E. Dummit's Math 3527 ~ Number Theory I, Spring 2023 ~ Homework 7, due Fri Mar 17th.

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. Submit scans of your responses via Canvas.

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) $N = 1084055561$ by looking for a Fermat factorization.

   (b) $N = 5686741440097$ by looking for a Fermat factorization.

   (c) $N = 1032899106233$ by using Pollard's $(p-1)$-algorithm with $a = 2$.

   (d) $N = 12038459$ by using Pollard's $(p-1)$-algorithm with $a = 2$.

   (e) $N = 1626641013131$ by using Pollard's ρ-algorithm with $a = 2$ and $p(x) = x^2 + 1$.

   (f) $N = 12038459$ by using Pollard's ρ-algorithm with $a = 2$ and $p(x) = x^2 + 1$.

---

2. Two of the following six integers are prime and the other four are composite:

$$\begin{aligned}
N_1 &= 1474512288873635866253234569665259057209898423127605097759586627754595366776247 41\\
N_2 &= 181724486732607374235034401344439931270145141565372874381350646276632766328969281\\
N_3 &= 258424126740178352128100370736889906817607518086806632752038758788555704304604649\\
N_4 &= 324234657928347051123113232023409710234012389751239847120398471917665655581200339\\
N_5 &= 408869971164328247524265450583823930434406844303142816841351879439544818685702841\\
N_6 &= 542408184634943257672698834917404611542248228873337459368210624910406937582942097
\end{aligned}$$

   (a) Try the Fermat test with $a = 2, 3, 5$ for each of these integers. (Stop if you find the integer is composite.)

   (b) Try the Miller-Rabin test with $a = 2, 3, 5$ for each of the integers remaining after part (a). (Stop if you find the integer is composite.)

   (c) Your results from parts (a)-(b) should have identified the four composite numbers. Why don't the results prove that the remaining two integers are actually prime?

---

3. For each element in each ring $\mathbb{Z}[\sqrt{D}]$, determine (i) whether it is a unit and if so find its multiplicative inverse, and (ii) whether it is irreducible and if not find a nontrivial factorization.

   (a) The elements $-i$, $3 + 2i$, $1 + i$, and $1 + 5i$ in $\mathbb{Z}[i]$.

   (b) The elements $1 + 2\sqrt{5}$, $9 + 4\sqrt{5}$, and $5 + \sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$.

---

4. 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 $11 + 27i$ and $-9 + 7i$ in $\mathbb{Z}[i]$.

   (c) The polynomials $x^3 + x^2 + 1$ and $x^4 + x$ in $\mathbb{R}[x]$.

   (d) The elements $43 - i$ and $50 - 50i$ in $\mathbb{Z}[i]$.

   (e) The elements $x^4 + 2x + 1$ and $x^3 + x$ in $\mathbb{F}_3[x]$.

   (f) The elements $9 + 43i$ and $22 + 10i$ in $\mathbb{Z}[i]$.

---

5. As proven on homework 2, the only possible primes of the form $a^n - 1$ are the Mersenne numbers $2^p - 1$ where p is a prime. The goal of this problem is to study the prime factorizations of Mersenne numbers.

   (a) Apply the Miller-Rabin test with $a = 2, 3, 5$ on $2^p - 1$ for $p = 11$, 13, 17, 19, 23, 29. You should find that three values are composite: why can you not conclude that the other three values are necessarily prime?

   (b) Use Pollard's ρ-algorithm with $a = 3$ and polynomial $p(x) = x^2 + 1$ to find the factorizations of the three values $2^p - 1$ you identitied as composite in part (a). (Note that the largest one has three prime factors; make sure to find all three by extending the computation past where the first prime factor is found.) How many steps are required to find the factorizations?

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

6. For all of the factorizations in problem 5, notice that all of the prime factors of $2^p - 1$ are congruent to 1 modulo p. The goal is now to prove this fact, which was first established by Euler.

   (a) Suppose that q is a prime that divides $2^p - 1$. Show that the order of 2 modulo q must equal p.

   (b) Suppose that q is a prime that divides $2^p - 1$. Show that $q \equiv 1 \pmod{p}$.
