Definibilidad de $\mathbb{N}$ en $(\mathbb{Q}, +, *, 0, 1)$

Enrique Acosta Jaramillo

Mayo 2006

1. Introducción

Teorema. $\mathbb{N}$ es definible en $\mathcal{Q} = (\mathbb{Q}, +, *, 0, 1)$, es decir:

existe una fórmula $\phi(x)$ de primer orden con una variable libre sobre el lenguaje $L = \{+, ., 0, 1\}$ tal que

$$\mathcal{Q} \models \phi[r] \Leftrightarrow r \in \mathbb{N}$$

1.1. Segundo Orden

En segundo orden la fórmula es simple, simplemente tome

$$\phi(x) : \forall A \subseteq \mathbb{Q}\Big\{ \Big[0 \in A \wedge \forall r(r \in A \rightarrow r + 1 \in A)\Big] \rightarrow x \in A\Big\}$$

2. Consecuencias

2.1. Decidibilidad

Definición. Una teoría T de primer orden se dice

$\diamond$ *Completa* si para toda sentencia ϕ se tiene

$$T \vdash \phi \quad o \quad T \vdash \neg\phi.$$

$\diamond$ *Decidible* si existe un algoritmo que decide para toda sentencia ϕ en un número finito de pasos si

$$T \vdash \phi \quad o \quad T \nvdash \phi.$$

$\diamond$ *Recursivamente Axiomatizable* si T eq T' con T' recursiva.

Ejemplos

1. Son decidibles

   $\diamond$ $Th(\mathbb{C}, +, *, 0, 1)$
   $\diamond$ $Th(\mathbb{R}, +, *, 0, 1)$
   $\diamond$ La teoría de campos algebraicamente cerrados de característica de una característica fija.

2. Son indecidibles
   - $\diamond$ $Th(\mathbb{C}, +, *, 0, 1, exp)$
   - $\diamond$ AP^1 (Axiomática de Peano de primer orden)
   - $\diamond$ Cualquier teoría que extienda a AP^1
   - $\diamond$ $Th(\mathcal{N})$
   - $\diamond$ Teoría de Grupos
   - $\diamond$ La teoría vacía (el cálculo de predicados) sobre el lenguaje de la aritmética.

3. Se desconoce la decidibilidad de
   - $\diamond$ $Th(\mathbb{R}, +, *, 0, 1, exp)$ (Propuesto por Tarski 19..)

Teorema 1. Si T es completa y recursivamente axiomatizable entonces T es decidible.

Demostración. Corra en paralelo el algotimo para ϕ y $\neg\phi$. □

Corolario 1.1. $TCAC_0$ es decidible pues es completa.

Corolario 1.2. $Th(\mathbb{C}, +, *, 0, 1)$es decidible.

Demostración. $Th(\mathbb{C}, +, *, 0, 1) = TCAC_0$ porque $TCAC_0$ es completa y $(\mathbb{C}, +, *, 0, 1) \models TCAC_0$. Como $TCAC_0$ es recursivamente axiomatizable, $Th(\mathbb{C}, +, *, 0, 1)$ es decidible. □

Así, todo lo que se pueda decir en primer orden sobre estas estructuras un computador puede revisar si es verdad o no.

2.2. Indecidibilidad de $Th(\mathcal{N})$

ESCRIBIR LA AXIOMATICA DE AP

Teorema 2. Toda extension consistente de AP^1 es indecidible.

Corolario 2.1. AP^1 es indecidible.

Corolario 2.2. $Th(\mathcal{N})$ es indecidible.

Corolario 2.3 (Incompletitud de Gödel)**.** Si $T \supseteq AP^1$ y T es recursivamente axiomatizable entonces T es incompleta.

Corolario 2.4. AP^1 es incompleta.

Corolario 2.5. $Th(\mathcal{N})$ no es recursivamente axiomatizable.

