Set 8

(A) More on induction

(1) Show that for all integers $n \geq 1$, 9 divides $4 \cdot 16^n + 5 \cdot 25^n$.

(2) Using mathematical induction, prove that for all integers $n \geq 1$ we have

$$1 + 4 + 7 + \cdots + (3n-2) = \frac{n(3n-1)}{2}.$$

(3) Prove that any polygon can be triangulated; that is, you can draw some diagonals (lines connecting nonadjacent vertices) to split the polygon into a collection of triangles.

(4) True or false? If you cut the plane with n distinct lines, the interior of the regions bounded by the lines can be two-colored; that is, you can fill all regions with black and some white so that no two regions sharing a common edge are the same color. If true, prove it, and if false find a counterexample.

(5) Let f_n denote the n-th Fibonacci number. Show that $f_n \leq 2^n$ for every n. You may need to use strong induction.

(6) Show that $n! > 3^n$ for all $n \geq 7$. [Hint: here, you don't start your induction at $n = 1$!]

(7) Our next goal is to prove the fundamental theorem of arithmetic, given below.

Theorem 4. *Every integer $a > 1$ can be represented as a product of primes $a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, where $p_1 < p_2 < \cdots < p_s$, and this representation is unique.*

(i) Start by showing that, if p is a prime number and a, b are integers such that $p|ab$, then $p|a$ or $p|b$. [Hint: translate this to a statement about $\mathbb{Z}/p$, and use that $\mathbb{Z}/p$ is a field.]

(ii) Now prove the fundamental theorem of arithmetic by using strong induction.

(8) (For enthusiasts) Consider the following argument using mathematical induction. Is it correct?

Theorem. *In any group of finitely many people, any two people have the same eye color.*

Proof. We prove this by induction, showing that for any $n \geq 1$, in any group of n people, everyone has the same eye color. The base case $n = 1$ is clearly true. Suppose then that the statement is true for any group of n people. We must show it is true for any group of $n+1$ people. For convenience, let us label the members of our group of $(n+1)$ people as $A_1, A_2, \ldots, A_{n+1}$. Consider the groups of n people $\{A_1, A_2, \ldots, A_n\}$ and $\{A_2, A_3, \ldots, A_{n+1}\}$. By the induction assumption (that the statement is true for groups of n people), persons $A_1, A_2, \ldots, A_n$ all have the same eye color; and similarly persons $A_2, A_3, \ldots, A_{n+1}$ all have the same eye color. Since there is a person (e.g. A_2) belonging to both groups, in fact everyone in both groups must have the same eye color. □

(B) GCDs and primes in $\mathbb{Z}[i]$:

(1) Use the Gaussian Euclidean algorithm to find $\alpha, \beta \in \mathbb{Z}[i]$ such that $(1+5i)\alpha + (5-3i)\beta = 2$.

(2) Given $\alpha, \beta \in \mathbb{Z}[i]$, what would it mean for them to be relatively prime? Show that, if α and β are relatively prime, then there are $x, y \in \mathbb{Z}[i]$ such that $1 = \alpha x + \beta y$.

(3) Recall that, in $\mathbb{Z}$, a key property of prime numbers is that $p|ab \implies p|a$ or $p|b$. Prove an analogous property for primes in $\mathbb{Z}[i]$.

(4) Let $\alpha, \beta \in \mathbb{Z}[i]$ be relatively prime. Show that if for some $\gamma \in \mathbb{Z}[i]$ we have $\alpha|\gamma$ and $\beta|\gamma$, then $\alpha\beta|\gamma$. [Hint: start by multiplying an equation $\alpha x + \beta y = 1$ by γ.]

(5) Recall that the fundamental theorem of arithmetic states that every positive integer n can be written uniquely as a product of primes $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$. What would be an analogous statement is $\mathbb{Z}[i]$? Is it true?

(C) Modular arithmetic in $\mathbb{Z}[i]$

(1) Consider the system of residue classes $\mathbb{Z}[i]/(3+2i)$. How many elements does it have? Write down a set of representative elements, and find which element on your list represents $(2+5i)(3-2i)$. How many elements of $\mathbb{Z}[i]/(3+2i)$ are units? Determine the order of each unit. How many of these units are squares?

(2) What would be a good definition of "$\varphi(\alpha)$" for a Gaussian integer $\alpha \in \mathbb{Z}[i]$? For clarity, let us call this new function by φ_G.

(3) Show that if $\alpha \in \mathbb{Z}[i]$ is a nonzero Gaussian integer, and β is a unit in $\mathbb{Z}[i]/\alpha$, then $\beta^{\varphi_G(\alpha)} = 1$. [Hint: recall our general result about groups: the order of an element $a \in G$ divides $\#G$.]

(4) List all elements of $\mathbb{Z}[i]/(3+4i)$, and determine which ones are invertible. How many elements does this ring have?

(5) For $n = 2, 3, 4$, how many elements does $\mathbb{Z}[i]/n$ have? What is the formula for general n?

(6) For $\alpha = 1+i, 2+i, 3+2i, 4+3i, 5+2i$, how many elements does $\mathbb{Z}[i]/\alpha$ have? Any conjectures?

