1 Exercise 1: Sums of powers of divisors

1.1 Problem

Let $n$ be a positive integer. Let $k \in \mathbb{N}$. Prove that

$$\sum_{d \mid n} d^k = \prod_{p \text{ prime}} \left( p^{0k} + p^{1k} + \cdots + p^{v_p(n)k} \right).$$

Here, the summation sign $\sum_{d \mid n}$ means a sum over all positive divisors $d$ of $n$.

1.2 Solution

[...]
2 Exercise 2: Another version of Jacobi’s two-squares theorem

2.1 Problem

Let \( n \) be a positive integer. Prove that

\[
\text{(the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2) = 4 \text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4) - 4 \text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4).
\]

[Hint: The formula for the left hand side that we proved in class can be freely used.]

2.2 Solution

[...]

3 Exercise 3: Characterizing Gaussian primes

3.1 Problem

Let \( \pi \) be a Gaussian prime.

Prove the following:

(a) If \( \pi \) is unit-equivalent to an integer, then \( \pi \) is unit-equivalent to a prime\(^1\) of Type 3.

(Recall that a prime \( p \) is said to be of Type 3 if it is congruent to 3 modulo 4.)

Assume, from now on, that \( \pi \) is not unit-equivalent to any integer. Let \( (p_1, p_2, \ldots, p_k) \) be a prime factorization of the positive integer \( N(\pi) \). (Thus, \( p_1, p_2, \ldots, p_k \) are primes such that \( N(\pi) = p_1 p_2 \cdots p_k \).)

(b) Prove that \( \pi | p_i \) for some \( i \in \{1, 2, \ldots, k\} \).

Fix an \( i \in \{1, 2, \ldots, k\} \) such that \( \pi | p_i \).

(c) Prove that \( p_i = \pi \bar{\pi} \).

(d) Prove that \( p_i \) is a prime of Type 1 or of Type 2.

(Recall that a prime \( p \) is said to be of Type 1 if it is congruent to 1 modulo 4, and is said to be of Type 2 if it equals 2.)

3.2 Remark

This exercise yields that the Gaussian primes are the primes of Type 3 and the Gaussian prime divisors of the primes of Types 1 and 2 (up to unit-equivalence). Conversely, any of the latter are indeed Gaussian primes (as we proved in class). This completes the characterization of Gaussian primes.

\(^1\)The unqualified word “prime” always means a prime in the original sense, i.e., an integer \( p > 1 \) whose only positive divisors are 1 and \( p \).

Darij Grinberg, 00000000
dgrinber@umn.edu
3.3 Solution

[...]

4 Exercise 4: Gaussian integers modulo a Gaussian integer

4.1 Problem

For any Gaussian integer \( \tau \), we let \( \equiv \) be the binary relation on \( \mathbb{Z}[i] \) defined by

\[
\left( \alpha \equiv \beta \mod \tau \right) \iff (\alpha \equiv \beta \mod \tau).
\]

It is straightforward to see (just as in the case of integers) that this relation \( \equiv \) is an equivalence relation. (You don’t need to prove this.) We shall refer to the equivalence classes of this relation \( \equiv \) as the Gaussian residue classes modulo \( \tau \); let \( \mathbb{Z}[i] / \tau \) be the set of all these classes.

Let \( n \) be a nonzero integer.

Prove that the equivalence classes of the relation \( \equiv \) (on \( \mathbb{Z}[i] \)) are the \( n^2 \) classes \([a + bi]_n\) for \( a, b \in \{0, 1, \ldots, |n| - 1\} \), and that these \( n^2 \) classes are all distinct.

4.2 Remark

This exercise yields \( |\mathbb{Z}[i] / n| = n^2 = N(n) \) for any nonzero integer \( n \). This is \([ConradG, \text{Lemma 7.15}]\). (Conrad proves this “by example”; you can follow the argument but you should write it up in full generality.)

