PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 49, Number 1, May 1975

ZEROS OF POLYNOMIALS OVER FINITE PRINCIPAL IDEAL RINGS

MURRAY MARSHALL AND GARRY RAMAGE

ABSTRACT. Let R be a finite commutative ring with identity. For $f \in R[X_1, \cdots, X_n]$ denote by $N(f)$ the number of zeros of f in $R^{(n)}$. For integers $n, d \geq 1$ denote by $A_{n,d}$ the greatest common divisor of the integers $N(f)$; $f \in R[X_1, \cdots, X_n]$, $\deg f = d$. J. Ax has shown that if R is a field, then $A_{n,d} = |R|^{\alpha}$ where α is the integer satisfying $\alpha < n/d \leq \alpha + 1$. In this paper, $A_{n,d}$ is computed in the case that R is a principal ideal ring.

Throughout, let R denote a finite commutative ring with identity, and let $R[X_1, \cdots, X_n]$ denote the ring of polynomials in n variables over R, $n \geq 1$. Let $f \in R[X_1, \cdots, X_n]$. An element $x = (x_1, \cdots, x_n) \in R^{(n)}$ is called a zero of f if $f(x) = 0$. Let $N(f) = N(f, R)$ denote the total number of zeros of f in $R^{(n)}$. Let $A_{n,d} = A_{n,d}(R)$ denote the greatest common divisor of the integers $N(f)$; $f \in R[X_1, \ldots, X_n]$, $\deg f = d$.

Suppose $\deg f = 1$. Then $f = f_0 + f_1$ where $f_0 = f(0)$, and where f_1 is linear when considered as a function from $R^{(n)}$ to R. Thus, either $N(f) = 0$ (if $f_0 \notin \operatorname{Im} f_1$) or $N(f) = |\operatorname{Kern} f_1|$. But $|\operatorname{Kern} f_1| = |R^{(n)}|/|\operatorname{Im} f_1|$. It follows easily from this that $A_{n,1} = |R|^{n-1}$. More generally, Ax [2] has shown that if R is a field, then $A_{n,d} = |R|^{\alpha}$ where α is the integer defined by $\alpha < n/d \leq \alpha + 1$. In this paper, we compute $A_{n,d}$ in case R is a principal ideal ring.

1. First assume R is a local principal ideal ring. Let q denote the order of the residue field of R, and define k by $q^k = |R|$. Assume R is not a field, i.e. that $k \geq 2$. Let π be a prime element of R. The following version of Hensel's lemma is useful:

Lemma. *Suppose* $g(x) = r_0 + r_1 X + \cdots + r_d X^d \in R[X]$ *is such that* $\pi | r_i$, $i = 2, \cdots, d$, $\pi \nmid r_1$. *Then* g *has a unique zero in* R.

Proof. $x_1 = -r_0/r_1$ is the unique zero of g modulo π. By induction, if x_i is the unique zero of g modulo π^i, then $x_{i+1} = x_i - g(x_i)/r_1$ is the unique

Received by the editors July 30, 1973.
AMS (MOS) subject classifications (1970). Primary 12C05, 13F10.

zero of g modulo π^{i+1}. Since $\pi^k = 0$, this implies x_k is the unique zero of g in R.

By this lemma, $A_{n,d} = 1$ for $n = 1$. Hence, we may assume $n, d \geq 2$. The computation of $A_{n,d}$ in this case is covered by the following

Theorem. *Suppose R is a finite local principal ideal ring which is not a field; notations as above. If $n, d \geq 2$, then $A_{n,d} = q^{\beta}$ where β is the integer defined by $\beta < nk/2 \leq \beta + 1$.*

Proof. Let $f \in R[X_1, \cdots, X_n]$, $\deg f = d$. Partition the zeros of f in $R^{(n)}$ into classes by considering two zeros $(x_1, \cdots, x_n)$, $(x_1', \cdots, x_n')$ to be equivalent if $x_i \equiv x_i' \bmod \pi$ for $i = 1, \cdots, n$. We show $q^{\beta} | N(f)$ by showing q^{β} divides the number of zeros in each class. Let $(x_1, \cdots, x_n)$ be a zero of f. Note that $f(x_1 + \pi X_1, \cdots, x_n + \pi X_n)$ is of the form $\pi g_1 + \pi^2 g_2 + \cdots + \pi^d g_d$ where $g_i \in R[X_1, \cdots, X_n]$ is homogeneous of degree i, $i = 1, \cdots, d$. Thus we wish to count the number of zeros of

$$g = g_1 + \pi g_2 + \cdots + \pi^{d-1} g_d$$

in $(R/\pi^{k-1})^{(n)}$.

If $k = 2$, $q^{\beta} | N(g, R/\pi^{k-1})$ by Ax's result since $g = g_1$. If one of the coefficients of g_1 is a unit, we may assume, without loss of generality, that it is the coefficient of X_1. Let $y_2, \cdots, y_n \in R/\pi^{k-1}$ be arbitrary and let $h(X) = g(X, y_2, \cdots, y_n)$. Then by the Lemma, h has a unique zero in R/π^{k-1}. Hence $N(g, R/\pi^{k-1}) = q^{(n-1)(k-1)}$. Thus

$$\begin{aligned} q^{\beta} | N(g, R/\pi^{k-1}) &\Leftrightarrow (n-1)(k-1) \geq \beta \\ &\Leftrightarrow (n-1)(k-1) \geq nk/2 - 1 \\ &\Leftrightarrow (n-2)(k-2) \geq 0 \end{aligned}$$

which is true since $n, k \geq 2$ by assumption.

