El lema de Hensel y sus aplicaciones

Alexey Beshenov (cadadr@gmail.com)

Universidad de El Salvador. Septiembre de 2018

1 Lema de Hensel

Sea K un cuerpo completo respecto a una norma no arquimediana $\|\cdot\|$. Denotemos por

$$\mathcal{O}_K := \{x \in K \mid \|x\| \le 1\}$$

el anillo de enteros correspondiente. Hay que tener en mente los siguientes dos ejemplos principales.

1) Sobre los números racionales $\mathbb{Q}$ consideremos la norma p-ádica

$$\left|\frac{m}{n}\right|_p := 1/p^{v_p(m)-v_p(n)}.$$

La completación de $\mathbb{Q}$ respecto a $\mathbb{Q}_p$ es el cuerpo de los números p-ádicos. El anillo $\mathbb{Z}_p := \mathcal{O}_{\mathbb{Q}_p}$ es el anillo de los enteros p-ádicos.

2) Sea k un cuerpo. Sobre el anillo de polinomios $k[X]$ definamos la valuación X-ádica mediante

$$v_X(0) := \infty, \quad v_X\left(\sum_{i\ge 0} a_i\,X^i\right) := \text{mín}\{i \mid a_i \ne 0\}, \text{ si } \sum_{i\ge 0} a_i\,X^i \ne 0$$

y la norma correspondiente sobre el cuerpo de funciones racionales $k(X)$

$$\left|\frac{f}{g}\right|_X := \rho^{v_X(f)-v_X(g)}$$

para algún parametro fijo $0 < \rho < 1$. La completación de $k(X)$ respecto a $|\cdot|_X$ es el cuerpo de las series de Laurent

$$k((X)) = \Big\{ \sum_{i\ge -n} a_i\,X^i \;\Big|\; a_i \in k,\ n = 0,1,2,3,\ldots \Big\},$$

mientras que $\mathcal{O}_{k((X))}$ es el anillo de las series formales

$$k[\![X]\!] = \Big\{ \sum_{i\ge 0} a_i\,X^i \;\Big|\; a_i \in k,\ n = 0,1,2,3,\ldots \Big\}.$$

Para cualquier cuerpo completo no arquimediano se cumple el siguiente resultado importante.

1.1. Teorema (Lema de Hensel[*]). *Sea $f(X) \in \mathcal{O}_K[X]$ un polinomio con coeficientes en $\mathcal{O}_K$. Supongamos que existe $x_0 \in \mathcal{O}_K$ tal que*

$$\|f(x_0)\| < \|f'(x_0)\|^2.$$

Entonces existe único $x \in \mathcal{O}_K$ tal que $f(x) = 0$ y $\|x - x_0\| < \|f'(x_0)\|$.

[*] Kurt Hensel (1861–1941), matemático alemán, estudiante de Kronecker y Weierstrass. Descubrió los números p-ádicos en 1897.

Antes de demostrar el lema de Hensel, necesitamos un par de sencillos lemas.

1.2. Lema. *Sea $h(X) \in \mathcal{O}_K[X]$ algún polinomio con coeficientes en $\mathcal{O}_K$. Entonces para cualesquiera $x, y \in \mathcal{O}_K$ se tiene*
$$\|h(x) - h(y)\| \le \|x - y\|.$$

Demostración. Si $h(X) = \sum_{0 \le i \le d} a_i\, X^i$ para algunos $a_i \in \mathcal{O}_K$, entonces
$$h(x) - h(y) = \sum_{0 \le i \le d} a_i\, x^i - \sum_{0 \le i \le d} a_i\, y^i = \sum_{1 \le i \le d} a_i\, (x^i - y^i) = (x - y)\, \phi(x, y),$$
donde $\phi(X, Y) \in \mathcal{O}_K[X, Y]$ es algún polinomio con coeficientes en $\mathcal{O}_K$. Luego,
$$\|h(x) - h(y)\| = \|x - y\| \cdot \|\phi(x, y)\| \le \|x - y\|,$$
ya que $\phi(x, y) \in \mathcal{O}_K$ y $\|\phi(x, y)\| \le 1$. ■

1.3. Lema. *Sea $f(X) \in \mathcal{O}_K[X]$ algún polinomio con coeficientes en $\mathcal{O}_K$. Entonces para cualesquiera $x, y \in \mathcal{O}_K$*
$$f(x + y) = f(x) + f'(x)\, y + z\, y^2$$
para algún $z \in \mathcal{O}_K$.

Demostración. Si $f(X) = \sum_{0 \le i \le d} a_i\, X^i$, entonces la fórmula del binomio nos da
$$f(X + Y) = \sum_{0 \le i \le d} a_i\, (X + Y)^i = \sum_{0 \le i \le d} a_i\, X^i + \sum_{1 \le i \le d} a_i\, i\, X^{i-1}\, Y + \sum_{1 \le i \le d} a_i\, g_i(X, Y)\, Y^2,$$
donde $g_i(X, Y) \in \mathbb{Z}[X, Y]$ son ciertos polinomios con coeficientes enteros. Notemos que $\sum_{1 \le i \le d} a_i\, i\, X^{i-1} = f'(X)$, y la identidad de arriba puede ser escrita como
$$f(X + Y) = f(X) + f'(X)\, Y + g(X, Y)\, Y^2,$$
donde $g(X, Y) := \sum_{1 \le i \le d} a_i\, g_i(X, Y) \in \mathcal{O}_K[X, Y]$ es algún polinomio con coeficientes en $\mathcal{O}_K$. ■

Demostración del lema de Hensel (el método de Newton p-ádico). Notamos primero que si $\|x - x_0\| < \|f'(x_0)\|$, entonces según 1.2 se cumple
$$\|f'(x) - f'(x_0)\| \le \|x - x_0\| < \|f'(x_0)\|,$$
así que
$$\|f'(x)\| = \|f'(x) - f'(x_0) + f'(x_0)\| = \text{máx}\{\|f'(x) - f'(x_0)\|, \|f'(x_0)\|\} = \|f'(x_0)\|.$$

