Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. Let $p = 281$. Given the following polynomials $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}_p[x]$, use a computer program to compute polynomials $\mathbf{d}$, $\mathbf{u}$, $\mathbf{v}$ in $\mathbb{F}_p$ such that $\gcd(\mathbf{a}, \mathbf{b}) = \mathbf{d} = \mathbf{ua} + \mathbf{vb}$. Python classes for working with polynomial rings are given in the supplementary file `polynom.py`.

   (a) $\mathbf{a} = x^5 - x^2 + 6x - 14$
   $\mathbf{b} = x^3 + 9x^2 + x - 1$

   (b) $\mathbf{a} = x^6 + x^5 - x^4 + 6x^3 + 2x^2 - 5x + 10$
   $\mathbf{b} = x^7 + 2x^5 + 2x^4 - 2x^3 + 6x^2 - x + 2$

2. Let $p = 53$. For the following triples $(\mathbf{a}, \mathbf{b}, \mathbf{f})$, compute $\mathbf{ab}$ in the quotient ring $\mathbb{F}_p[x]/\mathbf{f}$. You may check your work with a computer, but these computations should be done **by hand**.

   (a) $\mathbf{a} = 4x^5 - x^4 + 25x^3 + 18x^2 + 45x + 10$, $\mathbf{b} = 1$, $\mathbf{f} = x^3$

   (b) $\mathbf{a} = 4x^5 - x^4 + 25x^3 + 18x^2 + 45x + 10$, $\mathbf{b} = 1$, $\mathbf{f} = x^3 - 1$

   (c) $\mathbf{a} = 3x + 2$, $\mathbf{b} = x + 22$, $\mathbf{f} = x^2 + x + 1$

3. Let $p = 37$, and let $\mathbf{f} = x^7 - 1$. For each $\mathbf{a}$ in $\mathbb{F}_p[x]/\mathbf{f}$, either find the inverse $\mathbf{a}^{-1}$ or explain why the inverse does not exist. A computer program is needed for some (but not all) of these.

   (a) $\mathbf{a} = 8$ (b) $\mathbf{a} = 0$ (c) $\mathbf{a} = x$ (d) $\mathbf{a} = x + 1$ (e) $\mathbf{a} = x + 2$ (f) $\mathbf{a} = x^2 - 1$ (g) $\mathbf{a} = x^2 + 1$ (h) $\mathbf{a} = x^3 + x^2 + 1$

4. Alice and Bob agree to use the NTRU cryptosystem with public parameters $(N, p, q, d) = (7, 37, 479, 2)$. Use a computer program to solve the following problems.

   (a) Alice chooses $\mathbf{f} = x^5 - x^4 + x^2 - x + 1$ and $\mathbf{g} = x^6 + x^4 - x^2 - x$ as her private key. What is her public key $\mathbf{h}$?

   (b) Bob wants to send the message $\mathbf{m} = 4x^6 - 18x^5 + 7x^2 + x + 1$ to Alice and selects $\mathbf{r} = x^6 + x^3 - x - 1$ as his random element. What is the corresponding ciphertext $\mathbf{c}$?

   (c) The next day, Alice receives the ciphertext $\mathbf{c} = 350x^6 + 4x^5 + 415x^4 + 221x^3 + 276x^2 + 464x + 197$ from Bob. What message did Bob send?