Intro to Number Theory (Fall 2024)
Midterm Practice Problems

Instructions: Write your name at the top. No notes, text, calculators, etc. are allowed. Please answer the questions in the space provided below. You may continue an answer on the back, but if you do so, please write SEE BACK in the space provided.

Notation: Unless specified otherwise, assume $n \in \mathbb{N}$.

Remarks: this is longer than the actual exam will be, but the difficulty and content of questions should be largely similar to the actual exam.

1. For each of the following sets (with addition and multiplication defined as usual), state whether it is (i) a ring; and (ii) a field. In the case it is not a ring or field, briefly explain why.
   (a) $\{a + b\sqrt{53} : a, b \in \mathbb{Q}\}$
   (b) $\frac{1}{2}\mathbb{Z} = \{\frac{a}{2} : a \in \mathbb{Z}\}$
   (c) the set of polynomials in x with integer coefficients and degree at most 4
2. For each of the following sets with specified operation, state whether it is a group or not. If it is not, briefly explain why.
   (a) the set of nonzero elements of $\mathbb{Z}/3\mathbb{Z}$, under multiplication
   (b) the set of nonzero elements of $\mathbb{Z}/4\mathbb{Z}$, under multiplication
   (c) the set of polynomials in x with integer coefficients, under composition
3. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. State definitions, as precisely as you can, for the following notation:
   (a) $b \mid a$
   (b) $a \equiv b \mod n$
4. Compute $\gcd(1234, 12345)$ using the Euclidean algorithm.
5. Find (with proof) all elements of norm 5 in $\mathbb{Z}[i]$.
6. Find a unit in $\mathbb{Z}[\sqrt{3}]$ which is not ± 1. (Justify that your answer is actually a unit.)
7. Find an irreducible non-unit element in $\mathbb{Z}[\sqrt{-5}]$ which does not lie in $\mathbb{Z}$. (Justify it is irreducible and non-unit.)
8. Show that 2 is irreducible in $\mathbb{Z}[\sqrt{-3}]$.
9. Find 2 distinct (not differing by units/ordering) of 4 into irreducibles in $\mathbb{Z}[\sqrt{-3}]$. (You do not need to prove your factors are irreducible, but briefly explain why the factorizations do not differ by units.)
10. Let $d \in \mathbb{Z}$. State what it means for $\mathbb{Z}[\sqrt{d}]$ to have the prime divisor property. For which d do know this property holds?
11. Show $x^2 + 3y^2 = n$ has no solutions over $\mathbb{Z}$ when $n \equiv 2 \bmod 3$.
12. Say the base 8 (also known as octal) representation of n is $a_m a_{m-1} \dots a_1 a_0$ (where $0 \le a_i \le 7$ for each i). Show that n is divisible by 7 if and only if $a_m + a_{m-1} + \cdots + a_1 + a_0$ is.
13. Compute $\phi(12)$, where ϕ denotes the Euler phi function.
14. Let p be a prime. Prove a formula for $\phi(p^2)$, where ϕ denotes the Euler phi function.
15. Compute an inverse of 3 mod 100. (You may, though are not required to, make use of the Euclidean algorithm; in either case, explain your work.)