Demostremos que f puede tener solo una raíz x tal que
$$\|x - x_0\| < \|f'(x_0)\|.$$
Supongamos que para algunos $x, x' \in \mathcal{O}_K$ se cumple
$$f(x) = f(x') = 0, \quad \|x - x_0\| < \|f'(x_0)\|, \quad \|x' - x_0\| < \|f'(x_0)\|.$$
Tenemos
$$\|x' - x\| = \|(x' - x_0) - (x - x_0)\| \le \text{máx}\{\|x' - x_0\|, \|x - x_0\|\} < \|f'(x_0)\|.$$
Escribamos $x' = x + y$. Según 1.3 tenemos
$$0 = f(x') = f(x + y) = f(x) + f'(x)\, (x' - x) + z\, (x' - x)^2$$

para algún $z \in O_K$. Aquí $f(x) = 0$, entonces nos queda la identidad

$$f'(x)\, y = -z\, y^2.$$

Si $y \neq 0$, tenemos

$$f'(x) = -z\, y,$$

y en particular

$$\|f'(x)\| = \|z\| \cdot \|y\| \leq \|y\| = \|x' - x\| < \|f'(x_0)\| = \|f'(x)\|,$$

que es una contradicción. Entonces, la única opción es $y = 0$ y $x = x'$.

Ahora para demostrar que la raíz x existe, consideremos la sucesión de los elementos definidos a partir de x_0 por

$$x_{n+1} := x_n - \frac{f(x_n)}{f'(x_n)}.$$

Note que es la misma fórmula que se usa en el análisis real en el método de Newton. Denotemos

$$\delta := \left\| \frac{f(x_0)}{f'(x_0)^2} \right\| = \|f(x_0)\| \cdot \|f'(x_0)\|^{-2} < 1.$$

Vamos a demostrar por inducción que los números x_n satisfacen las siguientes propiedades:

1_n) $\|x_n\| \leq 1$; es decir, $x_n \in O_K$,

2_n) $\|f'(x_n)\| = \|f'(x_0)\|$,

3_n) $\|f(x_n)\| \leq \|f'(x_0)\|^2\, \delta^{2^n}$.

Antes de verificar 1_n), 2_n), 3_n), veamos por qué nuestra sucesión $\{x_n\}$ demuestra el teorema. Notemos que las desigualdades 2_n) y 3_n) nos dan

$$\|x_{n+1} - x_n\| = \left\| \frac{f(x_n)}{f'(x_n)} \right\| = \frac{\|f(x_n)\|}{\|f'(x_0)\|} \leq \|f'(x_0)\|\, \delta^{2^n}, \tag{1.1}$$

lo que implica que $\{x_n\}$ es una sucesión de Cauchy:

$$\|x_m - x_n\| = \|(x_m - x_{m-1}) + (x_{m-1} - x_{m-2}) + \cdots + (x_{n+1} - x_n)\| \leq \max\{\|x_m - x_{m+1}\|, \ldots, \|x_{n+1} - x_n\|\},$$

y por lo tanto podemos pasar al límite

$$x := \lim_{n\to\infty} x_n.$$

Ya que $x_n \in O_K$ para todo n, se tiene $x \in O_K$. Luego,

$$\|f'(x)\| = \lim_{n\to\infty} \|f'(x_n)\| = \|f'(x_0)\|$$

gracias a 2_n) y

$$\|f(x)\| = \lim_{n\to\infty} \|f(x_n)\| \leq \lim_{n\to\infty} \|f'(x_0)\|^2\, \delta^{2^n} = 0$$

gracias a 3_n), y entonces $f(x) = 0$.

Demostremos que

$$\|x - x_0\| = \left\| \frac{f(x_0)}{f'(x_0)} \right\|.$$

Va a ser suficiente demostrar que para todo $n = 1, 2, 3, \ldots$ se cumple

$$\|x_n - x_0\| = \left\| \frac{f(x_0)}{f'(x_0)} \right\|,$$

y luego pasar al límite $n \to \infty$. Para $n = 1$ esto se cumple por la definición $x_1 := x_0 - \frac{f(x_0)}{f'(x_0)}$. Luego, notemos que según (1.1), tenemos la desigualdad estricta

$$\|x_{n+1} - x_n\| \le \|f'(x_0)\|\, \delta^{2^n} < \|f'(x_0)\|\, \delta = \left\| \frac{f(x_0)}{f'(x_0)} \right\|.$$

Esto nos da el paso inductivo: si $\|x_n - x_0\| = \left\| \frac{f(x_0)}{f'(x_0)} \right\|$, entonces

$$\|x_{n+1} - x_0\| = \|(x_{n+1} - x_n) + (x_n - x_0)\| \le \text{máx}\{\|x_{n+1} - x_n\|, \|x_n - x_0\|\} = \left\| \frac{f(x_0)}{f'(x_0)} \right\|.$$

