Teoría de números algebraicos
Tarea 1

Alexey Beshenov (alexey.beshenov@cimat.mx)

19 de agosto de 2020

Fecha límite: viernes, 28 de agosto.

Ejercicio 1.1. Para $d \geq 3$ libre de cuadrados demuestre que 2 es irreducible, pero no es primo en los anillos

a) $\mathbb{Z}[\sqrt{-d}]$,

b) $\mathbb{Z}[\sqrt{d}]$ para $d \equiv 1 \pmod 4$.

Concluya que estos no son dominios de factorización única.

Solución. Primero, para la irreducibilidad de 2, la norma sobre $\mathbb{Z}[\sqrt{-d}]$ viene dada por $a^2 + db^2$. Tenemos $N(2) = 4$, y se ve que para $d \geq 2$ no hay elementos de norma 2. Esto implica que 2 es irreducible.

En el anillo $\mathbb{Z}[\sqrt{d}]$ con $d \equiv 1 \pmod 4$ la norma viene dada por

$$a^2 - db^2 \equiv a^2 - b^2 \pmod 4.$$

Los cuadrados módulo 4 son 0 y 1, y de allí se ve que $a^2 - b^2 \not\equiv 2 \pmod 4$. Esto demuestra la irreducibilidad de 2 en el caso b).

Si d es par, notamos que $2 \mid \sqrt{-d}\sqrt{-d}$, pero $2 \nmid \sqrt{-d}$ (aquí usamos que $4 \nmid d$). Si d es impar, entonces $2 \mid (1 + \sqrt{-d})(1 - \sqrt{-d})$, pero $2 \nmid 1 \pm \sqrt{-d}$. Esto demuestra que 2 no es primo en los anillos $\mathbb{Z}[\sqrt{-d}]$.

De la misma manera, para d impar se tiene $2 \mid (1 + \sqrt{d})(1 - \sqrt{d})$, pero $2 \nmid (1 \pm \sqrt{d})$. Esto demuestra que 2 no es primo en $\mathbb{Z}[\sqrt{d}]$ con d impar.

Recordemos que en un dominio de factorización única todo irreducible debe ser primo, así que acabamos de probar que los anillos en cuestión no tienen factorización única. □

Ejercicio 1.2. Sea $p \equiv 1 \pmod 3$ un primo racional. Usando la factorización única en $\mathbb{Z}[\zeta_3]$, demuestre que los números $u, v \in \mathbb{Z}$ en la expresión $4p = u^2 + 27v^2$ están bien definidos salvo el signo.

Solución. Supongamos que se tiene

$$4p = u^2 + 3v^2 = u'^2 + 3v'^2,$$

donde

$$v \equiv v' \equiv 0 \pmod 3.$$

Notamos que necesariamente

$$u \equiv v \pmod 2, \quad u' \equiv v' \pmod 2,$$

y además, $3 \nmid u$, $3 \nmid u'$. Un pequeño cálculo demuestra que

$$p = \pi\,\overline{\pi} = \pi'\,\overline{\pi'},$$

donde

$$\pi = \frac{u+v}{2} + v\zeta_3, \quad \pi' = \frac{u'+v'}{2} + v'\zeta_3$$

son primos, ya que tienen norma p. La factorización única implica que

$$\pi \sim \pi' \quad \text{o} \quad \pi \sim \overline{\pi'}.$$

Calculamos que

$$\overline{\pi} = \frac{u-v}{2} - v\zeta_3.$$

Entonces, cambiando el signo de v, podemos asegurarnos de que $\pi \sim \pi'$; es decir, $\pi = \epsilon\pi'$ con $\epsilon \in \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$. Consideremos una por una las seis posibilidades.

- Si $\epsilon = +1$, entonces

  $$\frac{u+v}{2} + v\zeta_3 = \frac{u+v}{2} + v'\zeta_3,$$

  así que $v' = v$ y $u' = u$.

- Si $\epsilon = -1$, entonces

  $$\frac{u+v}{2} + v\zeta_3 = -\frac{u+v}{2} - v'\zeta_3,$$

  de donde $v' = -v$ y $u = -u$.

