POLINOMIOS ENUMERADORES DE PRIMOS

Ana Carrasco Martín

Facultad de Matemáticas, Universidad de Sevilla

Índice de contenidos

Fórmulas que definen los primos I

$$p_n = \sum_{i=0}^{n^2} \left(1 \dot{-} \left(\left(\sum_{j=0}^{i} \operatorname{rem}((j \dot{-} 1)!^2, j) \right) \dot{-} n \right) \right).$$

Fórmulas que definen los primos II

$$f(n) = \lfloor A^{3^n} \rfloor$$

$$A \approx 1.306377883863\ldots$$

```
In [3]: thetaR= 1.30637788386308069046861449260260571291678458515671364436805375996643405376682659882150140370119739570729
```

```
In [4]: fR(n)=floor(thetaR^3^n)
```

```
In [10]: CR=[fR(n) for n in range(1,7)]
         CR
```

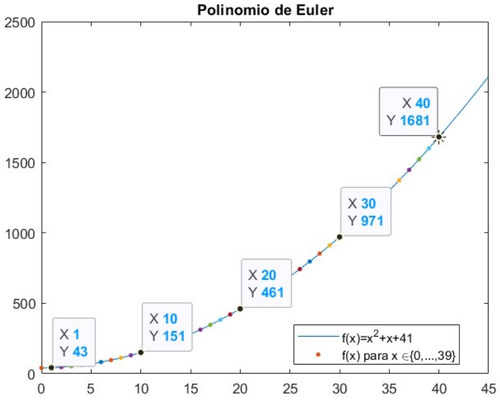
```
Out[10]: [2,
          11,
          1361,
          2521008887,
          16022236204009818131831320183,
          4113101149215104800030529537915953170486139623539759933135949994882770404074832568498]
```

```
In [11]: [is_prime(CR[i]) for i in range(0,len(CR))]
```

```
Out[11]: [True, True, True, True, True, False]
```

Fórmulas que definen los primos III

$$f(x) = x^2 + x + 41.$$



No existe un polinomio que represente únicamente primos

Teorema

Cualquier polinomio $P(x_1, \ldots, x_k)$ *con coeficientes complejos que represente únicamente valores primos al evaluarse en los enteros no negativos es constante.*

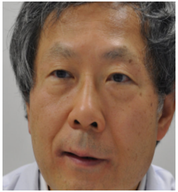
¿Existen polinomios que representen a **todos** los primos?

Polinomios enumeradores de primos

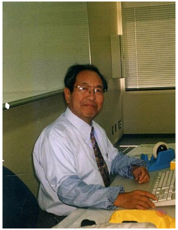
Yuri
Matijasevič

Polinomios enumeradores de primos

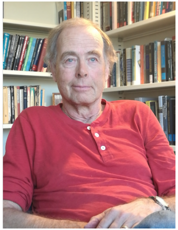
Yuri Matijasevič



Hideo Wada



Daihachiro Sato



Douglas Wiens

James P. Jones

Polinomios enumeradores de primos

Teorema

El conjunto de los números primos coincide con los valores positivos representados por el polinomio

$$
\begin{aligned}
P = {} & (k+2)\{1 - (wz+h+j-q)^2 - [(gk+2g+k+1)(h+j)+h-z]^2 - (2n+p+q+z-e)^2 \\
& - [16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 - [e^3(e+2)(a+1)^2+1-o^2]^2 - [(a^2-1)y^2+1-x^2]^2 \\
& - [16r^2y^4(a^2-1)+1-u^2]^2 - [((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 \\
& - (n+l+v-y)^2 - [(a^2-1)l^2+1-m^2]^2 - (ai+k+1-l-i)^2 - [p+l(a-n-1) \\
& + b(2an+2a-n^2-2n-2)-m]^2 - [q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
& - [z+pl(a-p)+t(2ap-p^2-1)-pm]^2\},
\end{aligned}
$$

donde las variables recorren los enteros no negativos.

Índice de contenidos

Los 23 problemas de Hilbert

Mathematische Probleme.

Vortrag, gehalten auf dem internationalen Mathematiker-Kongreß zu Paris 1900.

Von

D. Hilbert.

Wer von uns würde nicht gern den Schleier lüften, unter dem die Zukunft verborgen liegt, um einen Blick zu werfen auf die bevorstehenden Fortschritte unsrer Wissenschaft und in die Geheimnisse ihrer Entwickelung während der künftigen Jahrhunderte! Welche besonderen Ziele werden es sein, denen die führenden mathematischen Geister der kommenden Geschlechter nachstreben? welche neuen Methoden und neuen Thatsachen werden die neuen Jahrhunderte entdecken — auf dem weiten und reichen Felde mathematischen Denkens?