Para terminar la demostración, nos queda solo ver que los números x_n cumplen las propiedades 1_n), 2_n), 3_n). Para $n = 0$, estas son nuestras hipótesis sobre x_0. Para el paso inductivo, tenemos que ver que 1_n), 2_n), 3_n) implican 1_{n+1}), 2_{n+1}), 3_{n+1}). Primero, x_{n+1} está bien definido, ya que según 2_n),

$$\|f'(x_n)\| = \|f'(x_0)\| \ne 0,$$

y por lo tanto $f'(x_n) \ne 0$ (en efecto, la hipótesis $\|f(x_0)\| < \|f'(x_0)\|^2$ implica que $\|f'(x_0)\| \ne 0$). Para demostrar 1_{n+1}):

$$\|x_{n+1}\| = \left\| x_n - \frac{f(x_n)}{f'(x_n)} \right\| \le \text{máx}\{\|x_n\|, \left\| \frac{f(x_n)}{f'(x_n)} \right\|\} \overset{???}{\le} 1$$

es suficiente ver que $\left\| \frac{f(x_n)}{f'(x_n)} \right\| \le 1$. Esto sigue de las propiedades 2_n) y 3_n):

$$\left\| \frac{f(x_n)}{f'(x_n)} \right\| = \left\| \frac{f(x_n)}{f'(x_0)} \right\| \le \|f'(x_0)\|\, \delta^{2^n} \le 1.$$

Para demostrar 2_{n+1}), notemos que $\|f(x_n)\| \le \|f'(x_0)\|^2\, \delta^{2^n}$ según 3_n), y ya que $\delta < 1$, tenemos $\|f(x_n)\| < \|f'(x_0)\|^2$. La desigualdad 1.2 para $f'(X)$ nos da

$$\|f'(x_{n+1}) - f'(x_n)\| \le \|x_{n+1} - x_n\| = \left\| \frac{f(x_n)}{f'(x_n)} \right\| = \left\| \frac{f(x_n)}{f'(x_0)} \right\| < \|f'(x_0)\|.$$

Pero la desigualdad estricta

$$\|f'(x_{n+1}) - f'(x_n)\| < \text{máx}\{\|f'(x_{n+1})\|, \|f'(x_n)\|\}$$

es posible solo si $\|f'(x_{n+1})\| = \|f'(x_n)\|$. Esto demuestra 2_{n+1}). Para ver 3_{n+1}), podemos usar la identidad de 1.3 para x_n y $-\frac{f(x_n)}{f'(x_n)}$:

$$f(x_{n+1}) = f\left(x_n - \frac{f(x_n)}{f'(x_n)}\right) = f(x_n) + f'(x_n)\left(-\frac{f(x_n)}{f'(x_n)}\right) + z\left(-\frac{f(x_n)}{f'(x_n)}\right)^2 = z\left(-\frac{f(x_n)}{f'(x_n)}\right)^2$$

para algún $z \in \mathcal{O}_K$ (es decir, $\|z\| \le 1$). Entonces, usando 2_n) y la desigualdad 3_n), tenemos

$$\|f(x_{n+1})\| \le \left\| \frac{f(x_n)}{f'(x_n)} \right\|^2 \le \frac{(\|f'(x_0)\|^2\, \delta^{2^n})^2}{\|f'(x_0)\|^2} = \|f'(x_0)\|^2\, \delta^{2^{n+1}}.$$

Esto termina la demostración de 1_n), 2_n), 3_n) para todo n. ∎

1.4. Ejemplo. Recordemos el método de Newton del análisis real. Para resolver una ecuación $f(x) = 0$, se empieza por algún x_0 y luego se consideran las aproximaciones consecutivas

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Geométricamente, x_{n+1} es la intersección del eje x con la tangente a $f(x)$ en $x = x_n$. Si la aproximación inicial x_0 es buena, los x_n convergen a una raíz de f. Por ejemplo, si $f(x) = x^2 - 2$, entonces $f'(x) = 2\,x$, y empezando por $x_0 = 1$, se obtiene

$$x_1 = 1{,}5, \quad x_2 = 1{,}416666\ldots, \quad x_3 = 1{,}414215\ldots, \quad x_4 = 1{,}414213\ldots, \quad \ldots$$

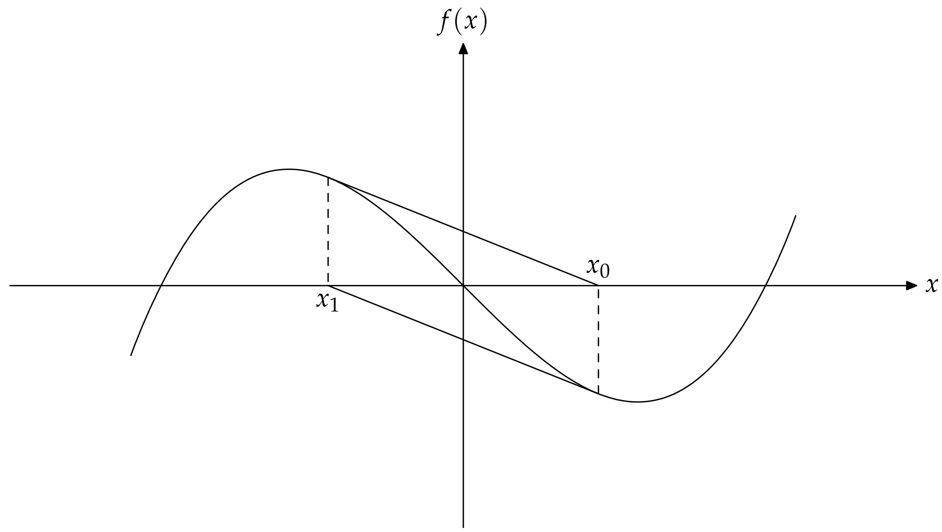
lo que converge rápidamente a $\sqrt{2}$.

```
? x = 1.0;
? for (i=0,6, printf ("x%d = %s\n", i,x); x = x - (x^2-2)/(2*x));
x0 = 1.0000000000000000000000000000000000000
x1 = 1.5000000000000000000000000000000000000
x2 = 1.4166666666666666666666666666666666667
x3 = 1.4142156862745098039215686274509803922
x4 = 1.4142135623746899106262955788901349101
x5 = 1.4142135623730950488016896235025302436
x6 = 1.4142135623730950488016887242096980786

? sqrt (2)
% =  1.4142135623730950488016887242096980786
```

