $a = 11 \bmod 25$. What is it?

3. Find all solutions of the equation $x^2 = 2$ in $\mathbf{Z}_{391}$. (Hint: $391 = 17 \cdot 23$.)

4. Find a greatest common divisor of the complex integers $7 + 5i$ and $2 - 8i$.

5. Explain why 1517 is composite, using the Miller-Rabin test.

6. State and prove an analogue of Euclidean division in $\mathbf{Z}[\sqrt{-2}]$.