2.3. Aplicaciones de la indecidibilidad de $Th(\mathcal{N})$ y su relación con $\mathcal{Q}$

Teorema 3. Sea $\mathcal{M}$ una estructura en el lenguaje de la aritmética con $\mathcal{N} \leq \mathcal{M}$. Si $\mathbb{N}$ es definible en $\mathcal{M}$ entonces $Th(\mathcal{M})$ es indecidible.

Demostración. Sea $\phi(x)$ la fórmula que define $\mathbb{N}$ en $\mathcal{M}$. Para cada sentencia θ sobre L sea $\theta^{\phi(x)}$ su relativización. Entonces,

$$\mathcal{N} \models \theta \Leftrightarrow \mathcal{M} \models \theta^{\phi(x)}$$

luego si $Th(\mathcal{M})$ fuera decidible, $Th(\mathcal{N})$ seria decidible que es una contradicción. □

Corolario 3.1. Si $\mathbb{N}$ es definible en $\mathcal{Q} = (\mathbb{Q}, +, *, 0, 1)$ entonces $Th(\mathcal{Q})$ es indecidible y no es recursivamente axiomatizable.

Corolario 3.2. $Th(\mathbb{Z}, +, *, 0, 1)$ es indecidible.

Demostración. Por el teorema de suma de cuatro cuadrados de Lagrange, todo número natural se puede escribir como suma de cuatro cuadrados. Así,

$$\phi(x) : \exists x_1 \exists x_2 \exists x_3 \exists x_4 (x = x_1^2 + x_2^2 + x_3^2 + x_4^2)$$

define a $\mathbb{N}$ en $(\mathbb{Z}, +, *, 0, 1)$, es decir,

$$(\mathbb{Z}, +, *, 0, 1) \models \phi[n] \Leftrightarrow n \in \mathbb{N}.$$

□

Corolario 3.3. $\mathbb{N}$ y $\mathbb{Z}$ no son definibles en $(\mathbb{C}, +, *, 0, 1)$ ni en $(\mathbb{R}, +, ., 0, 1)$.

Corolario 3.4. $Th(\mathbb{C}, +, *, 0, 1, exp)$ es indecidible.

3. Definibilidad de $\mathbb{N}$ en $(\mathbb{Q}, +, *, 0, 1)$

Es suficiente demostrar que $\mathbb{Z}$ es definible en $(\mathbb{Q}, +, *, 0, 1)$.

3.1. Motivación

$\diamond$ El problema: En no hay forma aparente de extraer el nominador y denominador de un racional en primer orden. Inclusive si esto se puede hacer, no hay forma de hablar de primos si uno ni siquiera tiene a los naturales (eso es lo que está tratando de hacer!).

Teorema 4 (Gauss-Legendre)**.** $n \in \mathbb{N}$ es suma de tres cuadrados racionales si y solo si n NO es de la forma $4^m(8k + 7)$ $m, k \in \mathbb{N}$.

Teorema 5 (Julia Robinson)**.** La fórmula

$$\phi(x) : \exists x_1 \exists x_2 \exists x_3 (7x^2 + 2 = x_1^2 + x_2^2 + x_3^2)$$

define a los racionales cuyo denominador exacto no es divisible por 2, es decir, para $r \in \mathbb{Q}$, $r = n/d$ con $mcd(n, d) = 1$

$$\mathcal{Q} \models \phi[r] \Leftrightarrow 2 \not| \, d.$$

Demostración. Existen $x_1, x_2, x_3 \in \mathbb{Q}$ tales que

$$7(n/d)^2 + 2 = x_1^2 + x_2^2 + x_3^2$$

si y solo si existen $x_1, x_2, x_3 \in \mathbb{Q}$ tales que

$$7n^2 + 2d^2 = x_1^2 + x_2^2 + x_3^2,$$

luego es suficiente ver que $7n^2 + 2d^2$ es suma de cuarto cuadrados racionales si y solo si d es impar.