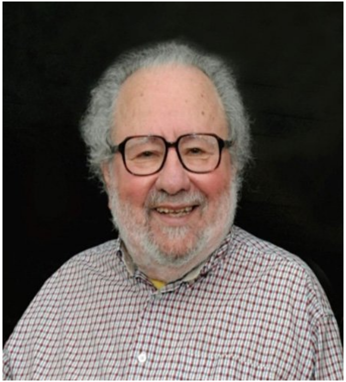
Die Geschichte lehrt die Stetigkeit der Entwickelung der Wissenschaft. Wir wissen, daß jedes Zeitalter eigene Probleme hat, die das kommende Zeitalter löst oder als unfruchtbar zur Seite schiebt und durch neue Probleme ersetzt. Wollen wir eine Vorstellung gewinnen von der muthmaßlichen Entwickelung mathematischen Wissens in der nächsten Zukunft, so müssen wir die offenen Fragen vor unserem Geiste passiren lassen und die Probleme überschauen, welche die gegenwärtige Wissenschaft stellt, und deren Lösung wir von der Zukunft erwarten. Zu einer solchen Musterung der Probleme scheint mir der heutige Tag, der an

10. DETERMINATION OF THE SOLVABILITY OF A DIOPHANTINE EQUATION.

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients:

To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

Conjetura de Davis



«Todo conjunto recursivamente enumerable es diofántico».

—**Martin Davis, 1953.**

El conjunto de los números primos es r.e.

"$p \in \mathbb{N}$ es primo si $p > 1$ y sus únicos divisores naturales son 1 y p"

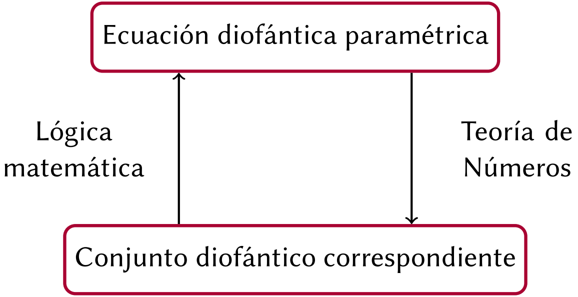
El conjunto de los números primos es r.e.

"$p \in \mathbb{N}$ es primo si $p > 1$ y sus únicos divisores naturales son 1 y p"

$$\text{Prime}(x) \iff x > 1 \ \& \ (\forall t)_{\leq x}\{t = 1 \lor t = x \lor \sim (t \mid x)\}$$

El conjunto de los números primos es diofántico

El conjunto de los primos es r.e. $\overset{\text{Davis}}{\Longrightarrow}$ es diofántico $\Longrightarrow \exists\ P(p, z_1, \dots z_n) = 0$ que tiene solución si y solo si p es primo



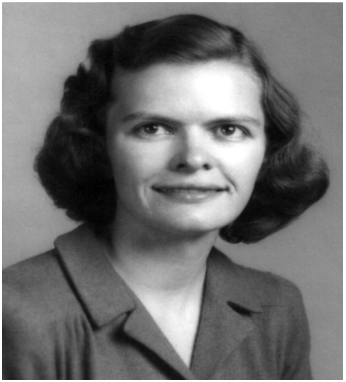
Método de Putnam

Teorema (Putnam, 1960)

Todo conjunto diofántico de enteros positivos coincide con el conjunto de enteros positivos representados por un polinomio.

$$P(p, z_1, \dots, z_n) = 0 \iff p = z_0(1 - P'^2(z_0, \dots z_n))$$

Observación de Julia Robinson



«El caso particular de la conjetura de Davis para los números primos implica la veracidad de la conjetura en su totalidad».

—Julia Robinson, 1960.

Teorema DPRM. Indecibilidad del décimo problema de Hilbert.

Teorema (DPRM)

Todo conjunto recursivamente enumerable es diofántico.

—Yuri Matijasevič, 1970.

Índice de contenidos

Polinomio enumerador de primos de grado 25 en 26 variables

Teorema

El conjunto de los números primos coincide con los valores positivos representados por el polinomio

$$\begin{aligned}
P = {} & (k+2)\{1-(wz+h+j-q)^2-[(gk+2g+k+1)(h+j)+h-z]^2-(2n+p+q+z-e)^2 \\
& -[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2 \\
& -[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 \\
& -(n+l+v-y)^2-[(a^2-1)l^2+1-m^2]^2-(ai+k+1-l-i)^2-[p+l(a-n-1) \\
& +b(2an+2a-n^2-2n-2)-m]^2-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
& -[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\},
\end{aligned}$$

donde las variables recorren los enteros no negativos.