- Si $\epsilon = \zeta_3$, se obtiene

  $$\frac{u+v}{2} + v\zeta_3 = -v' + \frac{u'-v'}{2}\zeta_3.$$

  Esto implicaría que $u = -2v' - v$, pero luego $3 \mid u$, y no es el caso.

- El caso de $\epsilon = -\zeta_3$ se descarta de manera similar.

- En fin, si $\epsilon = \pm\zeta_3^2$, entonces $\pi = \pm\zeta_3^2\pi'$ implica que $\pi' = \pm\zeta_3\pi$, y este caso ya fue considerado.

Podemos concluir que $\epsilon = \pm 1$, lo que implica que $u = \pm u'$ y $v = \pm v'$. $\square$

Ejercicio 1.3. Verifique sin computadora si la congruencia

$$x^3 \equiv 2 + 3\zeta_3 \pmod{23}$$

tiene solución en $\mathbb{Z}[\zeta_3]$.

Sugerencia: en total en $(\mathbb{Z}[\zeta_3]/(23))^\times$ *habrá* $\frac{23^2-1}{3} = 176$ *cubos y no es una buena idea enumerarlos uno por uno...*

En general, dado un primo racional $p \equiv 2 \pmod 3$, ¿cuándo $2 + 3\zeta_3$ es un cubo módulo p?

Solución. Notamos que $N(2 + 3\zeta_3) = 7$ es un primo racional, así que $2 + 3\zeta_3$ es un primo en $\mathbb{Z}[\zeta_3]$. Además, $2 + 3\zeta_3 \equiv 23 \equiv 2 \pmod 3$; se trata de primos primarios y se aplica la reciprocidad cúbica

$$\left(\frac{2 + 3\zeta_3}{23}\right)_3 = \left(\frac{23}{2 + 3\zeta_3}\right)_3.$$

Recordemos que $\mathbb{Z}[\zeta_3]/(2+3\zeta_3) \cong \mathbb{F}_7$, y por lo tanto la pregunta se reduce a ver si 23 es un cubo módulo 7. Hay solo $(7 - 1)/3 = 2$ cubos módulo 7, y estos son claramente ± 1. Tenemos $23 \equiv 2 \pmod 7$. Entonces, la respuesta es negativa.

En general, para un primo racional $p \equiv 2 \pmod 3$ el número $2 + 3\zeta_3$ es un cubo módulo p si y solamente si $p \equiv \pm 1 \pmod 7$. □

Ejercicio 1.4. Encuentre las soluciones enteras de $y^2 = x^3 - 4$.

Sugerencia: $y^2 + 4 = (y + 2i)\,(y - 2i)$.

Solución. Primero un *spoiler*: una búsqueda indica que hay cuatro soluciones

$$(x, y) = (2, \pm 2),\ (5, \pm 11),$$

pero hay que verificar que no hay otras. Para esto factorizamos en $\mathbb{Z}[i]$

$$x^3 = (y + 2i)\,(y - 2i).$$

Primero, supongamos que y es impar. Si un primo de Gauss π divide a $y + 2i$ e $y - 2i$, entonces $\pi \mid 4i$, y por lo tanto $\pi \sim 1 + i$. Pero y es impar, así que $y \pm 2i \equiv 1 \pmod{1 + i}$. Esto implica que

$$\operatorname{mcd}(y + 2i, y - 2i) = 1.$$

La factorización única en $\mathbb{Z}[i]$ nos permite concluir que

$$y + 2i = u\,(a + bi)^3,$$

donde $u \in \mathbb{Z}[i]^\times$. Todas las unidades en $\mathbb{Z}[i]$ son cubos, así que podemos asumir que $u = +1$. Escribamos

$$y + 2i = (a + bi)^3 = a^3 - 3ab^2 + (3a^2b - b^3)\,i = a\,(a^2 - 3b^2) + b\,(3a^2 - b^2)\,i.$$

De la ecuación $2 = b\,(3a^2 - b^2)$ se ve que las soluciones enteras son $(a, b) = (\pm 1, 1)$ y $(\pm 1, -2)$. Estas corresponden a $y = \pm 2$ (pero y es impar, así que este caso se puede descartar por el momento) y $y = \pm 11$.

