C.R. Math. Rep. Acad. Sci. Canada - Vol. XIII, No. 6, December 1991 decembre 271

On the number of solutions of polynomial congruences

by C.L. Stewart *, F.R.S.C.

Let f be a polynomial with integer coefficients, degree $r(\geq 2)$ and non-zero discriminant D. Let p be a prime number and let p^l denote the largest power of p which divides D. Assume that p does not divide the content of f. For each positive integer k we denote by $N(k)$ the number of solutions of the congruence

(1) $$f(x) \equiv 0 \pmod{p^k}$$

in congruence classes modulo p^k.

In 1921 Nagell [2] and Ore [3] proved that for all positive integers k,

$$N(k) \leq rp^{2l}.$$

This was improved by Sándor [4] in 1952 to

(2) $$N(k) \leq rp^{l/2}$$

for $k > l$. In 1981 Huxley [1] obtained (2) for all positive integers k. For any real number x let $[x]$ denote the greatest integer less than or equal to x. We have recently shown [5] that

(3) $$N(k) \leq 2p^{[l/2]} + r - 2$$

* Research supported in part by a Killam Research Fellowship and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

for all positive integers k. Estimate (3) is, in general, best possible as the following example shows. Let r be an integer with $r \geq 2$, let p be a prime number with $p > r$ and let m be a positive integer. Put

$$f(x) = (x + p^m)(x + 2p^m)(x + 3)\cdots(x + r).$$

Then l, the p-adic order of the discriminant of f, is $2m$. Let k be an integer with $k > l$. The complete solution of the congruence (1) is given by $x \equiv -p^m \pmod{p^{k-m}}$ or $x \equiv -2p^m \pmod{p^{k-m}}$ or $x \equiv -i \pmod{p^k}$ for $i = 3, \ldots, r$ hence, for this example,

$$N(k) = 2p^m + r - 2 = 2p^{l/2} + r - 2,$$

whenever $k > l$.

Let r, k and l be integers with $r \geq 2$, $k \geq 1$ and $l \geq 0$. Define $T = T(r, k, l)$ by

$$T = \begin{cases} \left[\frac{l}{2}\right] & \text{if } k \geq l, \\ \left[\frac{l}{(j+1)(j+2)} + \left(\frac{j}{j+2}\right) k\right] & \text{if } \frac{l}{j} \geq k \geq \frac{l}{j+1} \text{ for } j = 1, \ldots, r-2, \\ \left[\left(\frac{r-1}{r}\right) k\right] & \text{if } \frac{l}{r-1} \geq k \geq 1, \end{cases}$$

and note that

$$T = \min\left(\left[\left(\frac{r-1}{r}\right)k\right], \min_{j=0,\ldots,r-2}\left(\left[\frac{l}{(j+1)(j+2)} + \left(\frac{j}{j+2}\right)k\right]\right)\right).$$

Theorem *Let f be a polynomial with integer coefficients, degree $r(\geq 2)$ and non-zero discriminant D. Let p be a prime number and let l be the p-adic order of D. Assume that p does not divide the content of f. Let k be a positive integer. There is an integer t with $0 \leq t \leq r$ and there are non-negative integers $b_1, \ldots, b_t$ and $u_1, \ldots, u_t$ such that the complete solution of the congruence (1) is given by the t congruences*

$$x \equiv b_i \pmod{p^{k-u_i}},$$

for $i = 1, \ldots, t$. Further

$$(4) \qquad 0 \le u_i \le T,$$

for $i = 1, \ldots, t$ *and*

$$(5) \qquad u_1 + \cdots + u_t \le \min\left(2\left[\frac{l}{2}\right], r\left[\left(\frac{r-1}{r}\right)k\right]\right).$$

The above result is a special case of Theorem 2 of [5]. Since

$$N(k) = p^{u_1} + p^{u_2} + \cdots + p^{u_t},$$

we may use (4) and (5) to deduce (3) and indeed to sharpen (3) when $k \le l$. For details we refer to Corollary 2 of [5].

References

[1] Huxley, M.N., A note on polynomial congruences. In : Recent progress in analytic number theory, Volume 1, Halberstam, H., Hooley, C. eds., pp. 193-196. London: Academic Press, 1981.

[2] Nagell, T., Généralisation d'un theórème de Tchebicheff. *Journ. de Math.* 8 (1921) 343-356.

[3] Ore, O., Anzahl der Wurzeln höherer Kongruenzen. Norsk Matematisk Tidsskrift, 3 Aagang, Kristiana (1921) 343-356.

[4] Sándor, G., Uber die Anzahl der Lösungen einer Kongruenz. *Acta. Math.*, 87 (1952) 13-17.

[5] Stewart, C.L., On the number of solutions of polynomial congruences and Thue equations, *J. Amer. Math. Soc.*, to appear.

C.L. Stewart
Department of Pure Mathematics
The University of Waterloo
Waterloo, Ontario
Canada
N2L 3G1

Received October 4, 1991