Claves en la construcción de M I

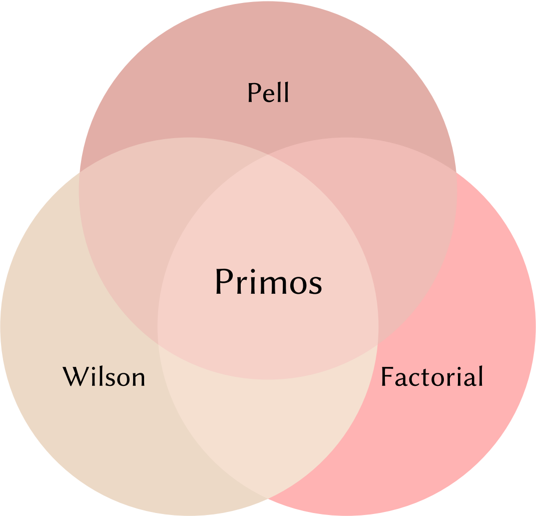
Proposición

Para cada entero no negativo k, se tiene que

$$k + 2 \text{ es primo si y solo si } M = 0 \text{ tiene solución en los enteros no negativos.}$$

+ MÉTODO DE PUTNAM: $P = (k+2)(1-M)$

Claves en la construcción de M II



Ecuación de Pell I

Definición (Ecuación de Pell)

Una ecuación de Pell es una ecuación diofántica de la forma

$$x^2 - dy^2 = 1,$$

donde $d \in \mathbb{Z}$ es un parámetro previamente determinado y x e y son variables enteras.

Ecuación de Pell I

Definición (Ecuación de Pell)

Una ecuación de Pell es una ecuación diofántica de la forma

$$x^2 - dy^2 = 1,$$

donde $d \in \mathbb{Z}$ es un parámetro previamente determinado y x e y son variables enteras.

Consideramos $x, y, d \in \mathbb{N}$. ¿Soluciones?

Ecuación de Pell I

Definición (Ecuación de Pell)

Una ecuación de Pell es una ecuación diofántica de la forma

$$x^2 - dy^2 = 1,$$

donde $d \in \mathbb{Z}$ es un parámetro previamente determinado y x e y son variables enteras.

Consideramos $x, y, d \in \mathbb{N}$. ¿Soluciones?

- Si $d = 0 \Rightarrow (x, y) = (1, y),\ \ y \in \mathbb{N}$.
- Si $d > 0$ y $d = \square \Rightarrow (x, y) = (1, 0)$.
- Si $d > 0$ y $d \neq \square \Rightarrow \exists\ \infty$ sols. no triviales.

Ecuación de Pell II

Caso de interés:

$$\begin{cases} x^2 - dy^2 = 1, & x, y \geq 0. \\ d = a^2 - 1, & a > 1. \end{cases}$$

Ecuación de Pell II

Caso de interés:

$$\begin{cases} x^2 - dy^2 = 1, & x, y \geq 0. \\ d = a^2 - 1, & a > 1. \end{cases}$$

¿Soluciones? $\exists\ \infty$ soluciones, que denotaremos $(\chi_a(n), \psi_a(n)),\ n \geq 0$.

Ecuación de Pell II

Caso de interés:

$$\begin{cases} x^2 - dy^2 = 1, & x, y \geq 0. \\ d = a^2 - 1, & a > 1. \end{cases}$$

¿Soluciones? $\exists\ \infty$ soluciones, que denotaremos $(\chi_a(n), \psi_a(n))$, $n \geq 0$.

- Expresadas como sucesiones de Lucas:

$$\begin{aligned} &\chi_a(0) = 1, \quad &&\chi_a(1) = a, \quad &&\chi_a(n+2) = 2a\chi_a(n+1) - \chi_a(n), \\ &\psi_a(0) = 0, \quad &&\psi_a(1) = 1, \quad &&\psi_a(n+2) = 2a\psi_a(n+1) - \psi_a(n). \end{aligned}$$

Ecuación de Pell II

Caso de interés:

$$\begin{cases} x^2 - dy^2 = 1, & x, y \geq 0. \\ d = a^2 - 1, & a > 1. \end{cases}$$

¿Soluciones? $\exists\ \infty$ soluciones, que denotaremos $(\chi_a(n), \psi_a(n)),\ n \geq 0$.

