POWER ROOTS OF POLYNOMIALS OVER ARBITRARY FIELDS

VINCENZO ACCIARO

Let F be an arbitrary field, and $f(x)$ a polynomial in one variable over F of degree $\geqslant 1$. Given a polynomial $g(x) \neq 0$ over F and an integer $m > 1$ we give necessary and sufficient conditions for the existence of a polynomial $z(x) \in F[x]$ such that $z(x)^m \equiv g(x) \pmod{f(x)}$. We show how our results can be specialised to $\mathbb{R}$, $\mathbb{C}$ and to finite fields. Since our proofs are constructive it is possible to translate them into an effective algorithm when F is a computable field (for example, a finite field or an algebraic number field).

1. INTRODUCTION

Let F be an arbitrary field, of characteristic $char(F)$, $f(x)$ a polynomial in one variable over F of degree $\geqslant 1$, $g(x)$ a nonzero polynomial over F and $m > 1$ an integer.

In [3] Miller gave some sufficient conditions for the existence of a polynomial $z(x) \in F[x]$ such that $z(x)^m \equiv g(x) \pmod{f(x)}$, when F is $\mathbb{R}$ or $\mathbb{C}$ – it is explicitly stated in his paper that the conditions given are not necessary.

In our paper we extend Miller's results by giving necessary and sufficient conditions for the existence of an m^{th} root in $F[x]/(f(x))$, when F is any field, not necessarily $\mathbb{C}$ or $\mathbb{R}$. While the methods used by Miller in [3] are analytical, ours are purely algebraic.

Moreover, since all the proofs given here are constructive, it is possible to translate them into an effective algorithm when F is a computable field (for example, an algebraic number field or a finite field).

When $char(F) \not| m$, we can summarise the results of this paper in the following theorem:

THEOREM 1. *Let F be a field, and $m > 1$ a positive integer, $char(F) \not| m$ if $char(F) > 0$. Let $g(x), f(x)$ be polynomials over F, with $g(x) \neq 0$ and $\deg f(x) \geqslant 1$. In $F[x]$ the congruence*

$$(1) \qquad z(x)^m \equiv g(x) \pmod{f(x)}$$

Received 30th December, 1993.
The author wishes to thank Professor J.D. Dixon for his invaluable and extremely helpful comments.

https://doi.org/10.1017/S0004972700013782 Published online by Cambridge University Press

admits a solution if and only if for every irreducible factor $p(x)$ of $f(x)$: if $l \geqslant 0$ denotes the highest exponent to which $p(x)$ divides $g(x)$ and $k \geqslant 1$ denotes the highest exponent to which $p(x)$ divides $f(x)$, then either

(i) $k \leqslant l$, *or*

(ii) $m \mid l$ *and* $y(x)^m \equiv g(x)/p(x)^l \pmod{p(x)}$ *is solvable for* $y(x)$.

When $char(F) \mid m$ the conditions for the solvability of the congruences $z_i(x)^m \equiv g(x) \left(\bmod p_i(x)^{k_i}\right)$ are more involved – we shall consider the case $char(F) \mid m$ in Section 2.2.

What this paper essentially shows is that we can reduce the problem of solving (1) to the problem of solving simpler equations, of the form $z(m)^m \equiv g(x) \pmod{p(x)}$, with $p(x)$ irreducible over F. But, as we shall show in Section 2, solving these simpler congruences is equivalent to extracting m^{th} roots in some algebraic extension of F.

We shall prove Theorem 1 in Section 2. In Sections 3, 4 and 5 we shall show how to specialise Theorem 1 to $\mathbb{C}$, $\mathbb{R}$ and to finite fields.

