Seek simplicity and distrust it. - Alfred North Whitehead.

1. Read F7 and F8.

2. Problems F7.2, F7.5

3. Find all units in $\mathbb{Z}[\sqrt{-1}]$ and in $\mathbb{Z}/p[x]$.

4. How many units are there mod 7, mod 49, and mod 21? How many units are there mod $p$, mod $p^2$ and mod $pq$ where $p$ and $q$ are distinct primes?

5. Prove $x^2 \equiv y^2 \mod p$ if and only if $x \equiv \pm y \mod p$. Explicitly justify each step using definitions and results from class. Determine the number of squares mod $p$.

6. A. Find the gcd of $a(x) = x^4 + 2x^3 + x + 3$ and $b(x) = 3x^3 + 5$ in $\mathbb{Z}/7[x]$.

    B. Find a solution $(u(x), v(x))$ to $a(x)u(x) + b(x)v(x) = \gcd(a(x), b(x))$.

7. Compute $(p-1)! \mod p$ for some small values of $p$, find a pattern and make a conjecture. Prove that your conjecture is correct.

8. Compute $(m-1)! \mod m$ for some small values of $m$ which are not prime. Find a pattern, make a conjecture, and prove that your conjecture is correct.

9. Decrypt WGVFKUGTBCHDHDKVICKTDIMQB which was encoded with the affine cipher using the information that the first two letters of the plaintext are “ga.”