- Expresadas como sucesiones de Lucas:

$$\begin{aligned} &\chi_a(0) = 1, \quad &&\chi_a(1) = a, \quad &&\chi_a(n+2) = 2a\chi_a(n+1) - \chi_a(n), \\ &\psi_a(0) = 0, \quad &&\psi_a(1) = 1, \quad &&\psi_a(n+2) = 2a\psi_a(n+1) - \psi_a(n). \end{aligned}$$

- Obtenidas a partir de la primera solución no trivial:

$$\chi_a(n) + \psi_a(n)\sqrt{d} = (\chi_a(1) + \psi_a(1)\sqrt{d})^n = (a + \sqrt{d})^n.$$

1. *(Congruence rule)* Sea $a \equiv b \mod c$. Para todo $n \geq 0$, se tiene que

$$\chi_a(n) \equiv \chi_b(n) \mod c, \text{ y}$$
$$\psi_a(n) \equiv \psi_b(n) \mod c.$$

Propiedades de las soluciones de la ecuación de Pell

1. *(Congruence rule)* Sea $a \equiv b \mod c$. Para todo $n \geq 0$, se tiene que

$$\chi_a(n) \equiv \chi_b(n) \mod c, \text{ y}$$
$$\psi_a(n) \equiv \psi_b(n) \mod c.$$

2. $\gcd(x_n, y_n) = 1$.

Propiedades de las soluciones de la ecuación de Pell

1. *(Congruence rule)* Sea $a \equiv b \mod c$. Para todo $n \geq 0$, se tiene que

$$\chi_a(n) \equiv \chi_b(n) \mod c, \text{ y}$$
$$\psi_a(n) \equiv \psi_b(n) \mod c.$$

2. $\gcd(x_n, y_n) = 1$.
3. $\psi_a(n+1) > \psi_a(n) \geq n$ y $\chi_a(n+1) > \chi_a(n) \geq a^n$.

Propiedades de las soluciones de la ecuación de Pell

1. *(Congruence rule)* Sea $a \equiv b \mod c$. Para todo $n \geq 0$, se tiene que

$$\begin{aligned} \chi_a(n) &\equiv \chi_b(n) \mod c, \text{ y} \\ \psi_a(n) &\equiv \psi_b(n) \mod c. \end{aligned}$$

2. $\gcd(x_n, y_n) = 1$.
3. $\psi_a(n+1) > \psi_a(n) \geq n$ y $\chi_a(n+1) > \chi_a(n) \geq a^n$.
4. *(First step down lemma)* Si $y_n^2 \mid y_t \implies y_n \mid t$.

Representación diofántica de las soluciones de la ecuación de Pell

Proposición

Sean $a \geq 2$, $n \geq 1$ e $y \in \mathbb{N}$. Se tiene que $y = \psi_a(n)$ si y solo si existen enteros no negativos $b, c, d, r, s, t, u, v, x$ tales que:

(1) $x^2 = (a^2 - 1)y^2 + 1$,
(2) $u^2 = (a^2 - 1)v^2 + 1$,
(3) $s^2 = (b^2 - 1)t^2 + 1$,
(4) $v = 4ry^2$,
(5) $b = a + u^2(u^2 - a)$,
(6) $s = x + cu$,
(7) $t = n + 4dy$,
(8) $n \leq y$.

Representación diofántica de las soluciones de la ecuación de Pell

Proposición

Sean $a \geq 2$, $n \geq 1$ e $y \in \mathbb{N}$. Se tiene que $y = \psi_a(n)$ si y solo si existen enteros no negativos $b, c, d, r, s, t, u, v, x$ tales que:

(1) $x^2 = (a^2 - 1)y^2 + 1$,
(2) $u^2 = (a^2 - 1)v^2 + 1$,
(3) $s^2 = (b^2 - 1)t^2 + 1$,
(4) $v = 4ry^2$,
(5) $b = a + u^2(u^2 - a)$,
(6) $s = x + cu$,
(7) $t = n + 4dy$,
(8) $n \leq y$.

Corolario

Sean $a \geq 2$, $n \geq 1$ e $y \in \mathbb{N}$. Se tiene que $y = \psi_a(n)$ si y solo si existen c, d, r, u, x enteros no negativos tales que:

(1) $x^2 = (a^2 - 1)y^2 + 1$,
(2) $u^2 = 16(a^2 - 1)r^2y^4 + 1$,
(3) $(x+cu)^2 = ((a+u^2(u^2-a))^2-1)(n+4dy)^2+1$,
(4) $n \leq y$.