2. The method

We can assume without loss of generality that $f(x)$ is monic, since if $z(x)^m \equiv g(x) \pmod{f(x)}$ holds, then $z(x)^m \equiv g(x) \pmod{cf(x)}$ holds for any $c \in F$. The method discussed in this paper can be summarised as follows:

(i) Factor $f(x)$ into monic irreducibles obtaining $f(x) = p_1(x)^{k_1} \dots p_n(x)^{k_n}$ where the $p_i(x)$ are distinct irreducibles and each $k_i \geqslant 1$;

(ii) Solve each of the congruences $z_i(x)^m \equiv g(x) \pmod{p_i(x)}$ for $z_i(x)$, $i \in \{1, \dots, n\}$;

(iii) Lift the solutions obtained in the previous step from $F[x]/(p_i(x))$ to $F[x]/\left(p_i(x)^{k_i}\right)$;

(iv) Combine the solutions of the previous step using the Chinese Remainder Theorem to obtain a solution of the original congruence.

Step (iv) does not present any technical difficulty, since it relies on the well known isomorphism [4, p.95]:

$$F[x]/(f(x)) \cong F[x]/\left(p_1(x)^{k_1}\right) \times \dots \times F[x]/\left(p_n(x)^{k_n}\right).$$

When $p(x)$ is a monic irreducible polynomial $F[x]/(p(x)) \cong F(\alpha)$ where α is any root of $p(x)$: the actual isomorphism is given by $k(x) + (p(x)) \mapsto k(\alpha)$. It follows that Step (ii), that is the extraction of an m^{th} root of $g(x)$ modulo $p(x)$, is equivalent to the extraction of an m^{th} root of $g(\alpha)$ in $F(\alpha)$.

https://doi.org/10.1017/S0004972700013782 Published online by Cambridge University Press

Therefore, most of the rest of this section will be devoted to explaining how Step (iii), that is, the lifting process, can be accomplished.

Fundamental to the entire process is the concept of the $p(x)$-adic expansion of a polynomial $f(x)$ [4, p.189]. Given $f(x), p(x) \in F[x]$, with $\deg p(x) \geqslant 1$, there exist unique polynomials $g_0(x), g_1(x), \dots, g_t(x) \in F[x]$ such that $\deg g_i(x) < \deg p(x)$ and $f(x) = g_0(x) + g_1(x)p(x) + g_2(x)p(x)^2 + \dots + g_t(x)p(x)^t$. The polynomials $g_i(x)$ can be computed recursively as follows:

- $g_0(x) := f(x) \bmod p(x)$
- $g_{i+1}(x) := \left(f(x) - \sum\limits_{k=0}^{i} g_k(x)p(x)^k\right)/p(x)^{i+1} \bmod p(x)$.

The lifting method is based on the following lemma, freely adapted from the proof of Hensel's lemma in [2, p.16].

Lemma 1. *Let $p(x)$ be an irreducible element of $F[x]$. Let $G(y)$ be a polynomial with coefficients in $F[x]$. Assume that there is an element $f_0(x) \in F[x]$, with $\deg f_0(x) < \deg p(x)$, such that $G(f_0(x)) \equiv 0 \pmod{p(x)}$ and $G'(f_0(x)) \not\equiv 0 \pmod{p(x)}$. Given any positive integer k there is a unique polynomial $f_{k-1}(x) \in F[x]$ of degree less than $\deg p(x)^k$ such that $G(f_{k-1}(x)) \equiv 0 \left(\bmod\, p(x)^k\right)$ and $f_{k-1}(x) \equiv f_0(x) \pmod{p(x)}$.*

Proof: We show how to construct a sequence of polynomials $f_1(x), \dots f_{k-1}(x) \in F[x]$ such that for all $n \in \{1, \dots, k-1\}$:

(i) $G(f_n(x)) \equiv 0 \left(\bmod\, p(x)^{n+1}\right)$
(ii) $f_n(x) \equiv f_{n-1}(x) \pmod{p(x)^n}$
(iii) $\deg f_n(x) < \deg p(x)^{n+1}$.

We prove that the sequence $(f_n(x))$ exists and is unique by induction on n. If $f_1(x)$ satisfies (ii) and (iii) then it must be of the form $f_0(x) + b_1(x)p(x)$, with $\deg b_1(x) < \deg p(x)$. When we expand $G(f_1(x))$ we obtain

$$G(f_1(x)) = G(f_0(x) + b_1(x)p(x)) = G(f_0(x)) + G'(f_0(x))b_1(x)p(x) + w(x)$$

where $w(x)$ is a polynomial divisible by $p(x)^2$.

