E. Dummit's Math 3527 ~ Number Theory I, Spring 2020 ~ Homework 7, due Wed Mar 11th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. Factor the given integers using the stated procedure (make sure to give enough detail so the computations can be followed):
   (a) $N = 5\,686\,741\,440\,097$ by looking for a Fermat factorization.
   (b) $N = 1\,032\,899\,106\,233$ by using Pollard's $(p-1)$-algorithm with $a = 2$.
   (c) $N = 1\,626\,641\,013\,131$ by using Pollard's ρ-algorithm with $a = 2$ and $p(x) = x^2 + 1$.

---

2. Use the Euclidean algorithm in each Euclidean domain to compute a greatest common divisor of each pair of elements, and then to write it as a linear combination of the elements:
   (a) The polynomials $x^6 - 1$ and $x^8 - 1$ in $\mathbb{R}[x]$.
   (b) The elements $43 - i$ and $50 - 50i$ in $\mathbb{Z}[i]$.
   (c) The elements $x^4 + 2x + 1$ and $x^3 + x$ in $\mathbb{F}_3[x]$.
   (d) The elements $11 + 27i$ and $-9 + 7i$ in $\mathbb{Z}[i]$.
   (e) The elements $9 + 43i$ and $22 + 10i$ in $\mathbb{Z}[i]$.

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

3. The goal of this problem is to explore a few aspects of the non-uniqueness of the quotient and remainder in the division algorithm in $\mathbb{Z}[i]$.
   (a) Let $a = 37+2i$ and $b = 11+2i$ in $\mathbb{Z}[i]$. Show that there are $q, r, q', r' \in \mathbb{Z}[i]$ such that $a = qb+r = q'b+r'$ with $N(r)$ and $N(r')$ both less than $\frac{1}{2}N(b)$, and with $r' \neq r$.

   One way we could try to solve the problem in part (a) is by always choosing the value of q that makes the remainder r have smallest norm. However:
   (b) Let $a = 1-7i$ and $b = 4+2i$. Show that, among all decompositions $a = qb+r$ with $q, r \in \mathbb{Z}[i]$, there are four different values of r which have smallest norm.

---

4. The goal of this problem is to prove that a finite integral domain is a field. So suppose R is a finite integral domain and let $r \in R$ be nonzero.
   (a) Show that $r^a = r^b$ for some positive integers $a < b$. [Hint: Consider the set $\{r, r^2, r^3, r^4, \dots\}$.]
   (b) Show that $r^k = 1$ for some positive integer k.
   (c) Show that r is a unit, and conclude that R is a field.

---

5. The goal of this problem is to prove that the ring $R = \mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain under its norm function $N(a + b\sqrt{-2}) = a^2 + 2b^2$.

   (a) Suppose that $c + d\sqrt{-2}$ is not zero. Show that $\dfrac{a + b\sqrt{-2}}{c + d\sqrt{-2}}$ can be written in the form $x + y\sqrt{-2}$ for rational numbers x and y.

   (b) With notation from part (a), let s be the closest integer to x and t be the closest integer to y. Set $q = s + t\sqrt{-2}$ and $r = (a + b\sqrt{-2}) - (s + t\sqrt{-2})(c + d\sqrt{-2})$. Prove that $N(r) \leq \dfrac{3}{4}N(c + d\sqrt{-2})$.

   (c) Show that R is a Euclidean domain.

   (d) [Optional] Adapt this proof to show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are also Euclidean domains under the absolute value of the field norm $\left|N(a + b\sqrt{D})\right| = \left|a^2 - Db^2\right|$.

   (e) Use the Euclidean algorithm in R to find the greatest common divisor of $33 + 5\sqrt{-2}$ and $8 + 11\sqrt{-2}$ in R, and then write it as a linear combination of these elements.

---

6. The goal of this problem is to show that $R = \mathbb{Z}[\sqrt{-3}]$ is not a Euclidean domain. Let $a = 2 + 2\sqrt{-3}$ and $b = 4$ and suppose that a and b have a greatest common divisor d in R.

   (a) Show that $N(d)$ must equal 4, 8, or 16.

   (b) Find all elements of norm 4, 8, or 16 in R, and show that none of them is a greatest common divisor of a and b. [Hint: Find two elements that must divide d, and two elements that d must divide.]

   (c) Deduce that R is not a Euclidean domain.
