MATH 4573: HOMEWORK 2

INSTRUCTOR: TYLER GENAO

Due: January 30, 2026.

This homework has two sections: the first section has the assigned problems that you will turn in to Gradescope for credit. The second section contains recommended and bonus problems, either from myself, the textbook or other sources. These latter problems are not graded for credit, but you may find them to be useful practice and/or interesting!

For any assigned problem in this homework, **you must show all of your work in order to receive full credit. Your solutions can only cite up to §1.5 of our notes. Everything else must be proven.**

1. Problems to Submit

Exercise 1. Say that an integer a is a *perfect square* if it is the square of an integer, i.e., $a = n^2$ for some $n \in \mathbb{Z}$. Prove that if $x, y \in \mathbb{Z}^+$ are odd, then $x^2 + y^2$ is not a perfect square.

Exercise 2. Prove that if an integer n is odd, then $n^2 - 1$ is divisible by 8. Show that if also $3 \nmid n$, then we have the stronger divisibility $24 \mid n^2 - 1$.

Exercise 3.

a) Show that if an integer $n > 0$ is a composite number, then it must have a prime divisor $p \in \mathbb{Z}^+$ which satisfies $p \leq \sqrt{n}$.

b) Use part a) to check by hand whether 283 is a prime number. (You may use a calculator to approximate $\sqrt{283}$.)

Exercise 4. This problem explores a special case of *Dirichlet's Theorem on Primes in Arithmetic Progressions.*

Theorem (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *Given positive coprime integers a and b, there exist infinitely many primes of the form $a + bk$.*

This exercise focuses on a proof for primes of the form $3 + 4k$ ($a = 3, b = 4$).

a) Show that a positive integer n of the form $3 + 4k$ has at least one prime factor of the same form.

b) Mimicking Euclid's proof of the infinitude of primes (see our notes, or [NZM91, Theorem 1.17]), use part a) to prove the following:

Theorem. *There are infinitely many primes of the form $3 + 4k$.*

(*Hint:* In mimicking this proof, construct an integer n of the form $3 + 4k$.)

Exercise 5. Use the Binomial Theorem to show that for each integer $n \geq 0$, one has

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Exercise 6. For this computational exercise, **you will need to submit your associated code as a text file onto Carmen.** In particular, your code must run without errors if pasted into SageCell by the class grader, and *automatically* print out the output you claim in your answer. Note that when you copy-paste your code into Carmen, it might mess some of the formatting up, so you may need to double-check that it works. The deadline for submitting the code is the same as this HW.

This exercise studies the **Mersenne primes.** These are the primes of the form $a^k - 1$ where $a, k \geq 2$ are integers.

a) Create `Sage` code for a function called `MersennePrimes`, which takes as input positive integers B and k, and outputs all Mersenne primes up to B of the form $a^k - 1$. Also include calculations with your function for $k = 2, 3, \ldots, 30$ when $B = 10000000$ (ten million).
b) What do you observe with your output from part a)? Make a conjecture based on it; you can also range over larger B and k. (one point)
c) Prove that if p is a Mersenne prime, then $p = 2^k - 1$ for some $k \geq 2$. (*Hint:* use the algebraic identity $1 + x + x^2 + \ldots + x^{n-1} = \frac{x^n - 1}{x - 1}$.)
d) Continuing part d), show that k must also be prime.
e) Do you think there are finitely or infinitely many Mersenne primes? (one point)

The Mersenne primes can be read about here: A000043.

Exercise 7. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From [NZM91, §1.3], pages 29–32: #9, 12, 13, 15, 22, 32.
From [NZM91, §1.4], pages 40–41: #2, 6.

Bonus Exercise 8. Prove the following result:

Theorem. *There are infinitely many primes of the form* $1 + 4k$.

Hint: Use the following special case of [NZM91, Theorem 2.12]:

Corollary. *For any integer* n *and any odd prime* p*, if* $p \mid (n^2 + 1)$ *then* p *is of the form* $1 + 4k$.

Then mimic Euclid's proof, constructing an integer n of the form $1 + (2k)^2$.

Bonus Exercise 9. This exercise will give a topological proof that there are infinitely many primes, due to H. Furstenberg.

Let us define a topology on $\mathbb{Z}$ as follows. Say that a subset $U \subseteq \mathbb{Z}$ is open if and only if it is a union of *arithmetic progressions,* i.e., sets of the form

$$S(a, b) := \{a + bn : n \in \mathbb{Z}\}.$$

a) Show that such a definition for open sets satisfies the axioms for a topology on $\mathbb{Z}$.
b) Show that for $a, b \in \mathbb{Z}$ one has

$$S(a,b) = \mathbb{Z} \smallsetminus \bigcup_{r=1}^{b-1} S(a+r, b).$$

Deduce that $S(a,b)$ is closed.
c) Show that

$$\mathbb{Z} \smallsetminus \{1,-1\} = \bigcup_{\text{prime } p} S(0,p).$$

Argue that $\mathbb{Z} \smallsetminus \{1,-1\}$ cannot be closed. Then using part b), conclude that there are infinitely many primes.

The following three exercises use *computational mathematics* to study the distribution of primes in the natural numbers. See also §1.5 of our notes.

Bonus Exercise 10. This exercise will attempt to convince ourselves that the *Prime Number Theorem* is true. Let us define the *prime counting function* $\pi\colon \mathbb{R} \to \mathbb{Z}^+$, where for each real number x, the integer $\pi(x)$ is the number of (positive) primes less than or equal to x.