Since $p(x) \mid G(f_0(x))$ by assumption, we can write $G(f_0(x)) \equiv a_0(x)p(x) \left(\bmod\, p(x)^2\right)$ where $\deg a_0(x) < \deg p(x)$. So, in order to get $G(f_1(x)) \equiv 0 \left(\bmod\, p(x)^2\right)$ we must have $a_0(x)p(x) + G'(f_0(x))b_1(x)p(x) \equiv 0 \left(\bmod\, p(x)^2\right)$, that is, $a_0(x) + G'(f_0(x))b_1(x) \equiv 0 \pmod{p(x)}$. The last congruence has a unique solution (mod $p(x)$) for $b_1(x)$ since by hypothesis $G'(f_0(x)) \not\equiv 0 \pmod{p(x)}$. Then $f_1(x) = f_0(x) + b_1(x)p(x)$ is the unique polynomial satisfying (i), (ii) and (iii) with $n = 1$.

https://doi.org/10.1017/S0004972700013782 Published online by Cambridge University Press

Next, assume that $f_1(x), f_2(x), \ldots, f_{n-1}(x)$ are known, and we want to find $f_n(x)$. By (ii) and (iii) we need $f_n(x) = f_{n-1}(x) + b_n(x)p(x)^n$ with $\deg b_n(x) < \deg p(x)$. We expand $G(f_n(x))$ obtaining

$$\begin{aligned} G(f_n(x)) &= G(f_{n-1}(x) + b_n(x)p(x)^n) \\ &\equiv G(f_{n-1}(x)) + G'(f_{n-1}(x))b_n(x)p(x)^n \pmod{p(x)^{n+1}}. \end{aligned}$$

Since $G(f_{n-1}(x)) \equiv 0 \pmod{p(x)^n}$ by the inductive hypothesis, we obtain

$$G(f_{n-1}(x)) \equiv a_{n-1}(x)p(x)^n \pmod{p(x)^{n+1}}$$

and the condition $G(f_n(x)) \equiv 0 \pmod{p(x)^{n+1}}$ becomes

$$a_{n-1}(x)p(x)^n + G'(f_{n-1}(x))b_n(x)p(x)^n \equiv 0 \pmod{p(x)^{n+1}},$$

that is

$$a_{n-1}(x) + G'(f_{n-1}(x))b_n(x) \equiv 0 \pmod{p(x)}.$$

Since $f_{n-1}(x) \equiv f_0(x) \pmod{p(x)}$ it follows that

$$G'(f_{n-1}(x)) \equiv G'(f_0(x)) \not\equiv 0 \pmod{p(x)}$$

and so the previous congruence has a unique solution $\pmod{p(x)}$ for $b_n(x)$. Then $f_n(x) = f_{n-1}(x) + b_n(x)p(x)^n$ is the unique polynomial satisfying (i), (ii) and (iii). □

Our objective is to solve the congruence:

$$y(x)^m \equiv g(x) \pmod{p(x)^k} \tag{2}$$

where $p(x)$ is a monic irreducible factor of $f(x)$.

Let $y_0(x)$ be a solution of $y(x)^m \equiv g(x) \pmod{p(x)}$; clearly if such an element $y_0(x)$ does not exist (2) cannot admit any solution.

If $my_0(x)^{m-1} \not\equiv 0 \pmod{p(x)}$ we can use the construction given in Lemma 1 with $G(y) := y(x)^m - g(x)$ to obtain a sequence of polynomials $y_1(x)$, $y_2(x)$, $\ldots$ such that $y_i(x)^m \equiv g(x) \pmod{p(x)^{i+1}}$. A solution of (2) is then given by $y_{k-1}(x)$, and this solution is unique, modulo $p(x)^k$.

If $my_0(x)^{m-1} \equiv 0 \pmod{p(x)}$ the lifting argument can not be applied, although (2) may still have a solution.

