Congruencias Superiores y Lema de Hensel

Alan Reyes-Figueroa

Teoría de Números (Aula 16) 07.septiembre.2021

Congruencias (Revisión)

Recordemos que al resolver una congruencia

$$f(x) \equiv 0 \pmod{n}, \tag{1}$$

con n compuesto de la forma $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, el Teorema Chino nos dice que dicha congruencia admite solución si, y sólo si, cada congruencia del sistema

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{k_1}}, \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_r^{k_r}}, \end{aligned}$$

tiene solución.

De hecho, si $N(p_i^{k_i})$ indica el número de soluciones de la congruencia $f(x) \equiv 0 \pmod{p_i^{k_i}}$, entonces el número de soluciones de (1) es

$$N(n) = N(p_1^{k_1}) \cdot N(p_2^{k_2}) \cdots N(p_r^{k_r}).$$

Congruencias (Revisión)

Ejemplo: Resolver la ecuación $x^2 + x + 3 \equiv 0 \pmod{15}$.

Observe que $(x+8)^2 \equiv x^2 + 16x + 64 \equiv x^2 + x + 4 \pmod{15}$. Entonces, la congruencia arriba es equivalente a resolver $(x+8)^2 - 1 \equiv (x+8-1)(x+8+1) \equiv (x+7)(x+9) \equiv 0 \pmod{15}$.

Por el Teorema Chino, esta última ecuación es equivalente al sistema

$$\begin{aligned} (x+7)(x+9) &\equiv (x+1)x \equiv 0 \pmod{3}, \\ (x+7)(x+9) &\equiv (x+2)(x+4) \equiv 0 \pmod{5}, \end{aligned}$$

de modo que $x \equiv 0, 2 \pmod{3}$ y $x \equiv 1, 3 \pmod{5}$.

Combinando los cuatro casos anteriores, obtenemos

- $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{5} \Rightarrow \ x \equiv 6 \pmod{15}$.
- $x \equiv 0 \pmod{3}$, $x \equiv 3 \pmod{5} \Rightarrow \ x \equiv 3 \pmod{15}$.
- $x \equiv 2 \pmod{3}$, $x \equiv 1 \pmod{5} \Rightarrow \ x \equiv 11 \pmod{15}$.
- $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5} \Rightarrow \ x \equiv 8 \pmod{15}$.

Portanto, la soluciones son $x \equiv 3, 6, 8, 11 \pmod{15}$.

Ejemplo: Resolver la ecuación $x^2 + x + 7 \equiv 0 \pmod{189}$.

Observe que $189 = 3^3 \cdot 7$. Además, $(x + 14)^2 \equiv x^2 + 28x + 196 \equiv x^2 + x + 7 \equiv 0 \pmod{189}$. Por el Teorema Chino, esta última ecuación es equivalente al sistema

$$\begin{aligned} (x+14)^2 &\equiv 0 \pmod{3^3}, \\ x^2 + x + 7 &\equiv x(x+1) \equiv 0 \pmod{7}, \end{aligned}$$

de modo que $x \equiv -14 \equiv 13 \pmod{27}$ y $x \equiv 0, 6 \pmod{7}$.

Combinando los dos casos anteriores, obtenemos

- $x \equiv 13 \pmod{27}$, $x \equiv 0 \pmod{7}$. Hacemos $n_1 = 7$, $n_2 = 27$, $c_1 = 7^{-1} \equiv 4 \pmod{27}$ y $c_2 = 27^{-1} \equiv 6^{-1} \equiv 6 \pmod{7}$.
  Luego, $x = 13c_1n_1 + 0c_2n_2 = 13(4)(7) = 364 \equiv 175 \equiv -14 \pmod{189}$.
- $x \equiv 13 \pmod{27}$, $x \equiv 6 \pmod{7}$. Hacemos $n_1 = 7$, $n_2 = 27$, $c_1 = 7^{-1} \equiv 4 \pmod{27}$ y $c_2 = 27^{-1} \equiv 6^{-1} \equiv 6 \pmod{7}$.
  Luego, $x = 13c_1n_1 + 6c_2n_2 = 13(4)(7) + 6(6)(27) = 1336 \equiv 13 \pmod{189}$.

Portanto, la soluciones son $x \equiv 13, -14 \pmod{189}$.