More generally, \( |\mathbb{Z}[i] / \tau| = N(\tau) \) for any nonzero Gaussian integer \( \tau \). This is proven in \([ConradG, \text{Theorem 7.14}]\) (using the above exercise as a stepping stone).

4.3 Solution

[...]

5 Exercise 5: A Fibonacci divisibility

5.1 Problem

Let \( \phi = \frac{1 + \sqrt{5}}{2} \) and \( \psi = \frac{1 - \sqrt{5}}{2} \) be the two (real) roots of the polynomial \( x^2 - x - 1 \). (The number \( \phi \) is known as the golden ratio.) It is easy to see that \( \phi + \psi = 1 \) and \( \phi \cdot \psi = -1 \).

Let \( \mathbb{Z}[\phi] \) be the set of all reals of the form \( a + b\phi \) with \( a, b \in \mathbb{Z} \).

(a) Prove that any \( \alpha, \beta \in \mathbb{Z}[\phi] \) satisfy \( \alpha + \beta \in \mathbb{Z}[\phi] \) and \( \alpha - \beta \in \mathbb{Z}[\phi] \) and \( \alpha \beta \in \mathbb{Z}[\phi] \).
(In the terminology of abstract algebra, this is saying that $\mathbb{Z}[\phi]$ is a subring of $\mathbb{R}$.)

(b) Prove that every element of $\mathbb{Z}[\phi]$ can be written as $a + b\phi$ for a unique pair $(a, b)$ of integers. (In other words, if four integers $a, b, c, d$ satisfy $a + b\phi = c + d\phi$, then $a = c$ and $b = d$.)

Given two elements $\alpha$ and $\beta$ of $\mathbb{Z}[\phi]$, we say that $\alpha \mid \beta$ in $\mathbb{Z}[\phi]$ if and only if there exists some $\gamma \in \mathbb{Z}[\phi]$ such that $\beta = \alpha\gamma$. Thus, we have defined divisibility in $\mathbb{Z}[\phi]$. Basic properties of divisibility of integers (such as Proposition 2.2.4) still apply to divisibility in $\mathbb{Z}[\phi]$ (with the same proofs).

(c) If $a$ and $b$ are two elements of $\mathbb{Z}$ such that $a \mid b$ in $\mathbb{Z}[\phi]$, then prove that $a \mid b$ in $\mathbb{Z}$.

Let $(f_0, f_1, f_2, \ldots)$ be the sequence of nonnegative integers defined recursively by

$$f_0 = 0, \quad f_1 = 1, \quad \text{and} \quad f_n = f_{n-1} + f_{n-2} \quad \text{for all} \quad n \geq 2.$$

This is the so-called Fibonacci sequence (and continues with $f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$ etc.).

It is well-known (Binet’s formula) that

$$f_n = \frac{\phi^n - \psi^n}{\sqrt{5}} \quad \text{for all} \quad n \geq 0.$$

(You don’t need to prove this; there is a completely straightforward proof by induction on $n$.)

(d) Prove that $f_d \mid f_{dn}$ for any nonnegative integers $d$ and $n$.

[Hint: Lemma 2.10.11 (a) holds not just for integers.]

5.2 REMARK

This exercise (specifically its part (d)) is an example of how a property of integers (here, $f_d \mid f_{dn}$) can often be proved by working in a larger domain (in our case, $\mathbb{Z}[\phi]$). Another example is our study of sums of two perfect squares using Gaussian integers (done in class). There are various others. While part (d) of this exercise has fairly simple solutions using integer arithmetic alone, some other properties of Fibonacci numbers are best understood by means of working in $\mathbb{Z}[\phi]$. For example, if $p \neq 5$ is a prime, then one of the two Fibonacci numbers $f_{p-1}$ and $f_{p+1}$ is divisible by $p$, while the other is $\equiv 1 \mod p$.

5.3 SOLUTION

[...]
6 Exercise 6: Non-unique factorization in $\mathbb{Z}[\sqrt{-3}]$

6.1 Problem

We let $\sqrt{-3}$ denote the complex number $\sqrt{3}i$.