Let us assume therefore that $my_0(x)^{m-1} \equiv 0 \pmod{p(x)}$. Since $F[x]/(p(x))$ is a field this may happen only in two cases: if $y_0(x) \equiv 0 \pmod{p(x)}$ or if $char(F) \mid m$. We discuss the first case in Section 2.1 and the second case in Section 2.2.

https://doi.org/10.1017/S0004972700013782 Published online by Cambridge University Press

REMARK. Let s_i denote the number of solutions of the congruence $z_i(x) \equiv g(x)$ $\left(\bmod\, p_i(x)^{k_i}\right)$. It is easy to see that the number of solution of (1) is given by $\Pi_{i=1}^{n} s_i$. In the case when $GCD(f(x), g(x)) = 1$ and $char(F) \nmid m$, Lemma 1 shows that the lifting process is unique and so s_i is also the number of m^{th} roots of $g(x)$ $(\bmod\, p_i(x))$.

2.1 LIFTING OF ZERO.

It is easy to see that the zero polynomial is a solution of $y(x)^m \equiv g(x)$ $(\bmod\, p(x))$ if and only if $p(x) \mid g(x)$. The following lemma deals with this case.

LEMMA 2. *Assume that $p(x) \mid g(x)$. Let l be the highest exponent to which $p(x)$ divides $g(x)$. If $k \leqslant l$ the zero polynomial is a solution of (2). If $k > l$ then (2) admits a solution if and only if $m \mid l$ and*

$$y(x)^m \equiv g(x)/p(x)^l \quad \left(\bmod\, p(x)^{k-l}\right) \tag{3}$$

admits a solution. In this case if $\widehat{y}(x)$ denotes a solution of (3) then $\widehat{y}(x)p(x)^{l/m}$ is a solution of (2).

PROOF: If $k \leqslant l$ the zero polynomial is obviously a solution of (2), so we shall suppose that $k > l$.

Assume that $\widehat{y}(x)^m \equiv g(x)/p(x)^l$ $\left(\bmod\, p(x)^{k-l}\right)$. This is equivalent to $p(x)^k \mid \widehat{y}(x)^m p(x)^l - g(x)$. Thus, if $m \mid l$ we can write the last relation as $p(x)^k \mid \widehat{y}(x)^m p(x)^{(l/m)m} - g(x)$, and so $\widehat{y}(x)p(x)^{l/m}$ is a solution of (2).

On the other hand, suppose that $k > l$ and (2) admits a solution. Let the $p(x)$-adic expansion of $g(x)$ be $a_1(x)p(x)^l + a_2(x)p(x)^{l+1} + \ldots$, with $a_1(x) \neq 0$. Let $\overline{y}(x) = b_1(x)p(x)^r + \ldots$ be a solution of (2), with $b_1(x) \neq 0$. Then the $p(x)$-adic expansion of $\overline{y}(x)^m$ is $(b_1(x)^m \bmod p(x))p(x)^{rm} + \ldots$.

Since $b_1(x) \neq 0$ and $\deg b_1(x) < \deg p(x)$ it follows that $b_1(x) \not\equiv 0$ $(\bmod\, p(x))$ and therefore $b_1(x)^m \not\equiv 0$ $(\bmod\, p(x))$, since $p(x)$ is prime. Now $\overline{y}(x)^m \equiv g(x)$ $\left(\bmod\, p(x)^k\right)$ if and only if $(b_1(x)^m \bmod p(x))p(x)^{rm} + \ldots$ and $a_1(x)p(x)^l + \ldots$ coincide up to the term in $p(x)^{k-1}$. Since $a_1(x) \neq 0$ and $b_1(x)^m \bmod p(x) \neq 0$ it follows that $l = rm$ and so $m \mid l$ as asserted. □

COROLLARY 1. *Under the assumptions of the previous lemma, if $char(F) \nmid m$ and $k > l$ then (2) admits a solution if and only if $m \mid l$ and $y(x)^m \equiv g(x)/p(x)^l$ $(\bmod\, p(x))$ admits a solution.*

PROOF: The Corollary follows immediately from Lemma 2 since the right hand side of (3) is not divisible by $p(x)$. □

Note that if $p(x) \mid g(x)$ and at the same time $char(F) \mid m$, we can use Lemma 2 to reduce this case to the case $p(x) \nmid g(x)$ and $char(F) \mid m$, which is handled in the next section.