(7) Which of the following are primes in the ring $\mathbb{Z}[i]$: $2, 3, 5, 1+i, 2+3i, 3+4i, 7, 17$? [Hint: if $N(\alpha)$ is a prime number then α is prime in $\mathbb{Z}[i]$. Why?]

(8) Factor the Gaussian integers $5+3i$ and $7+3i$ as products of primes in $\mathbb{Z}[i]$. [Hint: begin by considering their norms, and recall that $N(\alpha\beta) = N(\alpha)N(\beta)$.]

The following problems are taken from Keith Conrad's notes on the Gaussian integers, available for free at `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf`. Be sure to have a look if you want to learn more about Gaussian integers!

(9) For $0 \neq \alpha \in \mathbb{Z}[i]$, we denote by $n(\alpha)$ the number of elements of $\mathbb{Z}[i]/\alpha$. Recall that if $\alpha = a + ib$, its *complex conjugate* is the Gaussian integer $\overline{\alpha} = a - ib$. Show that $n(\alpha) = n(\overline{\alpha})$.

(10) Suppose $0 \neq \alpha, \beta \in \mathbb{Z}[i]$. Suppose $n(\alpha) = r$ and $n(\beta) = s$. Pick representatives $x_1, \ldots, x_r$ for $\mathbb{Z}[i]/\alpha$ and representatives $y_1, \ldots, y_s$ for $\mathbb{Z}[i]/\beta$. Show that the $x_i + \alpha y_j$, where $i = 1, \ldots, r$ and $j = 1, \ldots, s$, form a complete set of representatives for $\mathbb{Z}[i]/\alpha\beta$, and show that there are no repetitions. Conclude that $n(\alpha\beta) = n(\alpha)n(\beta)$.

(11) Show that, for any $0 \neq \alpha \in \mathbb{Z}[i]$, we have $n(\alpha) = N(\alpha)$. [Hint: start by considering $n(\alpha\overline{\alpha})$.]

(12) Suppose π is a Gaussian prime. Show that $\varphi_G(\pi) = N(\pi) - 1$.

(D) The primitive root theorem: Our goal here is to understand and prove the following result.

Theorem 5. *Let p be a prime number. Then there is a unit u in $\mathbb{Z}/p$ with order $p-1$.*

Recall that everything in $\mathbb{Z}/p$ is a unit except 0.

(1) For a nonzero element $u \in \mathbb{Z}/p$, show that u has order $p-1$ if and only if $(\mathbb{Z}/p)^\times = H_u$, using the notation of Set 6 (B). This means that every element of $(\mathbb{Z}/p)^\times$ can be written as a power of u. Groups with this property are called *cyclic groups*, and hence Theorem 5 can be rephrased as "The group $(\mathbb{Z}/p)^\times$ is cyclic".

For the next problem, we will assume the following lemma[1], which we will prove later:

Lemma. *Let A be a finite abelian group. Suppose $a \in A$ has order m and $b \in A$ has order k. Then there is an element of A that has order* $\operatorname{lcm}(m,k)$.

(2) Since $(\mathbb{Z}/p)^\times$ is a finite group, amongst all the orders of all its elements there must be a maximal one. Call this maximal order m, and choose $u \in (\mathbb{Z}/p)^\times$ with order m (note: there may be more than one u with this property!). Show that the order of every $v \in (\mathbb{Z}/p)^\times$ must divide m. [Hint: argue by contradiction: suppose $v \in (\mathbb{Z}/p)^\times$ has order k, where k does not divide m. Then use the lemma.]

[1] A lemma is a fact that, although perhaps not very interesting by itself, can be used to prove a deeper result

(3) Show that every element of $(\mathbb{Z}/p)^\times$ is a root of the polynomial $x^m - 1$, and use this to argue that $m \geq p - 1$.

(4) Finish the proof of Theorem 5.

(E) Proof of the Lemma: The following chain of exercises proves the lemma. We will take A to be an abelian group, which we will write additively (this means that the operation in our group is "+" instead of "·", and our identity element is written as "0"). Given an integer $n > 0$ and an element $a \in A$, we will write na for $na = a + a + \cdots + a$ (n times), and when $n < 0$ the element na will mean $na = (-a) + (-a) + \cdots + (-a)$ (n times). Note that the order of a is the smallest integer $n > 0$ for which $na = 0$.

(1) We will first assume that m and k are relatively prime, so that $\operatorname{lcm}(m, k) = mk$. In this case, we will show that the element $u + v$ has order mk. We begin by letting t be the order of $u + v$. Show that $km(u + v) = 0$, and thus t divides km.

(2) Use the fact that $t(u + v) = 0$ to show that the order of tu is equal to the order of tv.

(3) On the other hand, show that the order of tu is $\operatorname{lcm}(m, t)/t$ and that the order of tv is $\operatorname{lcm}(k, t)/t$.