Lema de Hensel

El problema de resolver una congruencia se reduce siempre a resolver congruencias módulo p, ó módulo p^k. Para resolver una congruencia polinomial $f(x) \equiv 0 \pmod{p^k}$, comenzamos con una solución módulo p, luego pasamos al módulo p^2, luego a p^3, y por iteración a p^k.

Suponga que $x = a$ es una solución de $f(x) \equiv 0 \pmod{p^j}$ y queremos usarla para obtener una solución módulo p^{j+1}. La idea es intentar obtener una solución de la forma $x = a + tp^j$, donde t se determina mediante la expansión de Taylor

$$f(a + tp^j) = f(a) + tp^j f'(a) + \tfrac{1}{2} t^2 p^{2j} f''(a) + \ldots + \tfrac{1}{n!} t^n p^{nj} f^{(n)}(a), \tag{2}$$

donde $n = \deg f$.

Todas las derivadas más allá de la n-ésima son idénticamente cero. Ahora, en módulo p^{j+1}, la ecuación (2) da

$$f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}, \tag{3}$$

como muestra el siguiente argumento.

Lema de Hensel

Lo que queremos establecer es que los coeficientes de $t^2, t^3, \ldots, t^n$ en la ecuación (2) son todos divisibles por p^{j+1}, por lo que se anulan en (3). Esto parece obvio ya que las potencias de p en esos términos son $p^{2j}, p^{3j}, \ldots, p^{nj}$; pero esto no es del todo inmediato por la presencia de los denominadores $2!, 3!, \ldots n!$ en estos términos.

La explicación es que la fracción $\frac{f^{(k)}(a)}{k!} \in \mathbb{Z}$, para cada valor de $k = 2, \ldots, n$. Para ver esto, sea cx^r un término arbitrario de $f(x)$. El término correspondiente a $f^{(k)}(a)$ es

$$c\, r(r-1)(r-2)\cdots(r-k+1)a^{r-k}.$$

Este término es el producto de k enteros consecutivos, de modo que es divisible entre $k!$. Portanto, los coeficientes de $t^2, t^3, \ldots, t^n$ en (2) son divisibles por p^{j+1}.

La congruencia (3) revela cómo debe elegirse t si $x = a + tp^j$ es una solución de $f(x) \equiv 0 \pmod{p^{j+1}}$. Queremos que sea una solución de

$$f(a) + tp^j f'(a) \equiv 0 \pmod{p^{j+1}}. \tag{4}$$

Lema de Hensel

Como $f(x) \equiv 0 \pmod{p^j}$ tiene solución $x = a$, ambos lados de la congruencia (4) tienen un factor p^j. Eliminando este factor, resulta

$$tf'(a) \equiv -\tfrac{1}{p^j} f(a) \pmod{p}, \tag{5}$$

la cual es una congruencia lineal en t. Esta congruencia puede no tener solución, una solución ó p soluciones. Si $f'(a) \not\equiv 0 \pmod{p}$, esta congruencia tiene exactamente una solución, y hemos demostrado el siguiente resultado

Teorema (Lema de Hensel)

Suponga que $f(x)$ es un polinomio con coeficientes enteros. Si $f(a) \equiv 0 \pmod{p^j}$ y $f'(a) \not\equiv 0 \pmod{p}$, entonces existe un único $t \pmod{p}$ tal que $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$. $\square$

Si $f(a) \equiv 0 \pmod{p^j}$ y $f(b) \equiv 0 \pmod{p^k}$, con $j < k$, entonces decimos que b se está **por encima** de a, o que b es el **levantamiento** de a, o que a se eleva a b.

Lema de Hensel

Si $f(a) \equiv 0 \pmod{p^j}$, entonces la raíz a se llama **no singular** si $f'(a) \not\equiv 0 \pmod{p}$; de lo contrario es una raíz **singular**.

Por el Lema de Hensel, vemos que una raíz no singular $a \pmod{p}$ se eleva a una raíz única $a_2 \pmod{p^2}$. Dado que $a_2 \equiv a \pmod{p}$, se sigue que $f'(a_2) \equiv f'(a) \not\equiv 0 \pmod{p}$. Una segunda aplicación del Lema de Hensel, implica que podemos levantar a_2 para formar una raíz a_3 de $f(x)$ módulo p^3. En general, encontramos que una raíz no singular $a \pmod{p}$ se eleva a una raíz única a_j módulo p^j, para $j = 2, 3, \ldots$.

