Teoria Aritmética de Números II – Prova II

Regras:

- Você pode fazer conjecturas, ou presumir que conjecturas conhecidas valem (não significa que você vai, ou que não vai, precisar disso!);
- Ao usar algum Teorema ou Lema:
  - se for simples, demonstre;
  - se não for simples, cite a fonte (não a Internet!), ou tente fazer uma demonstração parcial, ou em alto nível;

1 A norma é um baú de diversões

A norma define classes de equivalência em $\mathbb{Z}[\sqrt{d}]$; podemos denotar $[k] = \left\{ y \in \mathbb{Z}[\sqrt{d}] \ : \ N(y) = k \right\}$, para todo $k \in \mathbb{Z}$.

Denotaremos a união de todas classes de equivalências por $N(\mathbb{Z}[\sqrt{d}])$.

Agora definimos a operação $\boxtimes$:

$$[x] \boxtimes [y] = \left\{ z \in \mathbb{Z}[\sqrt{d}] \ : \ N(z) = N(x)N(y) \right\}$$

(Há claramente um abuso de notação, onde x e $[x]$ se confundem, mas é inócuo.)

Outra definição interessante é a do fatorial de uma classe de equivalência,

$$[x]! = \left\{ z \in \mathbb{Z}[\sqrt{d}] \ : \ N(z) = N(x)! \right\}$$

Responda (dê suas respostas em casos, dependendo do valor de d – trate pelo menos os casos $d = -1$. $d > 0$, $d < -1$):

a) O que pode ser dito a respeito do tamanho dos conjuntos $[x] \boxtimes [y]$, $([x] \boxtimes [y]) \cap \mathbb{Z}$, $([x] \boxtimes [y]) \setminus \mathbb{Z}$, $[x]!$, $[x]! \cap \mathbb{Z}$, e $[x]! \setminus \mathbb{Z}$?

b) E quanto a métodos para determinar membros destes conjuntos?

c) Considere as definições ligeiramente modificadas:

- $[k]^* = \left\{ a + b\sqrt{d} \ : \ N(a + b\sqrt{d}) = k, \ |a|, |b| < k \right\}$, para todo $k \in \mathbb{Z}$. (Não mais uma partição, mas os conjuntos $[k]$ estão bem definidos)
- $[k]_q = \left\{ y \in \mathbb{Z}[\sqrt{d}] \ : \ N(y) \equiv k \pmod{q} \right\}$.

Refaça os itens (a) e (b), usando estas definições.

2 Representações diferentes

Suponha que, ao invés da representação que estudamos para elementos em corpos quadráticos, onde $a + b\sqrt{d}$ é representado por $\left(\begin{smallmatrix} a & bd \\ b & a \end{smallmatrix}\right)$, usemos uma das duas a seguir:

$$\begin{pmatrix} a & bd & 0 \\ b & a & 0 \\ 0 & 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & bd & 0 \\ b & a & cd \\ 0 & c & a \end{pmatrix}$$

- Que elementos são representados? Quem são norma, traço, e como definimos elementos conjugados? (Lembre-se que, da forma como definimos durante o curso, $\mathbb{Q}[\sqrt{k}]$ é um corpo – a representação deve preservar as propriedades de corpo – verifique se ainda temos um corpo, ou se isso só acontece em alguns casos) Se não for um corpo, identifique que estrutura temos.
- Quem são os inteiros nesse corpo? Caso não seja, faz sentido definir inteiros nesta estrutura?
- Qual o impacto sobre as demonstrações que fizemos (nas notas de aula)?

3 Teorema de Liouville

Demonstre o Teorema de Liouville: se r é raiz de

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0,$$

com $a_i \in \mathbb{Z}$, $a_0 \neq 0$ então existe $\delta > 0$, tal que para qualquer racional $\frac{p}{q} \neq r$, com $q > 0$,

$$\left| r - \frac{p}{q} \right| > \frac{\delta}{q^n}$$

4 Um número não algébrico

Prove que o número

$$\sum_{n=1}^{\infty} 2^{-n!}$$

é transcendental.

5 Primos e irredutíveis

Prove que, se p é primo, então as afirmações a seguir são equivalentes:

- p é soma de dois quadrados
- p é redutível em $\mathbb{Z}[i]$

6 Complete...

A quantidade total de polinômios irredutíveis de grau n módulo p é

$$\frac{1}{n}\left(p^n - \sum_{q_1} p^{n/q_1} + \sum_{q_1,q_2} p^{n/q_1 q_2} + \sum_{q_1,q_2,q_3} p^{n/q_1 q_2 q_3}\right),$$

onde as somas são sobre os fatores primos q_i de n. A seguir há um rascunho incompleto de uma demonstração disso. Expanda esse rascunho, tornando-o mais claro e completando-o. (*Não* dê outra demonstração – complete esta, tornando-a clara!)

Se $x^{p^n} - x$ é fatorado em um produto de irredutíveis, e m é o grau de um desses fatores, sabemos que $m \mid n$. Da mesma forma, qualquer irredutível de grau m deve ser um dos fatores. Denote por ϕ_n a quantidade de polinômios irredutíveis módulo p de grau n. Usando funções aritméticas, chegamos ao resultado.

7 Convoluímos em um grupo?

As funções aritméticas multiplicativas formam um grupo, se usarmos como operação a convolução de Dirichlet?