Sin embargo, en algunos casos el método no converge. Por ejemplo, si $f(x) = x^3 - x$ y empezamos por $x_0 = 1/\sqrt{5}$, entonces

$$\begin{aligned}
x_1 &= \frac{1}{\sqrt{5}} - \frac{(1/\sqrt{5})^3 - 1/\sqrt{5}}{3\,(1/\sqrt{5})^2 - 1} = \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{5}} \cdot \frac{1/5 - 1}{3/5 - 1} = -\frac{1}{\sqrt{5}}, \\
x_2 &= -\frac{1}{\sqrt{5}} - \frac{(-1/\sqrt{5})^3 + 1/\sqrt{5}}{3\,(-1/\sqrt{5})^2 - 1} = -\frac{1}{\sqrt{5}} + \frac{1}{\sqrt{5}} \cdot \frac{1/5 - 1}{3/5 - 1} = \frac{1}{\sqrt{5}} = x_0, \\
x_2 &= x_1 = -\frac{1}{\sqrt{5}}, \\
&\ldots
\end{aligned}$$



En el caso no-arquimediano, el método de Newton siempre converge: la única condición para la aproximación inicial es $\|f(x_0)\| < \|f'(x_0)\|^2$. ▲

La demostración de arriba nos da un algoritmo concreto para calcular el resultado con una dada precisión. La desigualdad

$$\|x_{n+1} - x_n\| \le \|f'(x_0)\|\, \delta^{2^n}$$

de (1.1) implica que para todo $m > n$ se cumple

$$\|x_m - x_n\| \le \|f'(x_0)\|\, \delta^{2^n}$$

(use la desigualdad ultramétrica). Para $m \to \infty$ esto nos da

$$\|x - x_n\| \le \|f'(x_0)\|\, \delta^{2^n} = \|f'(x_0)\| \cdot \left\| \frac{f(x_0)}{f'(x_0)^2} \right\|^{2^n},$$

lo que significa que a cada paso la precisión por lo menos se dobla y el algoritmo es bastante eficaz.

1.5. Ejemplo. Calculemos una raíz cuadrada 3-ádica de 7. Buscamos entonces las raíces del polinomio $f(X) = X^2 - 7$ en $\mathbb{Z}_3$. Módulo 3 tenemos dos soluciones: $1^2 - 7 \equiv 0 \pmod 3$ y $2^2 - 7 \equiv 0 \pmod 3$. Consideremos, por ejemplo, $x_0 = 1$. Tenemos

$$|f(x_0)|_3 = |-6|_3 = \frac{1}{3}, \quad |f'(x_0)|_3^2 = |2|_3^2 = 1,$$

entonces la condición $|f(x_0)|_3 < |f'(x_0)|_3^2$ se cumple, y el lema de Hensel nos dice que existe único $x \in \mathbb{Z}_3$ tal que $f(x) = 0$ y $|x - x_0|_3 < 1$; es decir, $x \equiv x_0 \pmod 3$. Además, la demostración nos da una sucesión específica x_n tal que $x = \lim_{n\to\infty} x_n$. Calculemos algunos de estos x_n por la fórmula

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Tenemos

$$\begin{aligned} x_1 &= 1 - \frac{1^2 - 7}{2 \cdot 1} = 4, \\ x_2 &= 4 - \frac{4^2 - 7}{2 \cdot 4} = \frac{23}{8}, \\ x_3 &= \frac{977}{368}, \\ &\cdots \end{aligned}$$

La expansión 3-ádica de x_3 es dada por

$$1 + 3 + 3^2 + 2 \cdot 3^4 + 2 \cdot 3^7 + 3^9 + 3^{10} + 2 \cdot 3^{11} + 2 \cdot 3^{13} + \cdots$$

(esto se puede calcular en PARI/GP). Además, sabemos que el número de los dígitos p-ádicos correctos en las aproximaciones x_n por lo menos se dobla a cada paso; es decir,

$$v_p(x - x_n) \geq 2^n \iff x \equiv x_n \pmod{p^{2^n}}.$$

En particular, en x_3 los dígitos hasta a_7 coinciden con los dígitos de la verdadera raíz cuadrada x de 7 tal que $x \equiv 1 \pmod{3}$. Tenemos

$$x = 1 + 3 + 3^2 + 2 \cdot 3^4 + 2 \cdot 3^7 + \cdots$$

Si empezamos por $x_0' = 2$, se obtiene otro número $x' \in \mathbb{Z}_p$ tal que $x'^2 = 7$ y $x' \equiv x_0' \pmod{3}$. Es la otra raíz cuadrada de 7. Por supuesto, $x = -x'$:

$$-x = 2 + 3 + 3^2 + 2 \cdot 3^3 + 2 \cdot 3^5 + 2 \cdot 3^6 + 0 \cdot 3^7 + \cdots$$

Podemos verificar nuestro cálculo en PARI/GP:

```
? (1 + 3 + 3^2 + 2*3^4 + 2*3^7 + O (3^8))^2
% = 1 + 2*3 + O(3^8)

? (2 + 3 + 3^2 + 2*3^3 + 2*3^5 + 2*3^6 + O(3^8))^2
% = 1 + 2*3 + O(3^8)
```

PARI/GP puede calcular raíces cuadradas de números p-ádicos directamente:

```
? sqrt (7 + O (3^10))
% = 1 + 3 + 3^2 + 2*3^4 + 2*3^7 + 3^8 + 3^9 + O(3^10)
```

▲

Vamos a escribir simplemente "$\sqrt{x}$" para denotar una raíz cuadrada de $x \in \mathbb{Q}_p$. Esta notación viene del análisis real, donde $\sqrt{x}$ para $x > 0$ normalmente denota el número *positivo* tal que $(\sqrt{x})^2 = x$. En el caso p-ádico, también hay dos posibilidades, y la diferencia es el signo ± 1, pero ya no hay un modo tan canónico de elegir uno. Por ejemplo, la función `sqrt(x)` en PARI/GP devuelve la raíz cuadrada con el primer dígito p-ádico $0 \leq a_0 \leq p/2$.