Por (5) vemos que esta secuencia se genera mediante la recursividad

$$a_{j+1} \equiv a_j + tp^j \equiv a_j - \frac{f(a_j)}{f'(a_j)} \equiv a_j - f(a_j) f'(a_j)^{-1} \pmod{p}, \tag{6}$$

donde $f'(a)^{-1}$ es un número entero elegido de modo que $f'(a) f'(a)^{-1} \equiv 1 \pmod{p}$.

Obs! Note que (6) es análogo al método de Newton para hallar la raíz de una función diferenciable.

Lema de Hensel

Ejemplo: Resolver $x^2 + x + 47 \equiv 0 \pmod{7^3}$.

Note que $f(x) = x^2 + x + 47 \equiv x^2 + x + 5 \equiv (x+4)^2 + 3 \equiv (x^2+4) - 2^2 \equiv (x+2)(x+6) \pmod 7$. Luego, $x \equiv 1, 5 \pmod 7$ son las únicas soluciones de $x^2 + x + 47 \equiv 0 \pmod 7$.

Como $f'(x) = 2x + 1$, vemos que $f'(1) = 3 \not\equiv 0 \pmod 7$, y $f'(5) = 11 \equiv 4 \not\equiv 0 \pmod 7$. Entonces, las raíces no son singulares.

- Tomando $a_1 = 1$, $f'(1) = 5$, y de (6) tenemos que a_1 se eleva a
$$a_2 = a_1 - f(a_1)f'(a_1)^{-1} = 1 - 49(3)^{-1} = 1 - 49(5) = 1 \pmod{7^2}.$$
Ahora $f'(a_2) = f'(1) = 3$, y una nueva aplicación de Hensel implica
$$a_3 = a_2 - f(a_2)f'(a_2)^{-1} = 1 - 49(3)^{-1} = 1 - 49(5) = -244 \equiv 99 \pmod{7^3}.$$
- Si $a_1 = 5$, $\Rightarrow a_2 = a_1 - f(a_1)f'(a_1)^{-1} = 5 - 77(4)^{-1} = 5 - 77(2) = -149 \equiv -2 \pmod{7^2}$. Como $f'(-2) = 4$, $\Rightarrow a_3 = a_2 - f(a_2)f'(a_2)^{-1} = -2 - 49(2) = -100 \equiv 243 \pmod{7^3}$.

De ahí que 99 y 243 son las soluciones deseadas $\pmod{343}$.

Pasamos ahora al problema más difícil de levantar raíces singulares.

Suponga que $f(a) \equiv 0 \pmod{p^j}$ y que $f'(a) \equiv 0 \pmod{p}$. De la expansión de Taylor (2), vemos que $f(a+tp^j) \equiv f(a) \pmod{p^{j+1}}$, para todo $t \in \mathbb{Z}$.

Entonces, si $f(a) \equiv 0 \mod p^{j+1}$, se tiene que $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$, de modo que la raíz única $a \pmod{p^j}$ se eleva a p raíces módulo p^{j+1}.

Pero si $f(a) \not\equiv 0 \pmod{p^{j+1}}$, entonces ninguna de las p clases de residuos $a+tp^j$ es una solución módulo p^{j+1}, y luego no hay raíces $\pmod{p^{j+1}}$ encima de $a \pmod{p^j}$.

Ejemplo: Resolver $x^2+x+7 \pmod{81}$.

Comenzando con $f(x) = x^2+x+7 \pmod{3}$, tenemos $x^2x+7 \equiv x^2+x+1 \equiv (x+2)^2 \equiv (x-1)^2 \equiv 0 \pmod{3}$. Luego, $a_1 = x \equiv 1 \pmod{3}$ es la única solución.

En este caso, $f'(1) = 3 \equiv 0 \pmod{3}$, y $f(1) = 3 \equiv 0 \pmod{9}$, de modo que $a_2 = a_1 + tp$ es solución de la congruencia $f(x) \equiv 0 \pmod{3^2}$, para todo $t \in \mathbb{Z}$.

Lema de Hensel

Tenemos entonces las raíces para a_2: $x \equiv 1, 4, 7 \pmod 9$.

