E. Dummit's Math 3527 ~ Number Theory 1, Spring 2026 ~ Homework 7, due Fri Mar 13th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly and submit via Gradescope, making sure to select page submissions for each problem. Use of generative AI in any manner is not allowed on this or any other course assignments.

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

1. Factor the given integers using the stated procedure, making sure to give enough detail to show that you did actually use that method (just giving the factorization is not sufficient!):

   (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. Generate (however you like) three 10-digit, three 20-digit, three 30-digit, and three 40-digit numbers: one number should be prime, another should be a product of two primes of roughly equal sizes, and the third should be a product of three primes of roughly equal sizes.

   (a) Use the Fermat test (with three residues $a = 2, 3, 5$) and the Miller-Rabin test (with three residues $a = 2, 3, 5$) to test the primality of your integers. How effective are the tests?

   (b) Do the primality testing algorithms take noticeably longer for the larger numbers than the small ones? Briefly explain.

   (c) Factor the composite numbers using the Pollard $(p-1)$- and ρ-algorithms, stopping after a maximum of 1,000,000 steps. List the number of steps each algorithm takes to find a factor.

   (d) Do the algorithms take more steps for the larger numbers than the smaller ones? Briefly explain.

   (e) Is there a difference between the number of steps for products of two versus three primes? Briefly explain.

---

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

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

   (b) The elements $1 + 2\sqrt{5}$, $9 + 4\sqrt{5}$, $5 + \sqrt{5}$, $21 + 4\sqrt{5}$ 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. Let p be a prime.

   (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 $q \equiv 1 \pmod{p}$.

---

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

   (a) Suppose that $c + d\sqrt{-2}$ is not zero. Write $\dfrac{a + b\sqrt{-2}}{c + d\sqrt{-2}}$ in the form $x + y\sqrt{-2}$ for rational numbers x and y. [Hint: Rationalize the denominator.]

   (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) Deduce that R is a Euclidean domain.

   (d) 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 the gcd as a linear combination of these elements.

   Remark: By a similar argument, one may show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are also Euclidean domains.