2.2 The exponent m is a multiple of $char(F)$.

In this section we shall assume that $p(x) \not| g(x)$. When $q = char(F) > 0$ the map $a \mapsto a^q$ is always an endomorphism of F. It follows that if $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ is a polynomial over F then $a(x)^q = a_0^q + a_1^q x^q + \ldots + a_n^q x^{nq}$. We shall use this fact frequently in this section.

Lemma 3. *Let $q = char(F)$, $q \neq 0$. Assume that $m = q^t$ for some positive integer t, and $m \geqslant k$. If (2) admits a solution, then every solution of $y(x)^m \equiv g(x)$ $(\bmod\ p(x))$ is a solution of (2).*

Proof: Let us assume that (2) admits a solution $y_1(x)$. Let $y_0(x)$ be a solution of $y(x)^m \equiv g(x)$ $(\bmod\ p(x))$. Then $(y_0(x) - y_1(x))^m = y_0(x)^m - y_1(x)^m \equiv 0$ $(\bmod\ p(x))$. Since $p(x)$ is prime and $k \leqslant m$ it follows that $p(x)^k \mid (y_0(x) - y_1(x))^m$ and therefore $y_0(x)^m \equiv y_1(x)^m \left(\bmod\ p(x)^k\right)$, that is, $y_0(x)^m \equiv g(x) \left(\bmod\ p(x)^k\right)$. □

Note. Therefore, when $m = q^t$ and $m \geqslant k$, to test if (2) is solvable, it is enough to find *any* solution of $y(x)^m \equiv g(x)$ $(\bmod\, p(x))$ and check if it satisfies (2). Clearly if $y(x)^m \equiv g(x)$ $(\bmod\, p(x))$ does not admit any solution then (2) does not admit any solution.

Lemma 4. *Let $q = char(F)$, $q \neq 0$. Assume that $m = q^t$ for some positive integer t.*

If $m \mid k$ then (2) admits a solution if and only if $g(x)$ $\left(\bmod\ p(x)^k\right)$ is a polynomial in x^m and all its coefficients have an m^{th} root in F.

If $m \not| k$ let $w := \lfloor k/m \rfloor$, let $s := k \bmod m$, let $z(x) := g(x) \bmod p(x)^{mw}$ and $r(x) := (g(x) - z(x))/(p(x)^{mw}) \bmod p(x)^s$. Then (2) admits a solution if and only if $z(x)$ is a polynomial in x^m, all its coefficients have an m^{th} root in F and $j(x)^m \equiv r(x)$ $(\bmod\ p(x)^s)$ admits a solution.

Proof: Let $g_0(x) + g_1(x)p(x)^m + \ldots$ be the $p(x)^m$-adic expansion of $g(x)$.

If $y(x)$ is an m^{th} root of $g(x)$ modulo $p(x)^k$ and $y_0(x) + y_1(x)p(x) + \ldots$ is its $p(x)$-adic expansion then $y(x)^m = y_0(x)^m + y_1(x)^m p(x)^m + \ldots$ and this expression must coincide with the $p(x)^m$-adic expansion of $y(x)^m$.

Let us assume first that $m \mid k$. It can be seen that in this case (2) is satisfied if and only if

$$y_0(x)^m + y_1(x)^m p(x)^m + \ldots + y_{k/m-1}(x)^m p(x)^{m(k/m-1)}$$
$$= g_0(x) + g_1(x)p(x)^m + \ldots + g_{k/m-1}(x)p(x)^{m(k/m-1)}.$$

Therefore $g_i(x)$ must be the m^{th} power of $y_i(x)$, for $i = 0, \ldots, k/m - 1$. But then $g(x) \bmod p(x)^k$ is the m^{th} power of a polynomial $y(x)$, that is, it must be a polynomial in x^m and each of its coefficients must have an m^{th} root in F — it is easy at this point to find the actual polynomial $y(x)$.

