Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática

Ayudante: Nicholas Mc-Donnell
Email: namcdonnell@uc.cl

Solución Ayudantía 1

Álgebra I - MAT2227

Fecha: 2019/08/13

1) Dado p primo, demuestre que $\sqrt{p}$ es irracional usando descenso infinito.

Demostración. Asumamos que $\sqrt{p}$ es racional, o sea, existen $a, b \in \mathbb{N}$[1] tales que $\sqrt{p} = \frac{a}{b}$, se reescribe la ecuación de la siguiente forma:

$$b^2 p = a^2 \tag{1}$$

Se nota que $p \mid a^2$, por teorema visto en clase si $p \mid a \cdot a$ entonces $p \mid a$ o $p \mid a$, por lo que $a = pa_1$, donde $a_1 \in \mathbb{N}$ y $a_1 < a$. Volviendo a reescribir la ecuación se tiene lo siguiente:

$$b^2 p = p^2 a_1^2$$
$$\therefore b^2 = a_1^2 p$$

Con eso, se ve que se puede usar el mismo argumento anterior, y con esto se tiene que $p \mid b$, por lo que $b = pb_1$, con $b_1 \in \mathbb{N}$ y $b_1 < b$. Se reescribe la ecuación y se tiene lo siguiente:

$$b_1^2 p = a_1^2$$

Se puede ver que está es la misma ecuación que (1), pero con distintas variables, por lo que se puede repetir el proceso para generar $a_2, b_2 \in \mathbb{N}$ tales que $b_2^2 p = a_2^2$ y $0 < b_2 < b_1 < b, 0 < a_2 < a_1 < a$, como este proceso se puede repetir infinitamente, se tiene un cadena descendiente infinita de números enteros positivos, lo cual es una contradicción. $\square$

[1] $\sqrt{p}$ es positivo, por lo que a, b también lo son

2) Dado $(a, b) = 1$ y $(a, c) = 1$, demuestre que $(a, bc) = 1$.

Demostración. Sea $(a, bc) = k$, si $k > 1$, existe p primo tal que $p \mid k$[2], luego se tiene que $p \mid a$ y $p \mid bc$, ya que $k \mid a$ y $k \mid bc$. Con esto se tiene que sea uno de los siguientes:

$$(p \mid a \wedge p \mid b) \qquad\qquad (p \mid a \wedge p \mid c)$$

Con el primero se tiene que $p \mid (a, b)$, por lo que $(a, b) > 1$, lo que es una contradicción, análogamente con el segundo. $\square$

3) Demuestre que $a^p + b^p$ es divisible por p ssi $(a + b)^p$ es divisible por p.

Demostración. Se comienza viendo que $p \mid \binom{p}{k}$ para $0 < k < p$, se recuerda la definición de primo[3] y se escribe lo siguiente

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} = p\frac{(p-1)!}{(p-k)!k!}$$

Como p es primo, y $k, p-k$ son menores a p se tiene que son coprimos, por lo que $\frac{(p-1)!}{(p-k)!k!}$ es un entero, y entonces $\binom{p}{k}$ es divisible por p. Usando propiedades de divisibilidad[4], se tiene que

$$p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

Para $a, b \in \mathbb{N}$. Con esto, se ve que $(a + b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$, con lo que si $p \mid a^p + b^p$ se tiene que $p \mid (a + b)^p$ y vice-versa. $\square$

4) Demuestre que dado p primo, $p \mid b^2$ ssi $p^2 \mid b^2$. (*Demuéstrelo sin el teorema fundamental de la aritmética*)(Generalice a $p \mid b^n$ ssi $p^n \mid b^n$)

Demostración. $\underline{\implies}$: Si $p \mid b^2$, por una propiedad usada anteriormente se tiene que $p \mid b$, con lo que $p^2 \mid b^2$[5].
$\underline{\impliedby}$: Si $p^2 \mid b^2$, entonces $p \mid p^2$ y por transitividad $p \mid b^2$[6]. Con lo que se tiene lo pedido. $\square$

---

[2]Se puede demostrar sin usar el Teorema Fundamental de la Aritmética, o usandolo directamente.
[3]i.e. es un número natural mayor a 1 que no es la multiplicación de dos números naturales menores a este.
[4]i.e. $a \mid b, a \mid c \implies a \mid b + c$
[5]Equivalentemente $p^n \mid b^n$
[6]Equivalentemente $p \mid b^n$