En PARI/GP, `padicappr(f,a)` devuelve las raíces p-ádicas del polinomio f congruentes a a módulo p.

```
? padicappr(x^2-7, 1 + O (3^10))
% = [1 + 3 + 3^2 + 2*3^4 + 2*3^7 + 3^8 + 3^9 + O(3^10)]~
? padicappr(x^2-7, 2 + O (3^10))
% = [2 + 3 + 3^2 + 2*3^3 + 2*3^5 + 2*3^6 + 3^8 + 3^9 + O(3^10)]~
```

Ejercicio 1. Usando el método de Newton, calcule los primeros 8 dígitos de las raíces cuadradas $\pm\sqrt{-1}$ en $\mathbb{Q}_5$ y $\pm\sqrt{-3}$ en $\mathbb{Q}_7$. (Use PARI/GP para hacer cálculos con números racionales y encontrar sus expansiones p-ádicas).

1.6. Ejemplo. Calculemos la raíz cuadrada $\sqrt{1+X}$ en $\mathbb{Q}[\![X]\!]$; es decir, encontremos las raíces del polinomio $F(Z) = Z^2 - 1 - X \in \mathbb{Q}[\![X]\!][Z]$. Para $f_0 = 1$ tenemos

$$v_X(F(1)) = v_X(-X) = 1, \quad v_X(F'(1)) = v_X(2) = 0.$$

Entonces, se cumple $|F(1)|_X < |F'(1)|_X^2$ y podemos calcular las aproximaciones

$$f_{n+1} = f_n - \frac{F(f_n)}{F'(f_n)} = f_n - \frac{f_n^2 - 1 - X}{2\, f_n}.$$

Esta vez sería mejor hacerlo con ayuda de PARI/GP:

```
? f = 1;
? for (n=1,3, f = f - (f^2-1-X)/(2*f); printf ("f_%d = %s\n", n,f));
f_1 = 1/2*X + 1
f_2 = (X^2 + 8*X + 8)/(4*X + 8)
f_3 = (X^4 + 32*X^3 + 160*X^2 + 256*X + 128)/(8*X^3 + 80*X^2 + 192*X + 128)

? f + O (X^8)
% = 1 + 1/2*X - 1/8*X^2 + 1/16*X^3 - 5/128*X^4 + 7/256*X^5 - 21/1024*X^6 + 33/2048*X^7 + O(X^8)
```

Como sabemos, los coeficientes de f_3 coinciden con los coeficientes de $\sqrt{X+1} = \sum_{i\ge 0} a_i\, X^i$ por lo menos hasta a_7. Entonces,

$$\sqrt{X+1} = 1 + \frac{1}{2}\,X - \frac{1}{8}\,X^2 + \frac{1}{16}\,X^3 - \frac{5}{128}\,X^4 + \frac{7}{256}\,X^5 - \frac{21}{1024}\,X^6 + \frac{33}{2048}\,X^7 + \cdots$$

Lo que acabamos de calcular son los primeros coeficientes de la serie binomial

$$(1+X)^{1/m} = \sum_{i\ge 0} \binom{1/m}{i}\, X^i,$$

donde

$$\binom{Y}{i} := \frac{Y\,(Y-1)\cdots(Y-i+1)}{i!} \in \mathbb{Q}[Y].$$

▲

```
? (1+X)^(1/2) + O (X^8)
% = 1 + 1/2*X - 1/8*X^2 + 1/16*X^3 - 5/128*X^4 + 7/256*X^5 - 21/1024*X^6 + 33/2048*X^7 + O(X^8)

? vector (7,i,binomial(1/2,i))
% = [1/2, -1/8, 1/16, -5/128, 7/256, -21/1024, 33/2048]
```

El resto de este texto está dedicado a algunas aplicaciones típicas del lema de Hensel para los números p-ádicos.

2 Cuadrados en $\mathbb{Q}_p$

2.1. Proposición.

1) *Para $p \neq 2$, un número $u \in \mathbb{Z}_p^\times$ es un cuadrado en $\mathbb{Q}_p$ (es decir, $u = x^2$ para algún $x \in \mathbb{Q}_p$) si y solamente si u es un cuadrado módulo p.*

2) *Un número $u \in \mathbb{Z}_2^\times$ es un cuadrado en $\mathbb{Q}_2$ si y solamente si $u \equiv 1 \pmod{8}$.*

Demostración. Supongamos que $p \neq 2$. Si $u = x^2$ en $\mathbb{Q}_p$, notamos que $|x|_p^2 = |u|_p = 1$, y por lo tanto $x \in \mathbb{Z}_p^\times$. Luego, se tiene $u \equiv x^2 \pmod{p}$. En la otra dirección, si la ecuación $f(X) = X^2 - u$ tiene solución módulo p, esto significa que existe un número $0 \leq x_0 \leq p-1$ tal que $x_0^2 - u \equiv 0 \pmod{p}$. En términos de normas, $|f(x_0)|_p \leq 1/p$, mientras que $|f'(x_0)^2|_p = |2\,x_0|_p^2 = 1$, puesto que $p \neq 2$. Entonces, podemos aplicar el lema de Hensel que nos da un elemento $x \in \mathbb{Z}_p$ tal que $f(x) = x^2 - u = 0$.