Teorema de Wilson

Teorema (Teorema de Wilson)

Para $k \geq 1$*, se tiene que* $k+1$ *es primo si y solo si* $k+1 \mid k!+1$.

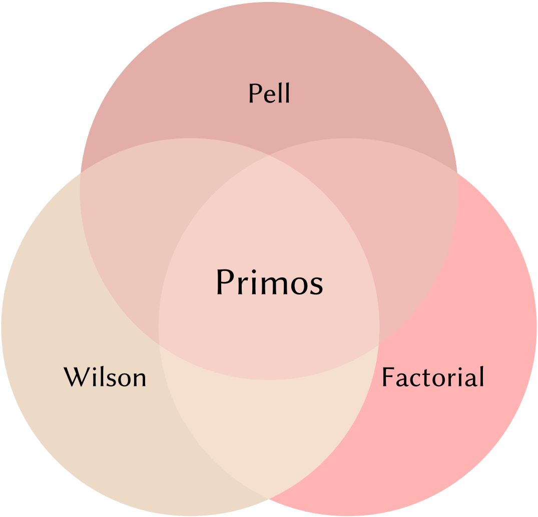
Representación diofántica del factorial

Proposición

Sean $k, f \in \mathbb{Z}_+$. Se tiene que $f = k!$ si y solo si existen enteros no negativos j, h, n, p, q, w, z tales que:

(1) $q = wz + h + j$,
(2) $z = f(h + j) + h$,
(3) $(2k)^3(2k + 2)(n + 1)^2 + 1 = \square$,
(4) $p = (n + 1)^k$,
(5) $q = (p + 1)^n$,
(6) $z = p^{k+1}$.

Representación diofántica del conjunto de los números primos I



Representación diofántica del conjunto de los números primos II

Teorema

Para cualquier $k \geq 1$, se tiene que $k+1$ es primo si y solo si existen $a, b, c, d, e, f, g, h, i, j, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z$ tales que

(1) $q = wz + h + j$,

(2) $z = (gk + g + k)(h + j) + h$,

(3) $(2k)^3(2k+2)(n+1)^2 + 1 = f^2$,

(4) $e = p + q + z + 2n$,

(5) $e^3(e+2)(a+1)^2 + 1 = o^2$,

(6) $x^2 = (a^2-1)y^2 + 1$,

(7) $u^2 = 16(a^2-1)r^2y^4 + 1$,

(8) $(x+cu)^2 = ((a+u^2(u^2-a))^2-1)(n+4dy)^2+1$,

(9) $m^2 = (a^2-1)l^2 + 1$,

(10) $l = k + i(a-1)$,

(11) $n + l + v = y$,

(12) $m = p + l(a-n-1) + b(2a(n+1)-(n+1)^2-1)$,

(13) $x = q + y(a-p-1) + s(2a(p+1)-(p+1)^2-1)$,

(14) $pm = z + pl(a-p) + t(2ap - p^2 - 1)$.

Polinomio enumerador de primos de grado 25 en 26 variables

Teorema

El conjunto de los números primos coincide con los valores positivos representados por el polinomio

$$
\begin{aligned}
P = {} & (k+2)\{1-(wz+h+j-q)^2-[(gk+2g+k+1)(h+j)+h-z]^2-(2n+p+q+z-e)^2 \\
& -[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2 \\
& -[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 \\
& -(n+l+v-y)^2-[(a^2-1)l^2+1-m^2]^2-(ai+k+1-l-i)^2-[p+l(a-n-1) \\
& +b(2an+2a-n^2-2n-2)-m]^2-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
& -[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\},
\end{aligned}
$$

donde las variables recorren los enteros no negativos.

Índice de contenidos

Pruebas aleatorias

In [2]:
```
R.<a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z> = PolynomialRing(ZZ,26)
R
```

Out[2]:
```
Multivariate Polynomial Ring in a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z over I
nteger Ring
```

In [3]:
```
pol=(k+2)*(1-(w*z+h+j-q)^2
            -((g*k+2*g+k+1)*(h+j)+h-z)^2
            -(2*n+p+q+z-e)^2
            -(16*(k + 1)^3*(k +2)*(n + 1)^2+1-f^2)^2
            -(e^3*(e +2)*(a + 1)^2+1-o^2)^2
            -((a^2-1)*y^2+1-x^2)^2
            -(16*r^2*y^4*(a^2-1)+1-u^2)^2
            -(((a+u^2*(u^2- a))^2- 1)*(n+4*d*y)^2+1-(x+c*u)^2)^2
            -(n+l+v-y)^2
            -((a^2-1)*l^2+1-m^2)^2
            -(a*i+k+1-l-i)^2
            -(p+l*(a-n-1)+b*(2*a*n+2*a-n^2-2*n-2)-m)^2
            -(q+y*(a-p-1)+s*(2*a*p+2*a-p^2-2*p-2)-x)^2
            -(z+p*l*(a-p)+t*(2*a*p-p^2-1)-p*m)^2)
```