$\diamond$ Si d es impar,

$$7n^2 + 2d^2 \equiv (\text{mod } 8) \begin{cases} 1 & n \text{ impar} \\ 2, 6 & n \text{ par} \end{cases}$$

en ambos casos n no es de la forma $4^m(8k + 7)$ $m, k \in \mathbb{N}$ pues todo entero de la forma $4^m(8k + 7) \equiv 7, 0, 4(\text{mod } 8)$ luego es suma de tres cuadrados racionales.

$\diamond$ Si d es par,

$7n^2 + 2d^2 \equiv 7(\text{mod } 8)$ luego no es suma de cuatro cuadrados racionales. $\square$

3.2. Los lemmas de Julia Robinson

$\diamond$ Los lemas fuertes enunciado.

Lema 6 (Julia Robinson)**.** Sean $r \in \mathbb{Q}$ y p primo $p \equiv 3(\text{mod } 4)$. Existen $x, y, z \in \mathbb{Q}$ tales que

$$x^2 + y^2 - pz^2 = pr^2 + 2$$

si y solo si el denominador exacto de r no es divisible por 2 ni por p.

Nota. $x^2 + y^2 - pz^2 = pr^2 + 2$ tiene solución en $\mathbb{Q}^3$ si y solo si $x^2 + y^2 - pz^2 = pn^2 + 2d^2$ tiene solución donde $r = n/d$. La demostración es similar a la del teorema 5, sin embargo, es necesario conocer que forma tienen los números representables en la forma $x^2 + y^2 - pz^2$.

Lema 7 (Julia Robinson)**.** Sean $r \in \mathbb{Q}$ y p, q primos impares con $p \equiv 1(\text{mod } 4)$ y $(q/p) = -1$. Existen $x, y, z \in \mathbb{Q}$ tales que

$$x^2 + qy^2 - pz^2 = qpr^2 + 2$$

si y solo si el denominador exacto de r no es divisible por p ni por q.

Nota. Al igual que en el lema 6, es necesario conocer que forma tienen los números representables en la forma $x^2 + qy^2 - pz^2$.

3.3. La fórmula $\phi(x)$

Definiendo

$$\sigma(q,p,x) : \exists y \exists z \exists w (y^2 + qz^2 = qpx^2 + pw^2 + 2)$$

las hipótesis de existencia de los lemas 6 y 7 se pueden reescribir como

$$\mathbb{Q} \models \sigma[1,p,r] \quad y \quad \mathbb{Q} \models \sigma[q,p,r].$$

Note además que si

$$\mathbb{Q} \models \sigma[q,p,r], \sigma[1,p,r]$$

para todos los primos p, q entonces $r \in \mathbb{Z}$. Esto se deduce de los lemas y el hecho que para todo primo impar $p \equiv 1 (\text{mod } 4)$ existe q primo impar tal que $(q/p) = -1$.

Uno esta tentado a pensar que la $\phi(x)$ buscada es precisamente

$$\phi(x) : \forall p \forall q \, \sigma(q,p,x)$$

pero p, q pueden tomar cualquier valor racional y deben existir un $n \in \mathbb{N}$ $p, q \in \mathbb{Q}$ tales que

$$\mathcal{Q} \not\models \sigma[q,p,n].$$

Sin embargo, definiendo

$$\phi(x) : \forall p \forall q \Big\{ \Big[\sigma(q,p,0) \wedge \forall r \Big(\sigma(q,p,r) \rightarrow \sigma(q,p,r+1) \Big) \Big] \rightarrow \sigma(q,p,x) \Big\}$$

se obtiene la definición buscada.