Theorem (The Prime Number Theorem)**.** *One has*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

a) Create code that calculates $\pi(x)$ for any real number x.
b) Compare the values of $\pi(x)$ and $\frac{x}{\log(x)}$ for $x = 10, 10^2, \ldots, 10^{10}$, and analyze what is happening to these two values as x gets increasingly large.
∗c) Find and understand an elementary proof of the Prime Number Theorem.

Bonus Exercise 11. Given a pair of positive integers (a,b), let $\pi_{a,b}\colon \mathbb{R} \to \mathbb{Z}^+$ be the function such that $\pi_{a,b}(x)$ counts the number of primes $1 \le p \le x$ of the form $a + bk$. For example, $\pi_{1,3}(20) = 3$.

a) Using a computer, calculate $\pi_{3,4}(x)$ for $x = 10, 10^2, \ldots, 10^{10}$. (To reiterate, we are counting the number of primes $p \le x$ of the form $3 + 4k$.)
b) For each x above, compute the ratio $\pi_{3,4}(x)/\pi(x)$. (This is the proportion of primes in $[1,x]$ of the form $3 + 4k$.)
c) What does the limit

$$\lim_{x\to\infty} \frac{\pi_{3,4}(x)}{\pi(x)}$$

seem to equal? Make a conjecture for primes of the form $3 + 4k$ based on this.
d) Do the same analysis for primes of the form $1 + 4k$. Explore this for other a, b as well. Can you come up with a general conjecture for the proportion of primes of the form $a + bk$, where $a, b \in \mathbb{Z}^+$ are coprime?

Bonus Exercise 12. The following theorem is a conjecture based on Dirichlet's Theorem above on Primes in Arithmetic Progressions, vastly generalizing it.

Conjecture (The Bunyakovsky Conjecture)**.** *Let $f(x)$ be a polynomial with integer coefficients, satisfying the following three properties:*

i) The leading coefficient of $f(x)$ is positive;
ii) $f(x)$ is irreducible over $\mathbb{Z}$;
iii) $\gcd(f(1), f(2), f(3), \ldots) = 1$.[1]

Then there are infinitely many primes of the form $f(n)$ where n ranges over positive integers.

a) Show that Dirichlet's Theorem on Primes in Arithmetic Progressions is a special case of the Bunyakovsky Conjecture.
b) Show that the following well-known conjecture is a special case of the Bunyakovksy Conjecture:

Conjecture. *There are infinitely many primes of the form $n^2 + 1$.*

c) The Bunyakovsky Conjecture is currently open for all polynomials of degree greater than 1 satisfying $i) - iii)$ above. Pick your favorite polynomial in $\mathbb{Z}[x]$ and try to understand whether $f(n)$ is prime for various values of n. If your polynomial doesn't satisfy all of $i) - iii)$, what do you observe goes wrong?

Bonus Exercise 13. The Fundamental Theorem of Arithmetic is a statement about the elements of $\mathbb{Z}$ different from $0, \pm 1$. In comparison, not all commutative rings admit an analogous unique factorization theorem for their elements. This exercise explores a particular example of an *algebraic number ring* which fails to have unique factorization (see also §1.3 of our notes).

Consider the ring

$$R := \mathbb{Z}[\sqrt{-6}] := \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}.$$

Define a norm map $N \colon \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}_{\geq 0}$ via

$$N(a + b\sqrt{-6}) := (a + \sqrt{-6})(a - \sqrt{-6}) = a^2 + 6b^2.$$

a) Show that for $\alpha, \beta \in R$ we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Recall that an element $u \in R$ is a *unit* if there exists $v \in R$ with $uv = 1$.

b) Show that an element $\alpha \in R$ is a unit if and only if $N(\alpha) = 1$.

For elements $\alpha, \beta \in R$, we say that β *divides* α, written $\beta \mid \alpha$, if $\alpha = \beta\gamma$ for some $\gamma \in R$; call β a *proper divisor* of α if $1 < N(\beta) < N(\alpha)$. We say that a non-unit element $\alpha \in R$ is *irreducible* if whenever $\alpha = \beta\gamma$, one has that either β or γ is a unit.

c) Show that an element $\alpha \in R$ is irreducible iff α has no proper divisors. Thus, an irreducible element of R is analogous to a prime in $\mathbb{Z}$.
d) Using the previous parts, show that every non-unit element in R has a factorization into irreducible elements.

Part d) shows that, just like in $\mathbb{Z}$, all non-unit elements of $\mathbb{Z}[\sqrt{-6}]$ factorize into products of irreducibles. However, unlike $\mathbb{Z}$, not all elements of R have a *unique* factorization.

[1]Recall that $\gcd(a_1, a_2, \ldots, a_k)$ is the greatest *simultaneous* divisor of the integers $a_1, a_2, \ldots, a_k$, i.e., the largest integer $d \in \mathbb{Z}$ for which $d \mid a_1, d \mid a_2, \ldots, d \mid a_k$. Then $\gcd(a_1, a_2, \ldots)$ is the greatest common divisor between all of the a_i terms.

e) Observe that

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

Using the norm map, show that $2, 5, 2 + \sqrt{-6}$ and $2 - \sqrt{-6}$ are irreducible. Thus, 10 has two distinct factorizations into irreducible elements in $\mathbb{Z}[\sqrt{-6}]$.

We conclude from part e) that $\mathbb{Z}[\sqrt{-6}]$ does not have a "fundamental theorem of arithmetic." However, $\mathbb{Z}[\sqrt{-6}]$, and any algebraic number ring in general, will have a unique factorization theorem for its *ideals.* (This is true of any ring that is a *Dedekind domain.*)

References

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).