En el caso de $p = 2$, de la misma manera, $u = x^2$ para algún $x \in \mathbb{Q}_2$ implica $x \in \mathbb{Z}_2^\times$ y podemos considerar la reducción módulo 8. En el anillo $\mathbb{Z}_2/8\mathbb{Z}_2 \cong \mathbb{Z}/8\mathbb{Z}$, los elementos invertibles son $1, 3, 5, 7$, y todos sus cuadrados son congruentes a 1 módulo 8:

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

Entonces, se tiene necesariamente $x^2 \equiv 1 \pmod{8}$. En la otra dirección, si $u \in \mathbb{Z}_2^\times$ satisface $u \equiv 1 \pmod{8}$, esto quiere decir que $|1-u|_2 \leq 1/8$. Apliquemos el lema de Hensel al polinomio $f(X) = X^2 - u$. Para $x_0 = 1$ tenemos

$$|f(x_0)|_2 = |1-u|_2 \leq 1/8 < |f'(x_0)|_2^2 = |2|_2^2 = 1/4,$$

así que existe $x \in \mathbb{Z}_2$ tal que $u = x^2$. ■

Hemos encontrado los cuadrados en $\mathbb{Z}_p^\times$, pero ¿qué sucede con los cuadrados en $\mathbb{Q}_p$? Pues, todo elemento $x \in \mathbb{Q}_p^\times$ puede ser escrito como $x = p^n\,u$, donde $n \in \mathbb{Z}$ y $u \in \mathbb{Z}_p^\times$. Luego, $|x|_p = |p^n\,u|_p = 1/p^n$. Note que si x es un cuadrado, entonces n tiene que ser par. Esto nos dice que los cuadrados en $\mathbb{Q}_p^\times$ son precisamente los números $p^n\,u$ donde $n \in \mathbb{Z}$ es par y u es un cuadrado en $\mathbb{Z}_p^\times$.

Ejercicio 2. Denotemos por $(\mathbb{Q}_p^\times)^2$ el grupo multiplicativo de cuadrados en $\mathbb{Q}_p^\times$. Demuestre que

$$\begin{aligned}
&\mathbb{R}^\times/(\mathbb{R}^\times)^2 \cong C_2,\\
&\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong C_2 \times C_2, \quad \text{si } p \neq 2,\\
&\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong C_2 \times C_2 \times C_2.
\end{aligned}$$

Ejercicio 3. Demuestre que si $p \equiv 2 \pmod{3}$, entonces para todo $a \in \mathbb{Z}$ tal que $p \nmid a$ tenemos $\sqrt[3]{a} \in \mathbb{Q}_p$. Para $p \not\equiv 2 \pmod{3}$, encuentre algún a tal que $p \nmid a$ y $\sqrt[3]{a} \notin \mathbb{Q}_p$.

El lector que todavía empieza a estudiar los números p-ádicos probablemente se había planteado la siguiente pregunta. El cuerpo $\mathbb{Q}_p$ contiene el cuerpo $\mathbb{Q}$ donde existe la noción de números positivos y negativos. ¿Se puede definir algo parecido para $\mathbb{Q}_p$?

Recordemos la siguiente definición. Se dice que un cuerpo F es **ordenado** si está definido un subconjunto $P \subset F$ de **elementos positivos** con las siguientes propiedades:

1) Para $x \in F$ se cumple precisamente una de las siguientes relaciones:

$$x \in P, \quad x = 0, \quad -x \in P.$$

2) Si $x, y \in P$, entonces $x + y \in P$ y $xy \in P$.

Normalmente si $x \neq 0$ y $x \in P$, se escribe "$x > 0$"; si $x \neq 0$ y $-x \in P$, se escribe "$x < 0$". De los axiomas se sigue que $1 > 0$ y $-1 < 0$: de hecho, $1 = 1^2 = (-1)^2$. Luego, la propiedad 2) implica que para todo $n = 1, 2, 3, \ldots$ tenemos

$$\underbrace{1 + \cdots + 1}_{n} > 0, \quad -\underbrace{(1 + \cdots + 1)}_{n} < 0.$$

En particular, un cuerpo de característica positiva no puede ser ordenado. Para $x \neq 0$ tenemos $x^2 = (-x)^2$, lo que significa que $x^2 > 0$ para todo $x \neq 0$: *todos los cuadrados de números no nulos tienen que ser positivos*.

Por ejemplo, $\mathbb{Q}$ y $\mathbb{R}$ son cuerpos ordenados. El cuerpo $\mathbb{C}$ no es ordenado: tenemos $i^2 = -1 < 0$, un cuadrado que no es positivo. De la misma manera, se puede ver que los cuerpos p-ádicos $\mathbb{Q}_p$ no son ordenados, ya que en cada uno de ellos se puede encontrar muchos cuadrados negativos.

2.2. Observación. *$\mathbb{Q}_p$ no puede ser ordenado para ningún primo finito p.*

Demostración. Por ejemplo, el cuerpo $\mathbb{Q}_2$ contiene la raíz cuadrada $\pm\sqrt{-7}$, y luego $(\sqrt{-7})^2 = -7 < 0$. Para $p > 2$, el cuerpo $\mathbb{Q}_p$ contiene, por ejemplo, $\pm\sqrt{1-p}$, y luego $(\sqrt{1-p})^2 = 1 - p < 0$. ■

3 Raíces de la unidad en $\mathbb{Q}_p$

Una **raíz n-ésima de la unidad** es un número $\zeta \in \mathbb{Q}_p$ tal que $\zeta^n = 1$. Notamos que esto implica que $|\zeta|_p = 1$, así que las raíces de la unidad en $\mathbb{Q}_p$ forman un subgrupo $\mu(\mathbb{Q}_p)$ del grupo multiplicativo $\mathbb{Z}_p^\times$. La reducción módulo p nos da un homomorfismo de grupos

$$\phi\colon \mu(\mathbb{Q}_p) \hookrightarrow \mathbb{Z}_p^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times. \tag{3.1}$$