(4) Show that, for any two positive integers r and s, we have $\operatorname{lcm}(r, s) = rs/\gcd(r, s)$. Use this to conclude that, in the context of our problem, we have

$$m \gcd(k, t) = k \gcd(m, t).$$

(5) Finish the proof of the lemma in the case that $\gcd(m, k) = 1$. [Hint: if $\gcd(m, k) = 1$, and m divides ks, then m must divide s.]

(6) Proof the general result. [Hint: let $u' = \gcd(m, k)u$. Show that the order of u' is $m/\gcd(m, k)$, and hence u' and v have coprime orders, so we can apply the lemma to the pair (u', v). Part (4) might also be useful.]

(F) The sums of squares theorem: Some of these problems you may have already done before. If so, explain them to everyone at your table.

(1) Which integers n with $2 \leq n < 50$ can be expressed as $n = x^2 + y^2$ where x and y are integers?

(2) Which p with $2 \leq p < 50$ can be expressed as $p = x^2 + y^2$ where x and y are integers? Any patterns or conjectures? Show that all of these primes "split" in $\mathbb{Z}[i]$.

(3) Show that if n can be written as $n = x^2 + y^2$, where x and y are integers, then $n \equiv 1 \mod 4$.

(4) Show that if a prime p splits in $\mathbb{Z}[i]$, then we must have $p = x^2 + y^2$ for some integers x and y. [Hint: if $p = \alpha\beta$ then $N(p) = N(\alpha)N(\beta)$; then use uniqueness of prime factorization in $\mathbb{Z}$.]

(5) Show that a Gaussian integer α is prime if and only if $\mathbb{Z}[i]/\alpha$ is a field. [Hint: if α, β are coprime then $1 = \alpha x + \beta y$ for some $x, y \in \mathbb{Z}[i]$.]

(6) Suppose F is a field, and that $f(x) \in F[x]$ is a polynomial of degree $\leq d$. Show that $f(x)$ can have at most d roots. [Hint: argue by induction on d. If $a \in F$ were a root, we can apply the division algorithm to show that $(x - a)$ divides $f(x)$.]

(7) Suppose R is a commutative ring in which we have $p = 0$ for some prime number p. Then $(x + y)^p = x^p + y^p$ for every $x, y \in R$. [Hint: recall the binomial theorem, and the behavior of $\binom{p}{i}$ when p is prime.]

(8) Suppose p is a prime in $\mathbb{Z}$ with $p \equiv 1 \mod 4$. Show that, in $\mathbb{Z}[i]/p$, every element α satisfies $\alpha^p = \alpha$. [Hint: write $\alpha = a + ib$, use the previous result, as well as Fermat's little theorem.]

(9) Show that if p is a prime number with $p \equiv 1 \mod 4$ then $\mathbb{Z}[i]/p$ is not a field. [Hint: The last problem shows that every element of $\mathbb{Z}[i]/p$ is a root of $x^p - x$. How many elements are there in $\mathbb{Z}[i]/p$?]

(10) Conclude that if p is a prime number with $p \equiv 1 \mod 4$ then we have $p = x^2 + y^2$ for some integers x and y.

(G) Applications of the Primitive Root Theorem: At the end of Problem Set 6, we proved the following.

Theorem. *Let p be a prime number. Then there is a unit u in $\mathbb{Z}/p$ with order $p-1$.*

Such a unit u is called a *primitive root*, and the theorem above is sometimes referred to as the Primitive Root Theorem. Even if you did not get to prove this, you may assume this theorem is true for this exercise.

(1) For $p = 2, 3, 5, 7$, and 11, find a primitive root in $\mathbb{Z}/p$.

(2) For $p = 2, 3, 5, 7$ and 11, find how many of the units in $\mathbb{Z}/p$ are squares (we say a unit u is a square if $u = x^2$ for some other unit x). Any conjectures?

(3) For $p = 2, 3, 5, 7$ and 11, calculate $(p-1)! \mod p$. Any conjectures?

(4) Explain why the primitive root theorem tells us that the group $((\mathbb{Z}/p)^\times, \cdot)$ is, "in disguise", the same as the group $(\mathbb{Z}/(p-1), +)$. [Hint: do some small examples like $p = 3$ to wrap your head around this.]

(5) Can you rephrase your conjectures from (2) and (3) in the group $(\mathbb{Z}/(p-1), +)$? Can you prove them?

(6) How many of the units in $\mathbb{Z}/p$ are cubes?

(7) Can you say precisely what it means for two groups to be the same "in disguise"? In mathematical terminology two such groups are called *isomorphic*.

(8) What should it mean for $\mathbb{Z}/n$ to have a primitive root when n is not prime? Does that happen for $n = 4$? How about $n = 15$?

(H) More modular arithmetic

(1) Find all the units in $\mathbb{Z}/3[x]/(x^2+1)$ and $\mathbb{Z}/3[x]/(x^2+2)$. For each unit, list its powers and find its order. What is different about these examples? Do the same for $\mathbb{Z}/5[x]/(x^2+x+1)$.

(2) For a prime number p, let $f_p(x) = x(x-1)(x-2)\cdots(x-(p-1)) \in \mathbb{Z}/p[x]$. Compute $f_p(x)$ for $p = 2, 3, 5, 7$. Any conjectures?