Teorema 8. $\phi(x)$ define a $\mathbb{Z}$ en $\mathcal{Q} = (\mathbb{Q}, +, *, 0, 1)$, es decir,

$$\mathcal{Q} \models \phi[r] \Leftrightarrow r \in \mathbb{Z}.$$

Demostración. dem. □

3.4. Formas cuadráticas sobre $\mathbb{Q}$

Al igual que con el teorema que define a los racionales cuyo denominador exacto no es divisible por 2, la demostración de los lemas 6 y 7 está estrechamente ligada con los números representables en $\mathbb{Q}$ por formas cuadráticas racionales diagonales.

Definición. Sea D un anillo, una *forma cuadrática diagonal sobre* D es una función de la forma

$$f(x_1, \ldots, x_n) = a_1 x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2.$$

con $a_1, a_2, \ldots, a_n \in D$.

Teorema 9. Dada una forma cuadrática $f(x_1, \ldots, x_n)$ sobre un campo F de característica distinta de 2 y $a \in F$, la ecuación

$$f(x_1, \ldots, x_n) = a$$

tiene solución en F^n si y solo si $f - ax_{n+1}^2$ tiene solución no trivial en F^{n+1}.

Demostración. Si $f(x_1, \ldots, x_n) = a$ tiene solución entonces $f - ax_{n+1}^2 = 0$ tiene solución no trivial tomando $x_{n+1} = 1$. Si $f - ax_{n+1}^2 = 0$ tiene una solución no trivial $(r_1, \ldots, r_n, r_{n+1})$ con $r_{n+1} \neq 0$ entonces $f(r_1/r_{n+1}, \ldots, r_n/r_{n+1}) = a$ es una solución no trivial. Si en la solución no trivial $(r_1, \ldots, r_n, r_{n+1})$ se tiene $r_{n+1} = 0$ entonces $f(r_1, \ldots, r_n) = 0$ donde se puede suponer $r_1 \neq 0$. Tomando $\tau = a(4f(1, 0, \ldots, 0)r_1^2)^{-1}$ se tiene que $x_1 = (1 + \tau)r_1$, $x_k = (1 - \tau)r_k$, $k = 2, 3, \ldots, n$ es una solución de $f = a$. □

Así, el teorema de suma de tres cuadrados de Gauss se puede reescribir como

Teorema 10. Dado $n \in \mathbb{N}$,

$$x^2 + y^2 + z^2 - nw^2 = 0$$

tiene solución no trivial en $\mathbb{Q}$ si y solo si n no es de la forma $4^m(8k + 7)$ con $m, k \in \mathbb{N}$.

Este resultado, al igual que los que caracterizarán los números representables por las formas cuadráticas a las que se hace referencia en los lemas 6 y 7 son consecuencias del siguiente teorema.

Teorema 11 (Hasse-Minkowski)**.** La ecuación

$$a_1x_1^2 + \ldots + a_nx_n^2 = 0$$

con $a_1, \ldots, a_n \in \mathbb{Z}$ tiene solución no trivial en $\mathbb{Q}^n$ si y solo si tiene solución no trivial ni divisible por p en $\mathbb{Z}$ módulo p^n para todo primo p y todo $n \geq 1$.

Que en realidad fue enunciado y demostrado por Hasse en la siguiente forma un poco más general.

Teorema 12 (Hasse-Minkowski, enunciado de Hasse)**.** Sea $f(x_1, \ldots, x_n)$ una forma cuadratica sobre $\mathbb{Q}$. Entonces

$$f(x_1, \ldots, x_n) = 0$$

tiene solución no trivial en $\mathbb{Q}$ si y solo si tiene solución no trivial en $\mathbb{R}$ y en $\mathbb{Q}_p$ (el campo de los números p-adicos) para todo primo p.

El siguiente teorema (sin demostración ni comentarios sobre esta), caracteriza completamente estas formas en $\mathbb{Q}_p$ en función de sus coeficientes.