3.1. Proposición. *El homomorfismo ϕ es sobreyectivo; específicamente, en $\mathbb{Q}_p$ hay raíces de orden $p-1$ que dan diferentes restos módulo p.*

Demostración. Consideremos el polinomio

$$f(X) = X^p - X = X\,(X^{p-1} - 1) \in \mathbb{Z}_p[X]$$

cuyas raíces no nulas corresponden a las raíces de la unidad de orden $p-1$. Según el pequeño teorema de Fermat la ecuación

$$x_0^p - x_0 \equiv 0 \pmod{p}$$

tiene p soluciones $0 \le x_0 \le p-1$. Tenemos

$$|f(x_0)|_p \le 1/p < |f'(x_0)|_p^2 = |p\,x_0^{p-1} - 1|_p^2 = 1,$$

así que el lema de Hensel funciona y para cada x_0 produce un elemento único $x \in \mathbb{Z}_p$ que satisface $x^p - x = 0$ y $x \equiv x_0 \pmod{p}$. ■

Ejercicio 4. He aquí otro modo de encontrar las raíces de la unidad de orden $p-1$. Demuestre que para todo $x \in \mathbb{Z}_p$ se cumple

$$x^{p^{n+1}} \equiv x^{p^n} \pmod{p^{n+1}}$$

y que el límite $\lim_{n\to\infty} x^{p^n}$ existe, y es precisamente la raíz del polinomio $X^p - X$ que es congruente a x modulo p.

En $\mathbb{Q}_p$ no hay otras raíces de la unidad.

3.2. Proposición. *Las únicas raíces de la unidad en $\mathbb{Q}_2$ son ± 1.*

Las únicas raíces de la unidad en $\mathbb{Q}_p$ para $p \neq 2$ son las $(p-1)$-ésimas raíces que acabamos de encontrar.

Demostración. **Primero examinemos el caso** $p = 2$. Toda raíz de la unidad $\zeta \in \mu(\mathbb{Q}_2)$ es un producto de una raíz de la unidad de orden 2^k y una raíz de la unidad de orden impar n, así que será suficiente considerar las raíces de orden 2^k y orden impar por separado.

La raíz de la unidad primitiva de orden 2 es -1, pero -1 no es un cuadrado en $\mathbb{Z}_2^\times$, así que en $\mathbb{Z}_2^\times$ no hay raíces de la unidad de orden 2^k para $k \geq 2$.

Ahora sea $\zeta \in \mu(\mathbb{Q}_2)$ una raíz de la unidad tal que $\zeta^n = 1$ para n impar. Consideremos el polinomio $f(X) = X^n - 1$. Tenemos $f(1) = 0$ y $f'(1) = n \not\equiv 0 \pmod{2}$, y entonces el lema de Hensel nos dice que existe *único* $x \in \mathbb{Z}_2$ tal que $f(x) = 0$ y $x \equiv 1 \pmod{2}$. Pero *todo* elemento de $\mathbb{Z}_2^\times$ se reduce a 1 módulo 2, así que $\zeta = 1$. Esto demuestra que en $\mathbb{Z}_2^\times$ no hay raíces de la unidad no triviales de orden impar.

Ahora examinemos el caso $p \neq 2$. Hemos probado usando el lema de Hensel que el homomorfismo $\phi\colon \mu(\mathbb{Q}_p) \to (\mathbb{Z}/p\mathbb{Z})^\times$ de (3.1) es sobreyectivo, y hay que demostrar que ϕ es también inyectivo. Sea $\zeta \in \mu(\mathbb{Q}_p)$ una n-ésima raíz de la unidad tal que $\phi(\zeta) = 1$; a saber, $\zeta = 1 + p\,x$ para algún $x \in \mathbb{Z}_p$. Necesitamos ver que $x = 0$. Tenemos

$$\zeta^n = (1 + p\,x)^n = 1,$$

y entonces, aplicando el teorema del binomio,

$$n\,p\,x + \binom{n}{2} p^2\,x^2 + \binom{n}{3} p^3\,x^3 + \cdots + p^n\,x^n = 0.$$

Luego,

$$x\left(n + \binom{n}{2} p\,x + \binom{n}{3} p^2\,x^2 + \cdots + p^{n-1}\,x^{n-1}\right) = 0.$$

Si $p \nmid n$, entonces la expresión en paréntesis no puede ser nula y $x = 0$. Si $p \mid n$, podemos reemplazar ζ por ζ^p y n por n/p. De nuevo, el mismo argumento demuestra que $x = 0$ o $p \mid n$. Repitiendo este proceso, todo se reduce al caso $n = p$. Tenemos entonces

$$x\left(p + \binom{p}{2} p\,x + \binom{p}{3} p^2\,x^2 + \cdots + p^{p-1}\,x^{p-1}\right) = 0.$$

Sin embargo, $p \neq 2$, así que todos los términos en la suma

$$\binom{p}{2} p\,x + \binom{p}{3} p^2\,x^2 + \cdots + p^{p-1}\,x^{p-1}$$

son divisibles por p^2, la expresión en paréntesis no puede ser nula y $x = 0$. ■

3.3. Corolario. *Los cuerpos $\mathbb{Q}_p$ no son isomorfos para diferentes p.*

Demostración. El orden del grupo de las raíces de la unidad nos permite distinguir todos los $\mathbb{Q}_p$, excepto $\mathbb{Q}_2$ y $\mathbb{Q}_3$, donde las raíces de la unidad son ± 1. En este caso excepcional podemos notar, por ejemplo, que $\sqrt{-2} \in \mathbb{Q}_3$, mientras que $\sqrt{-2} \notin \mathbb{Q}_2$. ■

Ejercicio 5. Sea p un número primo.

1) Sea n un número entero, posiblemente negativo. Demuestre que si $p \nmid n$ y $x \in \mathbb{Z}_p$ satisface $x \equiv 1 \pmod{p}$, entonces x tiene una raíz n-ésima: existe y tal que $y^n = x$.

