Boletín de Matemáticas
Vol. XII (1978) págs. 119 - 125

SOBRE UN NUMERO DE SOLUCIONES DE CONGRUENCIAS ALGEBRAICAS

por

Víctor Albis

En el excelente libro de T. Nagell citado en la bibliografía aparece el siguiente resultado:

Teorema 1. (Nagell-Ore) Sea $f(X)$ un polinomio de coeficientes enteros, primitivo y de grado n; entonces la congruencia

$$f(X) \equiv 0 (\text{mód } p^a)$$

tiene a lo más nD^2 raíces, donde D es el discriminante del polinomio ([1] pág. 90).

Sin embargo, cuando se trata de averiguar cotas para el número de soluciones de una congruencia específica, el valor de nD^2 puede ser muy gran de; así, por ejemplo, si $f(X) = X^3 + 3X + 9$, $nD^2 = 3^7.5^2.11^2$ para la congruencia $X^3 + 3X + 9 \equiv 0 \pmod{2^5}$, cuando ésta no posee solución alguna en $\mathbb{Z}/32\mathbb{Z}$. Por esta razón solemos presentar en nuestros cursos de teoría de los números una acotación diferente, bastante elemental, la cual se comporta adecuadamente para valores pequeños de p^{m-1}, además de que es aplicable a polinomios de coeficientes en un anillo finito arbitrario.

Supongamos, pues, que A es un anillo finito, conmutativo con elemento unidad, y sea $\mathfrak{m}$ uno de sus ideales maximales; entonces el epimorfismo canónico $\mu : A \to A/\mathfrak{m}$ puede prolongarse a un epimorfismo $\overline{\mu} : A[X] \to (A/\mathfrak{m})[X]$, como lo indica el siguiente diagrama

$$\begin{array}{ccc} A & \xrightarrow{\mu} & A/\mathfrak{m} \\ \downarrow & & \downarrow \\ A[X] & \xrightarrow{\overline{\mu}} & (A/\mathfrak{m})[X] \end{array}$$

Si $f(X) \in A[X]$ escribimos $\overline{f}(X)$ en vez de $\overline{\mu}(f(X))$. La familia $F_{\mathfrak{m}} \subset A[X]$ consiste de todos los $f(X)$ que cumplen $\overline{f}(X) \neq 0$; es decir,

$$f(X) = \sum_{k=o}^{n} a_k X^k \in F_{\mathfrak{m}} \quad \text{si, y sólo si, algún } a_k \notin \mathfrak{m}.$$

Haremos uso del siguiente resultado

Teorema 2. Sean $f(X) \in A[X]$ y $\beta \in A$ una raíz de $f(X)$. Entonces $f(X) = (X - \beta)\, q(X)$, donde

$q(X) \in A[X]$.

Por otra parte, si $f(X) \in A[X]$, definimos la multiplicidad de la raíz $\beta \in A$ de $f(X)$ como

$$m(\beta) = \text{máx}\,\{m \;;\; (X-\beta)^m q(X) = f(X)\}.$$

Esta definición es conveniente pues, por ejemplo, $f(X) = X^3 - X^2 - X + 1 \in (\mathbb{Z}/8\mathbb{Z})[X]$ admite las dos factorizaciones distintas

$$(X - 1)^2 (X + 1) = (X - 1)(X - 5)(X + 5)$$

en $(\mathbb{Z}/8\mathbb{Z})[X]$.

Establecemos en seguida nuestra acotación:

Teorema 3. Sean A un anillo conmutativo, finito, con elemento unidad, y $\mathfrak{m}$ uno de sus ideales maximales. Si $f(X) \in F_{\mathfrak{m}}$ es un polinomio de grado n, entonces $f(X)$ tiene a lo más $n.N(\mathfrak{m})$ raíces en A, contadas con sus multiplicidades, donde $N(\mathfrak{m})$ es el número de elementos de $\mathfrak{m}$.

Demostración: Sea B el conjunto de todas las soluciones de $f(X) \in F_{\mathfrak{m}}$. Si $\beta \in B$ tiene multiplicidad $m(\beta)$, entonces

$$\overline{f}(X) = (X-\overline{\beta})^{m(\beta)} \overline{q}(X), \text{ donde } \overline{\beta} = \mu(\beta),$$

en virtud del Teorema 2. Esto implica que la multiplicidad de $m(\overline{\beta})$ como raíz de $\overline{f}(X)$, es mayor que $m(\delta)$ para todos los $\delta \in \overline{\beta}$. Sean ,

$A_1,\ldots,A_s$, las clases de A módulo $\mathfrak{m}$, y hagamos $B_i = A_i \cap B$. Es claro ahora que

$$\sum_{\delta\in B} m(\delta) = \sum_{i=1}^{s} \sum_{\delta\in B_i} m(\delta)$$

es el número total de raíces de $f(X)$, contadas con sus multiplicidades. Pero

$$\sum_{i=1}^{s} \sum_{\delta\in B_i} m(\delta) \leqslant \sum_{i=1}^{s} \sum_{\delta\in B_i} m(\overline{\delta}) = \sum_{i=1}^{s} m(\overline{\delta}) \sum_{\delta\in B_i} 1$$

$$\leqslant \sum_{i=1}^{s} m(\overline{\delta}) \sum_{m\in\mathfrak{m}} 1 = N(\mathfrak{m}) \sum_{i=1}^{s} m(\overline{\delta}) \leqslant N(\mathfrak{m}).n$$

Esto termina la demostración del Teorema.