Ahora bien, supongamos que y es par. Analizando la ecuación $y^2 = x^3 - 4$, se ve que la máxima potencia de 2 que puede dividir a y^2 es 4, así que $y = 2y'$, donde $2 \nmid y'$. Se obtiene

$$x^3 = 4\,(y' + i)\,(y' - i).$$

Aquí

$$\mathrm{mcd}(y' + i, y' - i) = 1 + i.$$

Entonces, podemos escribir

$$x^3 = 2^3 \cdot \frac{y' + i}{1 + i} \cdot \frac{y' - i}{1 - i},$$

donde los factores son coprimos. Esto implica que

$$\frac{y' + i}{1 + i}$$

es un cubo. Escribamos

$$y' + i = (1 + i)\,(a + bi)^3 = (a - b)\,(a^2 + 4ab + b^2) + (a + b)\,(a^2 - 4ab + b^2)\,i.$$

Se sigue que

$$a + b = \pm 1, \quad a^2 - 4ab + b^2 = \mp 1.$$

Las soluciones enteras son $(a, b) = (0, -1), (-1, 0)$, y estas nos dan $y' = \pm 1$, así que $y = \pm 2$. □

Ejercicio 1.5. Consideremos la ecuación $x^2 - 7y^2 = n$, donde

$$n = 2, 3, 4, 5, 6, 7, 8, 9, 10.$$

¿Para cuáles de estos n existen soluciones enteras? Demuestre que en este caso hay un número infinito de ellas.

Solución. Primero consideremos la ecuación

$$x^2 - 7y^2 = 1.$$

Una solución no trivial es $(8, 3)$. Esta corresponde a la unidad

$$u = 8 + 3\sqrt{7} \in \mathbb{Z}[\sqrt{7}]^\times.$$

Luego, $\pm u^k$ para todo $k \in \mathbb{Z}$ son también unidades, y son diferentes: $u^k = u^\ell$ para $k \neq \ell$ sucede solamente cuando $u = \pm 1$.

En realidad, se puede verificar que u es la unidad fundamental y

$$\mathbb{Z}[\sqrt{7}]^\times = \{\pm 1\} \times \langle u \rangle,$$

pero esto no es necesario para el ejercicio.

De la misma manera, una solución de $x^2 - 7y^2 = n$ corresponde a un elemento $\alpha = x + y\sqrt{7}$ con $N(\alpha) = n$, y luego $N(u^k\alpha) = N(\alpha) = n$, así que los números

$$x' + y'\sqrt{7} = u^k\alpha$$

para diferentes k nos dan diferentes soluciones. Esto demuestra que si hay una solución de $x^2 - 7y^2 = n$, entonces habrá un número infinito de ellas.

Reduciendo módulo 7 se obtiene $x^2 \equiv n \pmod 7$. Los cuadrados módulo 7 son 1, $2 \equiv 3^2$ y 4. Esto demuestra que para $n = 3, 5, 6, 10$ no hay soluciones. Por otra parte, reduciendo módulo 4, notamos que $x^2 - 7y^2 \equiv x^2 + y^2 \pmod 4$, así que $n \not\equiv 3 \pmod 4$. De esta manera descartamos $n = 3$ y 7.

Nos quedan $n = 2, 4, 8, 9$, y para estos valores es fácil encontrar una solución. Notamos que si n es un cuadrado, entonces existe una solución obvia $(x, y) = (\sqrt{n}, 0)$, así que para $n = 4, 9$ habrá soluciones.

Para $n = 2$ se encuentra la solución $(3, 1)$ que corresponde a $N(3+\sqrt{7}) = 2$. Luego

$$N((3 + \sqrt{7})^3) = N(3 + \sqrt{7})^3 = 8.$$

Calculamos que

$$(3 + \sqrt{7})^3 = 90 + 34\sqrt{7},$$

así que $(90, 34)$ es una solución para $n = 8$. También se puede notar que $(6, 2)$ es una solución. □