If, on the other hand, π divides all the coefficients of g_1, write $g_1 = \pi g_1'$, and let

$$g' = g_1' + g_2 + \pi g_3 + \cdots + \pi^{d-2} g_d.$$

Then $N(g, R/\pi^{k-1}) = N(g', R/\pi^{k-2}) q^n$. By induction (or by Ax's result, if $k = 3$), $N(g', R/\pi^{k-2})$ is divisible by q^{γ}, $\gamma < n(k-2)/2 \leq \gamma + 1$. Hence $N(g, R/\pi^{k-1})$ is divisible by $q^{n+\gamma}$. But $n + \gamma = \beta$. Thus $q^{\beta} | N(f)$ for every $f \in R[X_1, \cdots, X_n]$ of degree d, so $q^{\beta} | A_{n,d}$.

We deal with the reverse divisibility in several steps. First note that $A_{n,d}$ is a power of the characteristic of the residue field of R. For example,

consider any polynomial $f \in R[X_1, \cdots, X_n]$ of the form $f = f_0 + f_1 + \pi f_2 + \cdots + \pi f_d$ where f_i is homogeneous of degree i and where at least one of the coefficients of f_1 is a unit. Applying the Lemma as before, f has $q^{(n-1)k}$ zeros, so $A_{n,d} \mid q^{k(n-1)}$.

We now complete the case $d = 2$ by constructing, for each integer $n \geq 2$, a polynomial $f \in R[X_1, \cdots, X_n]$ of degree 2 such that $N(f) \equiv -q^{\beta}$ mod $q^{\beta+1}$. If $n = 2$ take $f = X_1X_2 - 1$. Then $N(f) = q^k - q^{k-1} \equiv -q^{k-1}$ mod q^k. For $n = 2t$, $t \geq 2$ define

$$f = X_1X_{t+1} + X_2X_{t+2} + \cdots + X_tX_{2t}.$$

For $0 < s \leq k$ there are $q^{st} - q^{(s-1)t}$ tuples $(x_1, \cdots, x_t)$ such that $Rx_1 + \cdots + Rx_t = R\pi^{k-s}$, and for each such tuple, the linear function $(y_1, \cdots, y_t) \to x_1y_1 + \cdots + x_ty_t$ maps $R^{(t)}$ onto $R\pi^{k-s}$, so has q^{kt-s} solutions. Thus

$$N(f) = q^{kt} + \sum_{s=1}^{k} (q^{st} - q^{(s-1)t})q^{kt-s}.$$

For $t \geq 2$, this is congruent to $-q^{kt-1}$ modulo q^{kt}.

For $n = 2t + 1$, $t \geq 1$ take

$$f = X_1X_{t+1} + \cdots + X_tX_{2t} + \pi^{\epsilon}X_{2t+1}^2,$$

where $\epsilon = 0$ or 1 according to whether k is even or odd. For $0 < s \leq k$ there are

$$(q^{st} - q^{(s-1)t})q^{(k+\epsilon)/2 + \delta(s)}$$

tuples $(x_1, \cdots, x_t, x)$ satisfying

$$Rx_1 + \cdots + Rx_t = R\pi^{k-s} \supseteq R\pi^{\epsilon}x^2,$$

where $\delta(s)$ is the greatest integer $\leq s/2$. For each such tuple, $x_1y_1 + \cdots + x_ty_t + \pi^{\epsilon}x^2 = 0$ has q^{kt-s} solutions $(y_1, \cdots, y_t)$. Thus

$$N(f) = q^{(k+\epsilon)/2}q^{kt} + \sum_{s=1}^{k} (q^{st} - q^{(s-1)t})q^{(k+\epsilon)/2 + \delta(s)}q^{kt-s}.$$

For $t \geq 1$ this is congruent to $-q^{(k+\epsilon)/2+kt-1}$ modulo $q^{(k+\epsilon)/2+kt}$.

To handle the case $d \geq 3$ write $d = 2r + s$ where $s = 0$ or 1 and define

$$g(X_1, \cdots, X_n) = f(X_1, \cdots, X_n) + \pi^{k-1}f(X_1, \cdots, X_n)^rX_1^s,$$

where f is the polynomial of degree two constructed in the previous step. Then g has the same zeros as f, and g has degree d, so the proof is complete.

Remark. Let R be a local principal ideal ring. It follows from the above formulae for $A_{n,d}$ (or from Ax's formula if $k = 1$) that $A_{n,d} | A_{n,d'}$ if $d \geq d'$. We will see later that this holds even when R is not local.

2. Now let R be any finite commutative principal ideal ring with identity. Then R decomposes canonically as $R = R_1 \oplus \cdots \oplus R_s$ where the R_i are local principal ideal rings [1, p. 90]. This decomposition induces a natural isomorphism

$$R[X_1, \cdots, X_n] \cong \bigoplus_{i=1}^{s} R_i[X_1, \cdots, X_n],$$

and if $f \in R[X_1, \cdots, X_n]$ decomposes as $(f_1, \cdots, f_s)$ under this isomorphism, then $\deg f = \max\{\deg f_i\colon\ i = 1, \cdots, s\}$ and $N(f, R) = \prod_{i=1}^{s} N(f_i, R_i)$. It follows from this, together with the remark, that

$$A_{n,d}(R) = \prod_{i=1}^{s} A_{n,d}(R_i).$$

This completes the computation of $A_{n,d}$ for R any finite commutative principal ideal ring with identity.

REFERENCES

1. M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969. MR 39 #4129.

2. J. Ax, *Zeroes of polynomials over finite fields*, Amer. J. Math. 86 (1964), 255–261. MR 28 #3986.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SASKATCHEWAN, SASKATOON, CANADA S7N 0W0