<u>Observación</u>: Si A es un cuerpo, esta acotación es la mejor posible.

Discutamos ahora el caso en que $A = \mathbb{Z}/r\mathbb{Z}$, r es un entero positivo. Si $a \in \mathbb{Z}$, su clase modulo r la designamos por $\mathring{a}$.

<u>Teorema 4</u>. Sea $f(X) = \sum \mathring{a}_k X^k \in (\mathbb{Z}/\mathbb{Z}p^m)[X]$ un polinomio de grado n. Si para algún $k = 0,\ldots,n$, $p \nmid a_k$, entonces $f(X)$ tiene a lo más np^{m-1} raíces en $\mathbb{Z}/\mathbb{Z}p^m$, contadas con sus multiplicidades.

<u>Demostración:</u> El anillo $\mathbb{Z}/\mathbb{Z}p^m$ tiene un único ideal maximal $\mathfrak{m} = \mathbb{Z}p/\mathbb{Z}p^{m-1} = \{\mathring{a} \in \mathbb{Z}/\mathbb{Z}p^m \,;\, p|a\}$,

de modo que $f(X) \in F_{\mathfrak{M}}$ si, y sólo si, $p \nmid a_k$ para algún $k = 0,1,\ldots,n$; por otra parte, es fácil verificar que $\mathfrak{M}$ tiene p^{m-1} elementos. En virtud del Teorema 3, resulta que $f(X)$ tiene a lo más np^{m-1} raíces, contadas con sus multiplicidades.■

Corolario 1. Sean $f(X) \in \mathbb{Z}[X]$ un polinomio primitivo de grado n. Entonces la congruencia $f(X) \equiv 0 \ (\text{mód } p^m)$ tiene a lo más np^{m-1} soluciones incongruentes módulo p^m.

Demostración: Sigue del hecho de que los coeficientes de un polinomio primitivo tienen como máximo común divisor al número uno.

De acuerdo con lo anterior la congruencia $X^3 + 3X + 9 \equiv 0 \ (\text{mód } 2^5)$, mencionada al principio tendría a lo más $3.2^4 = 48$ soluciones en $\mathbb{Z}/32\mathbb{Z}$, acotación que es mucho mejor que la dada por el Teorema de Nagell-Ore. El siguiente resultado ya no produce en general una buena estimación.

Corolario 2. Sea $f(X) \in \mathbb{Z}[X]$ un polinomio primitivo de grado n. Entonces la congruencia $f(X) \equiv 0 \ (\text{mód } r)$, $r = p_1^{m_1} \cdots p_t^{m_t}$, tiene a lo más

$$n\, p_1^{m_1-1}, p_2^{m_2}, \ldots, p_t^{m_t}$$

soluciones incongruentes módulo r.

Demostración; Como $\mathbb{Z}/r\mathbb{Z} = \bigoplus_{i=1}^{t} (\mathbb{Z}/p_i^{m_i}\mathbb{Z})$, y los ideales maximales de $\mathbb{Z}/r\mathbb{Z}$ están dados por

$$\mathcal{M}_i = (\mathbb{Z}/p_1^{m_1}\mathbb{Z})\oplus\ldots\oplus(p_i\mathbb{Z}/p_i^{m_i}\mathbb{Z})\oplus\ldots\oplus(\mathbb{Z}/p_t^{m_t}\mathbb{Z}),$$

$i = 1,\ldots,t$, un polinomio primitivo $f(X) = \sum_{k=1}^{n} a_k X^k \in \mathbb{Z}[X]$, de grado n, es tal que $\sum \mathring{a}_k X^k \in F\mathcal{M}_i$, para todo $i = 1,\ldots,t$. Por lo tanto, la congruencia $f(X) \equiv 0 \pmod{r}$ tiene a lo más $nN(\mathcal{M}_1)$, si $p_1 < p_2 < \ldots < p_t$. Como $N(\mathcal{M}_1) = p_1^{m_1-1} p_2^{m_2} \ldots p_t^{m_t}$, el corolario resulta.

Tendremos resultados parecidos en el caso en que $A = R/\mathcal{Y}^m$, donde R es un anillo de enteros algebraicos y $\mathcal{Y}$ uno de sus ideales primos, reemplazando en los resultados anteriores el primo p por la norma del ideal $\mathcal{Y}$.

A título de ejemplo, mencionaremos que usando el Teorema 3 es posible obtener resultados del tipo siguiente:

Teorema 5: Sean $A = \mathbb{F}_p[T]/(T^m)$ (donde $\mathbb{F}_p$ designa el cuerpo de p elementos, p un número primo) y $f(X) = \sum_{k=o}^{n} a_k X^k \in A[X]$ un polinomio de grado n tal que para algún k, $a_k \not\subset (T)/(T^m)$. Entonces $f(X)$ tiene a lo más np^{m-1} raíces en A. En particular, si $p = 2$ y $m = 3$ un polinomio $f(X) \in A[X]$ tiene a lo más $4n$ raíces en A. Si p es arbitrario y $m = 2$ $f(X)$ tiene a lo más np raíces en A.

***

REFERENCIAS

[1] T. Nagell, Number Theory, 2nd. ed., Chelsea Pub. Co., Nueva York, 1964.

Departamento de Matemáticas y Estadística.
Universidad Nacional de Colombia
Bogotá, D.E., Colombia, S.A.