MATH 4573: HOMEWORK 2

INSTRUCTOR: TYLER GENAO

Due: February 2.

This homework has two sections: the first section has the problems that you'll turn in for credit. The second section contains recommended problems from the textbook, myself or other sources; you are not required to do these, but I recommend that you check them out.

For any problem in this assignment, **you must show all of your work in order to receive full credit.** Please do not use words such as "clear", "obvious" or "trivial" in your solutions. **Your solutions should not use theorems from sections which come after the day the homework was assigned.**

1. Problems to Submit

Exercise 1.

a) List all integers $1 \leq n \leq 100$ which are congruent to 1 mod 18.
b) Give a complete residue system modulo 13 comprised of multiples of 4.
c) Give a reduced residue system modulo 16. What is $\phi(16)$?
d) Give a reduced residue system modulo 11. For each representative r of this residue system, write down a number $x \in \mathbb{Z}$ for which $rx \equiv 1 \pmod{11}$.

Exercise 2. Recall that a *perfect square* $a \in \mathbb{Z}$ 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 $x^2 + y^2$ isn't a perfect square.

Exercise 3.

a) Show that if $n \in \mathbb{Z}^+$ 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 congruent to 3 modulo 4 (which is the case where $a = 3$ and $b = 4$).

a) Show that an integer $n \in \mathbb{Z}^+$ of the form $3 + 4k$ has at least one prime factor of the same form.
b) Mimicking Euclid's proof on the infinitude of primes (see [NZM91, Theorem 1.17]), use part a) to prove the following:

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

(*Hint:* Construct an n of the form $3 + 4k$.)

Exercise 5. Use the binomial theorem to show that for each $n \geq 0$,

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

Exercise 6. Show that if $n \in \mathbb{Z}$ 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 7. As you already know, for any real numbers x and y and for any integer $n > 0$, one usually has $(x + y)^n \neq x^n + y^n$. However, this expectation changes when considering integers modulo a prime p.

Show that for any integers $a, b \in \mathbb{Z}$, one has $(a + b)^p \equiv a^p + b^p \pmod{p}$.

Exercise 8. Show that for prime powers p^e, one has $\phi(p^e) = p^e - p^{e-1}$.

Exercise 9. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From the textbook, pages 29–32: $\#9, 12, 13, 15, 22, 32$.
Pages 40–41: $\#2, 6$.
Pages 56–57: $\#1 - 13$.

Bonus Exercise 10. Prove the following result:

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

Hint: Use the following special case of Theorem 2.12 from the book:

Corollary. *For any integer* $n \in \mathbb{Z}$ *and any odd prime* $p \in \mathbb{Z}^+$*, 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 11. 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 iff it is a union of nonconstant 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

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

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 two exercises will use *computational mathematics* to count the distribution of primes in the natural numbers $\mathbb{Z}^+$.

Bonus Exercise 12. 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 $x = 10, 10^2, \ldots, 10^{10}$; 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 13. Given a pair $(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$, let $\pi_{a,b}\colon \mathbb{R} \to \mathbb{Z}^+$ be the function such that $\pi_{a,b}(x)$ counts the number of primes $1 \leq p \leq x$ 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 $p \leq x$ 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 14. 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 $f(x) \in \mathbb{Z}[x]$ 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) $\gcd(f(1), f(2), f(3), \ldots) = 1$.

Then there are infinitely many primes of the form $f(n)$ where n ranges over $\mathbb{Z}^+$.

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 15. The Fundamental Theorem of Arithmetic is a special result which applies to elements $n \in \mathbb{Z}$ not equal to 0 or ± 1; however, 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.

Consider the ring

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

Define a norm $N \colon \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}_{\geq 0}$ 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 iff $N(\alpha) = 1$.

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, "irreducible" in R is an analogous notion to "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, this analogy breaks down when considering *uniqueness* of this factorization.

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 $\mathbb{Z}[\sqrt{-6}]$.

Therefore, $\mathbb{Z}[\sqrt{-6}]$ does not have a "unique factorization theorem" for its elements. 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 "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).