In [4]:
```
C=IntegerListsLex(7901690358098896161685556879749949186326380713409290912,length=26)
R=[C[n] for n in range(10)]
```

In [5]:
```
[pol(tuple(_)) for _ in R]
```

Out[5]:
```
[-2188,
 -499493684122184494867821824799660909453992170501477618897798092816282618948213265245351649657823653672069026988,
 -2188,
 -2188,
 -70170170759424175205627967216283637926401875893197212105278552996129549922940624961348863883450284302794180484626
401429349275564635147760951551692714039765508424081653506526688578530293553670230098668080272700938883610766,
 -2058,
 -2188,
 -2198,
 -124873421030546123716955456199915227363498042625369404756056284636466239383795543830337709159761436271654422028,
 -2192]
```

Teorema

Para cualquier $k \geq 1$, se tiene que $k+1$ es primo si y solo si existen $a, b, c, d, e, f, g, h, i, j, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z$ tales que

(1) $q = wz + h + j$,
(2) $z = (gk + g + k)(h + j) + h$,
(3) $(2k)^3(2k + 2)(n + 1)^2 + 1 = f^2$,
(4) $e = p + q + z + 2n$,
(5) $e^3(e + 2)(a + 1)^2 + 1 = o^2$,
(6) $x^2 = (a^2 - 1)y^2 + 1$,
(7) $u^2 = 16(a^2 - 1)r^2y^4 + 1$,
(8) $(x+cu)^2 = ((a+u^2(u^2-a))^2-1)(n+4dy)^2+1$,
(9) $m^2 = (a^2 - 1)l^2 + 1$,
(10) $l = k + i(a - 1)$,
(11) $n + l + v = y$,
(12) $m = p+l(a-n-1)+b(2a(n+1)-(n+1)^2-1)$,
(13) $x = q+y(a-p-1)+s(2a(p+1)-(p+1)^2-1)$,
(14) $pm = z + pl(a - p) + t(2ap - p^2 - 1)$.

Solución fundamental de la ecuación de Pell

1. ¿Cuál es la solución fundamental de $x^2 - 3y^2 = 1$?

Solución fundamental de la ecuación de Pell

1. ¿Cuál es la solución fundamental de $x^2 - 3y^2 = 1$?
   - Si $x = 1 \implies y = 0$ (solución trivial)

Solución fundamental de la ecuación de Pell

1. ¿Cuál es la solución fundamental de $x^2 - 3y^2 = 1$?
   - Si $x = 1 \implies y = 0$ (solución trivial)
   - Si $x = 2 \implies y = 1$ ✓

Solución fundamental de la ecuación de Pell

1. ¿Cuál es la solución fundamental de $x^2 - 3y^2 = 1$?
   - Si $x = 1 \implies y = 0$ (solución trivial)
   - Si $x = 2 \implies y = 1$ ✓
2. ¿Cuál es la solución fundamental de $x^2 - 32^3(32+2)y^2 = 1$?

Solución fundamental de la ecuación de Pell

1. ¿Cuál es la solución fundamental de $x^2 - 3y^2 = 1$?
   - Si $x = 1 \implies y = 0$ (solución trivial)
   - Si $x = 2 \implies y = 1$ ✓
2. ¿Cuál es la solución fundamental de $x^2 - 32^3(32+2)y^2 = 1$? **X**

Fracción continua simple

$$\langle a_0, a_1, a_2, \dots \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

Convergentes de una fracción continua

Definición (Convergentes de una fracción continua)

Sea $\langle a_0, a_1, \dots \rangle$ *una fracción continua simple. Para cada* $n \geq 0$*, denotemos* r_n *al resultado de truncar por* a_n *la fracción continua, esto es,* $r_n := \langle a_0, a_1, \dots, a_n \rangle$*. Diremos que* r_n *es el* $n-$*ésimo convergente de la fracción continua.*

Convergentes de una fracción continua

Definición (Convergentes de una fracción continua)

Sea $\langle a_0, a_1, \dots \rangle$ una fracción continua simple. Para cada $n \geq 0$, denotemos r_n al resultado de truncar por a_n la fracción continua, esto es, $r_n := \langle a_0, a_1, \dots, a_n \rangle$. Diremos que r_n es el $n-$ésimo convergente de la fracción continua.