Let $\mathbb{Z}[\sqrt{-3}]$ be the set of all complex numbers of the form $a + b\sqrt{-3}$ with $a, b \in \mathbb{Z}$. These complex numbers are called the 3-Gaussian integers.

It is easy to see that the set $\mathbb{Z}[\sqrt{-3}]$ is closed under addition, subtraction and multiplication (i.e., that any $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$ satisfy $\alpha + \beta \in \mathbb{Z}[\sqrt{-3}]$ and $\alpha - \beta \in \mathbb{Z}[\sqrt{-3}]$ and $\alpha\beta \in \mathbb{Z}[\sqrt{-3}]$). (In the terminology of abstract algebra, this is saying that $\mathbb{Z}[\sqrt{-3}]$ is a subring of $\mathbb{C}$.)

It is also easy to see that each element of $\mathbb{Z}[\sqrt{-3}]$ can be written as $a + b\sqrt{-3}$ for a unique pair $(a, b)$ of integers.

(a) Prove that each 3-Gaussian integer $\alpha$ satisfies $N(\alpha) \in \mathbb{N}$ and $N(\alpha) \neq 2 \mod 3$.

(Recall that $N(\alpha)$ is defined for every complex number $\alpha$, and thus for every 3-Gaussian integer $\alpha$, since 3-Gaussian integers are complex numbers.)

Given two elements $\alpha$ and $\beta$ of $\mathbb{Z}[\sqrt{-3}]$, we say that $\alpha \mid \beta$ in $\mathbb{Z}[\sqrt{-3}]$ if and only if there exists some $\gamma \in \mathbb{Z}[\sqrt{-3}]$ such that $\beta = \alpha\gamma$. Thus, we have defined divisibility in $\mathbb{Z}[\sqrt{-3}]$. Basic properties of divisibility of integers (such as Proposition 2.2.4) still apply to divisibility in $\mathbb{Z}[\sqrt{-3}]$ (with the same proofs).

If $\alpha \in \mathbb{Z}[\sqrt{-3}]$, then a 3-Gaussian divisor of $\alpha$ shall mean a $\beta \in \mathbb{Z}[\sqrt{-3}]$ such that $\beta \mid \alpha$ in $\mathbb{Z}[\sqrt{-3}]$.

We define the notions of “inverse”, “unit” and “unit-equivalent” for 3-Gaussian integers as we did for Gaussian integers.

A nonzero 3-Gaussian integer $\pi$ that is not a unit is called a 3-Gaussian prime if each 3-Gaussian divisor of $\pi$ is either a unit or unit-equivalent to $\pi$.

(b) List all the 3-Gaussian integers having norms $< 4$.

(c) List all units in $\mathbb{Z}[\sqrt{-3}]$.

(d) Prove that $2$, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are 3-Gaussian primes.

(e) Prove that $2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$.

(f) Define two 3-Gaussian integers $\alpha$ and $\beta$ by $\alpha = 2$ and $\beta = 1 + \sqrt{-3}$. Prove that there exist no 3-Gaussian integers $\gamma$ and $\rho$ such that $\alpha = \gamma \beta + \rho$ and $N(\rho) < N(\beta)$.

[Hint: Your list in part (b) should contain 5 entries. Your list in part (c) should contain 2 entries: Unlike the ring $\mathbb{Z}[i]$ with its 4 units, the ring $\mathbb{Z}[\sqrt{-3}]$ has only 2 units.

For (d), discuss the norm of any possible 3-Gaussian divisor.]

6.2 Remark

Parts (d) and (e) of this exercise show that unique factorization into primes is not automatically preserved when we extend a number system. Neither is division with remainder, as part (f) illustrates (though we already have seen the geometric reason for this in class). (Neither is the existence of a well-behaved greatest common divisor.)
6.3 Solution

[...]

REFERENCES