- Tome $a_2 = 1$. Ahora $f(1) = 9 \not\equiv 0 \pmod{27}$, $f'(1) = 3 \equiv 0 \pmod 3$, y por lo tanto no hay raíz $x \pmod{27}$ para la cual $x \equiv 1 \pmod 9$.
- Para $a_2 = 4$. Ahora $f(4) = 27 \equiv 0 \pmod{27}$, $f'(1) = 9 \equiv 0 \pmod 3$, y por lo tanto $a_3 = 4 + tp^2$ son raíces módulo 27. Así, hay tres raíces raíz $x = 4, 13, 22 \pmod{27}$, que son congruentes con $4 \pmod 9$.
- Por otro lado, si $a_2 = 7$, ahora $f(7) = 63 \not\equiv 0 \pmod{27}$, $f'(7) = 15 \equiv 0 \pmod 3$, por lo que no hay raíces $a_3 \pmod{27}$ congruentes con $7 \pmod 9$.

Ahora estamos en condiciones de determinar cuáles de las raíces $4, 13, 22 \pmod{27}$ se pueden levantar hasta las raíces $\pmod{81}$.

Encontramos que $f(4) = 27 \not\equiv 0 \pmod{81}$, $f(13) = 189 \equiv 27 \not\equiv 0 \pmod{81}$ y $f(22) = 513 \equiv 27 \not\equiv 0 \pmod{81}$, de donde deducimos que la congruencia $f(x) \equiv 0$ no tiene solución $\pmod{81}$.

En este ejemplo, vemos que una solución singular $a \pmod p$ puede elevarse a algunas potencias superiores de p, pero no necesariamente a potencias arbitrariamente altas. Ahora mostramos que si la potencia de p que divide a $f(a)$ es suficientemente grande en comparación con la potencia de p que divide a $f'(a)$, entonces la solución se puede levantar sin límite.

Teorema

Sea $f(x)$ un polinomio con coeficientes enteros. Suponga que $f(a) \equiv 0 \pmod{p^j}$, que $p^\tau \,\|\, f'(a)$, y que $j \geq 2\tau + 1$. Si $b \equiv a \pmod{p^{j-\tau}}$, entonces $f(b) \equiv f(a) \pmod{p^j}$ y $p^\tau \,\|\, f'(b)$. Además, hay una única $t \pmod p$ tal que $f(a + tp^{j-\tau}) \equiv 0 \pmod{p^{j+1}}$.

En esta situación, una colección de p^τ soluciones $\pmod{p^j}$ dan lugar a p^τ soluciones $\pmod{p^{j+1}}$, mientras que la potencia de p dividiendo f' permanece constante. Dado que las hipótesis del teorema se aplican con a reemplazado por $a + tp^{j-\tau}$ y $\pmod{p^j}$ reemplazado por $\pmod{p^{j+1}}$, con τ sin cambios, el levantamiento puede repetirse y continúa indefinidamente.

Lema de Hensel

Prueba: Por la expansión de Taylor (2), vemos que

$$f(b) = f(a + tp^{j-\tau}) \equiv f(a) + tp^{j-\tau} f'(a) \pmod{p^{2j-2\tau}}.$$

Aquí el módulo es divisible por p^{j+1}, ya que $2j - 2\tau = j + (j - 2\tau) \geq j + 1$. Entonces

$$f(a + tp^{j-\tau}) \equiv f(a) + tp^{j-\tau} f'(a) \pmod{p^{j+1}}.$$

Como ambos términos del lado derecho son divisibles por p^j, el lado izquierdo también lo es. Además, al dividir la congruencia entre p^j, encontramos que

$$\frac{f(a + tp^{j-\tau})}{p^j} \equiv \frac{f(a)}{p^j} + t\,\frac{p^{j-\tau} f'(a)}{p^j} \pmod{p},$$

y el coeficiente de t es primo relativo con p, de modo que hay un único $t \pmod{p}$ para el cual el lado derecho es divisible por p. Esto establece la afirmación final del teorema. Para completar la prueba, observe que $f'(x)$ es un polinomio con coeficientes enteros, de modo que

$$f'(a + tp^{j-\tau}) \equiv f'(a) \pmod{p^{j-\tau}},$$

para cualquier $t \in \mathbb{Z}$.

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Pero $j-\tau \geq \tau+1$, por lo que esta congruencia se mantiene $\pmod{p^{j+1}}$. Dado que $p^\tau \parallel f'(a)$, concluimos que $p^\tau \parallel f'(a+tp^{j-\tau})$. $\square$

Ejercicio: Discutir las soluciones de la congruencia $x^2 + x + 223 \equiv 0 \pmod{3^j}$.