$$
\begin{aligned}
&h_{-2} = 0, \quad && h_{-1} = 1, \quad && h_i = a_i h_{i-1} + h_{i-2}, \quad && \text{para } i \geq 0. \\
&k_{-2} = 1, \quad && k_{-1} = 0, \quad && k_i = a_i k_{i-1} + k_{i-2}, \quad && \text{para } i \geq 0.
\end{aligned}
$$

Convergentes de una fracción continua

Definición (Convergentes de una fracción continua)

Sea $\langle a_0, a_1, \dots \rangle$ *una fracción continua simple. Para cada* $n \geq 0$*, denotemos* r_n *al resultado de truncar por* a_n *la fracción continua, esto es,* $r_n := \langle a_0, a_1, \dots, a_n \rangle$*. Diremos que* r_n *es el* $n-$*ésimo convergente de la fracción continua.*

$$h_{-2} = 0, \quad h_{-1} = 1, \quad h_i = a_i h_{i-1} + h_{i-2}, \quad \text{para } i \geq 0.$$
$$k_{-2} = 1, \quad k_{-1} = 0, \quad k_i = a_i k_{i-1} + k_{i-2}, \quad \text{para } i \geq 0.$$

Teorema

Para todo $n \geq 0$*, se tiene que* $r_n = \frac{h_n}{k_n}$.

Teorema (Lagrange, 1770)

Un número es un irracional cuadrático si y solo si la fracción continua simple que lo representa es periódica.

Teorema (Lagrange, 1770)

Un número es un irracional cuadrático si y solo si la fracción continua simple que lo representa es periódica.

$$\text{Solución de Pell} \Rightarrow \text{Convergente de } \sqrt{d}$$
$$\not\Leftarrow$$

Teorema

Sea l la longitud del período de la fracción continua de $\sqrt{d}$. La solución fundamental (x_1, y_1) de $x^2 - dy^2 = 1$ es

$$(x_1, y_1) = \begin{cases} (h_{l-1}, k_{l-1}) & \textit{si } l \textit{ es par,} \\ (h_{2l-1}, k_{2l-1}) & \textit{si } l \textit{ es impar.} \end{cases}$$

Solución fundamental de la ecuación de Pell II

```
sage: def convergent_fundamentalsol(d):

    if d.is_square()== False:

        Qd.<sqrtd>=QuadraticField(d)
        cfrac=continued_fraction(sqrtd)
        per=cfrac.period()
        lperiod=len(per)

        if mod(lperiod,2)==0:
            return cfrac.numerator(lperiod-1), cfrac.denominator(
                    lperiod-1)
        else:
            return cfrac.numerator(2*lperiod-1), cfrac.denominator(
                    2*lperiod-1)
    else:
        print("Error: d es cuadrado")
```

Evaluación del polinomio enumerador de primos

Teorema

Para cualquier $k \geq 1$, se tiene que $k+1$ es primo si y solo si existen $a, b, c, d, e, f, g, h, i, j, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z$ tales que

(1) $q = wz + h + j$,
(2) $z = (gk + g + k)(h + j) + h$,
(3) $(2k)^3(2k+2)(n+1)^2 + 1 = f^2$,
(4) $e = p + q + z + 2n$,
(5) $e^3(e+2)(a+1)^2 + 1 = o^2$,
(6) $x^2 = (a^2-1)y^2 + 1$,
(7) $u^2 = 16(a^2-1)r^2y^4 + 1$,
(8) $(x+cu)^2 = ((a+u^2(u^2-a))^2-1)(n+4dy)^2+1$,
(9) $m^2 = (a^2-1)l^2 + 1$,
(10) $l = k + i(a-1)$,
(11) $n + l + v = y$,
(12) $m = p+l(a-n-1)+b(2a(n+1)-(n+1)^2-1)$,
(13) $x = q+y(a-p-1)+s(2a(p+1)-(p+1)^2-1)$,
(14) $pm = z + pl(a-p) + t(2ap - p^2 - 1)$.