2) Demuestre que $1 + p$ no tiene raíces p-ésimas en $\mathbb{Q}_p$.

3) Demuestre que $x \in \mathbb{Z}_p$ tiene una raíz p-ésima si $x \equiv 1 \pmod{p^2}$ y $p \neq 2$.

Indicación: use el lema de Hensel en 1). En 2), si $y = b_0 + b_1\,p + b_2\,p^2 + \cdots$, calcule los primeros dígitos p-ádicos de y^p. En 3), use el lema de Hensel con una buena aproximación inicial.

Ejercicio 6. He aquí otro modo de demostrar que $\mathbb{Q}_p$ no tiene raíces p-ésimas de la unidad no triviales.

1) Recuerde el **criterio de Eisenstein** en la siguiente versión. Sea

$$f(X) = a_n\,X^n + a_{n-1}\,X^{n-1} + \cdots + a_1\,X + a_0 \in R[X]$$

un polinomio con coeficientes en un dominio de factorización única R. Sea $p \in R$ un elemento primo tal que

- $p \mid a_i$ para todo $i = 0, \ldots, n-1$,
- $p \mid a_n$,
- $p^2 \nmid a_0$.

Entonces $f(X)$ es irreducible en $K[X]$ donde K es el cuerpo de fracciones de R. Es decir, $f(X)$ no puede ser expresado como un producto de dos polinomios de grado $< n$.

2) Usando el criterio de Eisenstein para $\mathbb{Z}_p[X]$, demuestre que el polinomio ciclotómico

$$f(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

es irreducible en $\mathbb{Q}_p[X]$. Concluya que la única p-ésima raíz de la unidad en $\mathbb{Q}_p$ es 1.

Indicación: en 2), considere el polinomio $f(X+1)$.

4 Automorfismos de $\mathbb{Q}_p$

4.1. Proposición. *El único automorfismo $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ es la aplicación identidad.*

Primero notemos que todo automorfismo $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ deja $\mathbb{Q}$ fijo. Primero, para todo $n \in \mathbb{N}$

$$f(\pm n) = f(\pm \underbrace{1 + \cdots + 1}_{n}) = \pm n\, f(1) = \pm n.$$

Luego, para $m/n \in \mathbb{Q}$ tenemos

$$n\, f\left(\frac{m}{n}\right) = f\left(n\,\frac{m}{n}\right) = f(m) = m,$$

así que $f(m/n) = m/n$.

Se sigue que **el único automorfismo <u>continuo</u> $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ es la aplicación identidad.** De hecho, ya que $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, todo elemento $x \in \mathbb{Q}_p$ puede ser representado como $x = \lim_{n\to\infty} x_n$ para $x_n \in \mathbb{Q}$, y si f es una aplicación continua,

$$f(x) = f\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} x_n = x,$$

puesto que f deja $\mathbb{Q}$ fijo.

Entonces, para demostrar 4.1, sería suficiente ver que todo automorfismo $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ es automáticamente continuo. Para esto nos va a servir una caracterización algebraica del grupo de unidades $\mathbb{Z}_p^\times$.

4.2. Lema. *Las siguientes condiciones son equivalentes para $x \in \mathbb{Q}_p^\times$:*

1) x^{p-1} tiene n-ésimas raíces para un número infinito de n;

2) $x \in \mathbb{Z}_p^\times$.

Demostración. Si $x^{p-1} = y^n$ para algún n, entonces

$$(p-1)\, v_p(x) = n\, v_p(y).$$

Si esto se cumple para un número infinito de n, entonces las relaciones $n \mid (p-1)\, v_p(x)$ implican que $v_p(x) = 0$; es decir, si $x \in \mathbb{Z}_p^\times$.

En la otra dirección, si $x \in \mathbb{Z}_p^\times$, tenemos $x \not\equiv 0 \pmod{p}$, y luego $x^{p-1} \equiv 1 \pmod{p}$ por el pequeño teorema de Fermat. Luego, para $f(X) = X^n - x^{p-1} \in \mathbb{Z}_p[X]$ tenemos $f(1) \equiv 0 \pmod{p}$ y $f'(1) \not\equiv 0$ si $p \nmid n$. El lema de Hensel nos da entonces $y \in \mathbb{Z}_p$ tal que $y^n = x^{p-1}$. ■

El lema que acabamos de demostrar implica que $f(\mathbb{Z}_p^\times) \subseteq \mathbb{Z}_p^\times$. Ahora todo $x \in \mathbb{Q}_p^\times$ puede ser escrito como $x = p^n\, u$, donde $n \in \mathbb{Z}$ y $u \in \mathbb{Z}_p^\times$. Tenemos

$$f(x) = f(p^n\, u) = f(p^n)\, f(u) = p^n\, f(u).$$

Luego,

$$v_p(f(x)) = v_p(p^n\, f(u)) = n = v_p(x).$$

Esto significa que para todo $x, y \in \mathbb{Q}_p$

$$|f(x) - f(y)|_p = |f(x-y)|_p = |x-y|_p.$$

Entonces, f es una aplicación continua, y esto termina la demostración. ■

Ejercicio 7. Demuestre que el único automorfismo $f\colon \mathbb{R} \to \mathbb{R}$ es la aplicación identidad.

1) Note que $f(x^2) = f(x)^2$, así que f aplica números positivos en números positivos y en general, preserva el orden:
$$x \le y \Longrightarrow f(x) \le f(y).$$

2) De nuevo, f es identidad sobre $\mathbb{Q}$. Demuestre que esto junto con preservación del orden implica que f es identidad sobre todo $\mathbb{R}$.

Note que $\mathbb{C}$ ya tiene un número infinito de automorfismos no contínuos.