Teorema 13. Dada una forma cuadrática $f(x_1, \ldots, x_n)$ sobre $\mathbb{Q}_p$ con determinante $d \neq 0$, la ecuación

$$f(x_1, \ldots, x_n) = 0$$

tiene solución no trivial si y solo si

$\diamond$ $n = 2 : -d$ es un cuadrado (en $\mathbb{Q}_p$).
$\diamond$ $n = 3 : c_p(f) = 1$.
$\diamond$ $n = 4 : c_p(f) = 1$ cuando d es un cuadrado.
$\diamond$ $n \geq 5$.

Nota. .
Si $d = 0$, existe una solución no trivial.
$c_p(f)$ es una función de los coeficientes de f en $\{-1, 1\}$.

Los siguientes lemas caracterizan a los enteros representables por las formas cuadráticas que se mencionan en los lemas 6 y 7.

Lema 14. Sean $n \in \mathbb{N}$, $n \neq 0$ y p primo $p \equiv 3 (\text{mod } 4)$. Existen $x, y, z \in \mathbb{Q}$ tales que

$$x^2 + y^2 - pz^2 = n$$

si y solo si al escribir n en la forma $n = st^2$ con s "squarefree" se cumplen las dos condiciones siguientes

a. $s \not\equiv p \pmod 8$

b. si $s = pk$ entonces $(k \,|\, p) = -1$.

Lema 15. Sean $n \in \mathbb{N}$, $n \neq 0$ y p, q primos impares con $p \equiv 1 (\text{mod } 4)$ y $(q/p) = -1$. Existen $x, y, z \in \mathbb{Q}$ tales que

$$x^2 + qy^2 - pz^2 = n$$

si y solo si al escribir n en la forma $n = st^2$ con s "squarefree" se cumplen las dos condiciones siguientes

a. Si $s = pk$ entonces $(k \,|\, p) = 1$.

b. Si $s = qk$ entonces $(k \,|\, q) = 1$.

En los lemas 14 y 15 es suficiente que $x^2 + y^2 - pz^2 - nw^2 = 0$ y $x^2 + qy^2 - pz^2 - nw^2 = 0$ tienen soluciones no triviales en $\mathbb{Q}$ respectivamente.

Así, por el teorema de Hasse-Minkowski, dado que ambas formas ecuaciones tienen soluciones no triviales en $\mathbb{R}$, es suficiente ver bajo que condiciones sobre n existen soluciones no triviales (mod p^k) para todo primo p y $k \in \mathbb{N}$.

Los siguientes teoremas generales, que se demuestran con teoría elemental de números le permiten a uno demostrar los lemas 14 y 15, (no se si mencionarlos en la exposición).

Definición. Sea $f(x_1, \ldots, x_n)$ una forma cuadrática sobre $\mathbb{Z}$. Se dice que f *representa cero módulo* p^n si

$$f(x_1, \ldots, x_n) = 0$$

tiene solución no trivial ni divisible por p en $\mathbb{Z}$ módulo p^n.

Teorema 16. Si p es un primo impar y $a, b, c, d \in \mathbb{N}$ con $p \nmid abcd$ entonces

- $ax^2 + by^2 + cz^2$

representa cero módulo p^n para todo n y las siguientes representan cero módulo p^n para todo n si y solo si

- $ax^2 + by^2$: $(-ab \,|\, p) = 1$.
- $ax^2 + by^2 + pcz^2 + pdw^2$: $(-ab \,|\, p) = 1$ o $(-cd \,|\, p) = 1$.

Teorema 17. Si $a, b, c, d \in \mathbb{N}$ son impares entonces

- $ax^2 + by^2 + cz^2 + 2dw^2$

representa cero módulo 2^n para todo n y las siguientes representan cero módulo 2^n para todo n excepto cuando

- $ax^2 + by^2 + cz^2$: $a \equiv b \equiv c \,(\text{mod } 4)$.
- $ax^2 + by^2 + cz^2 + dw^2$: $a \equiv b \equiv c \equiv d (\text{mod } 4)$ y $a + b + c + d \equiv 4 (\text{mod } 8)$.