Evaluación del polinomio enumerador de primos

1. $k = 1$
2. $k! = gk + g + k \Longrightarrow g = 0$
3. (III) $(2k)^3(2k+2)(n+1)^2 + 1 = f^2 \Longrightarrow 32(n+1)^2 + 1 = f^2 \Longrightarrow (f, n) = (17, 2)$
4. Caracterización factorial

$$p = 3, \quad q = 4^2 = 16, \quad z = 3^2 = 9,$$
$$w = \frac{16-7}{9} = 1, \quad h = 9 - 7 = 2, \quad j = 7 - 2 = 5.$$

5. (IV) $e = p + q + z + 2n \Longrightarrow e = 32$
6. (V) $e^3(e+2)(a+1)^2 + 1 = o^2 \Longrightarrow$

$$o = 8340353015645794683299462704812268882126086134656108363777,$$
$$a = 790169035809889616168555687974994918632638071340929 0912.$$

Evaluación del polinomio enumerador de primos

```
In [1]: def convergent_fundamentalsol(d):

            if d.is_square()==False:

                Qd.<sqrtd>=QuadraticField(d)
                cfrac=continued_fraction(sqrtd)
                per=cfrac.period()
                lperiod=len(per)

                if mod(lperiod,2)==0:

                    return cfrac.numerator(lperiod-1), cfrac.denominator(lperiod-1)

                else:

                    return cfrac.numerator(2*lperiod-1), cfrac.denominator(2*lperiod-1)
            else:
                print("Error: d es cuadrado")

In [2]: convergent_fundamentalsol(32)

Out[2]: (17, 3)

In [3]: e=32
        rho=32^3*(e+2)

In [4]: convergent_fundamentalsol(rho)

Out[4]: (834035301564579468329946270481226888212608613465610836377 7,
         790169035809889616168555687974994918632638071340929091 3)

In [5]: a=7901690358098896161685556879749949186326380713409290912
        theta=32*a*(a^2-1)

In [*]: convergent_fundamentalsol(theta) # RIP point.
```

Índice de contenidos

Ecuaciones universales

$$x \in D \iff (\exists z_1, \ldots, z_\nu)(P(x, z_1, \ldots, z_\nu) = 0).$$

Para ciertos δ y ν, existe un polinomio U de grado δ en $z_1, \ldots, z_\nu$ tal que, para cualesquiera x y n,

$$x \in D_n \iff (\exists z_1, \ldots, z_\nu)(U(x, n, z_1, \ldots, z_\nu) = 0).$$

Son pares universales (ν, δ): $(58, 4)$, $(38, 8)$, $(19, 2668)$, $(11, 4.6 \times 10^{44})$, …

Reducción de las variables

- Resultados universales

Reducción de las variables

- Resultados universales
- Jones et. al $\longrightarrow$ Polinomio enumerador de primos en 12 variables

Reducción de las variables

- Resultados universales
- Jones et. al $\longrightarrow$ Polinomio enumerador de primos en 12 variables
- Matijasevič $\longrightarrow$ Polinomio enumerador de primos en 10 variables

Caracterización de los primos en 12 variables

Teorema

Para cualquier entero positivo k, se tiene que $k+1$ es primo si y solo si el sistema $(1)-(21)$ tiene solución en los enteros no negativos:

(1) $(2k+2)^3(2k+4)(n+1)^2+1=\square$,

(2) $(2n+2)^3(2n+4)(x+1)^2+1=\square$,

(3) $M=16nx(w+2)+1$,

(4) $A=M(x+1)$,

(5) $B=n+1$,

(6) $C=m+B$,

(7) $DFI=\square,\ F \mid H-C$,

(8) $D=(A^2-1)C^2+1$,

(9) $E=2(i+1)DC^2$,

(10) $F=(A^2-1)E^2+1$,

(11) $G=A+F(F-A)$,

(12) $H=B+2(j+1)C$,

(13) $I=(G^2-1)H^2+1$,

(14) $$\left[\frac{R}{\left(\frac{C}{KL}-(w+1)x\right)\left(1-\frac{R}{C}\right)^2 L}-(S+1)\right]^2<\frac{1}{4},$$

(15) $(M^2-1)K^2+1=\square$,

(16) $(M^2x^2-1)L^2+1=\square$,

(17) $(M^2n^2x^2-1)R^2+1=\square$,

(18) $K=n-k+1+p(M-1)$,

(19) $L=k+1+l(Mx-1)$,

(20) $R=k+1+r(Mnx-1)$,

(21) $S=(z+1)(k+1)-2$.

Reducción del grado

Teorema

Todo conjunto diofántico tiene grado menor o igual que 4.

Reducción del grado

Teorema

Todo conjunto diofántico tiene grado menor o igual que 4.

Demostración. El grado del polinomio P que define el sistema diofántico D puede ser reducido incluyendo variables adicionales z_j como sigue:

$$\begin{aligned} z_j &= x_i x_k \\ z_j &= x_k^2 \\ z_j &= y x_i \\ z_j &= y^2. \end{aligned}$$

Muchas gracias por su atención.