Assume next that $m \nmid k$. The argument used above tells us that $g_i(x) = y_i(x)^m$ for $i = 0, \dots, \lfloor k/m \rfloor - 1$, and $g_i(x) \equiv y_i(x)^m \pmod{p(x)^s}$ for $i = \lfloor k/m \rfloor$, as asserted. Since $s < m$, the last congruence can be handled using Lemma 3. $\square$

Note that Lemma 3 and Lemma 4 are valid for any field of characteristic $q > 0$. When the map $a \mapsto a^q$ is an automorphism of F (that is, if F is a perfect field) we can say much more, as the next theorem shows.

THEOREM 2. *Let F be a perfect field of characteristic q. Assume that $m = q^t$ for some integer t. Then (2) admits a solution for any $k \geqslant 1$.*

PROOF: When F is perfect the map $a \mapsto a^q$ is an automorphism of any finite extension of F, and so is the map $a \mapsto a^m$ since m is a power of q.

Let A be the F-algebra $F[x]/\left(p(x)^k\right)$. This algebra is clearly finite dimensional over F.

As a consequence of Nakayama's lemma (see [6, Section 4.2]) the endomorphism $a \mapsto a^m$ of A is onto if and only if the induced endomorphism of $A/rad(A)$ given by $a + rad(A) \mapsto a^m + rad(A)$ is onto.

But $A/rad(A) \cong F[x]/(p(x))$ and by what we have just said the induced map $a + (p(x)) \mapsto a^m + (p(x))$ is surjective.

Therefore (2) admits a solution for any $k \geqslant 1$. $\square$

REMARK. When $q \mid m$ but m is not a power of q, write m as $q^t r$, with $q \nmid r$. Write (2) as $\left(y(x)^{q^t}\right)^r \equiv g(x) \left(\operatorname{mod} p(x)^k\right)$.

Set $z(x) := y^{q^t}$ and solve $z(x)^r \equiv g(x) \left(\operatorname{mod} p(x)^k\right)$ for $z(x)$. Finally solve $y(x)^{q^t} \equiv z(x) \left(\operatorname{mod} p(x)^k\right)$ for $y(x)$ to obtain a solution of (2).

3. The complex case

In $\mathbb{C}[x]$ an irreducible polynomial $p(x)$ can have only degree 1, and therefore we can take $p(x) = x - \alpha$, with $\alpha \in \mathbb{C}$. We recall here that $\mathbb{C}[x]/(x - \alpha) \cong \mathbb{C}$ under the isomorphism $g(x) + (x - \alpha) \mapsto g(\alpha)$.

If $p(x) \nmid g(x)$, the congruence $y(x)^m \equiv g(x) \pmod{p(x)}$ always admits a (nonzero) solution, since $\mathbb{C} \cong \mathbb{C}[x]/p(x)$ is algebraically closed, and this solution can be lifted to a solution modulo $p(x)^k$, since m doesn't divide the characteristic of $\mathbb{C}$.

If $g(x) \equiv 0 \pmod{p(x)}$ then (2) admits a solution if and only if the conditions imposed by Lemma 2 are satisfied. We summarise our results in the following theorem:

Theorem 3. *In $\mathbb{C}[x]$ the congruence (1) admits a solution if and only if for every common root α of $f(x)$ and $g(x)$ either the multiplicity of α in $g(x)$ is greater than or equal to the multiplicity of α in $f(x)$ or else m divides the multiplicity of α in $g(x)$.*

4. The real case

In $\mathbb{R}[x]$ an irreducible polynomial $p(x)$ can have only degree 1 or 2. Assume first that $p(x) \not| g(x)$.

If $\deg p(x) = 1$, then we can take $p(x) = x - \alpha$, with $\alpha \in \mathbb{R}$; then $\mathbb{R}[x]/(p(x)) \cong \mathbb{R}$ under the isomorphism $g(x) + (p(x)) \mapsto g(\alpha)$. Then $y(x)^m \equiv g(x) \pmod{p(x)}$ admits a solution unless $g(\alpha) < 0$ and m is even. Moreover this solution can always be lifted to a solution modulo $p(x)^k$.

If $\deg p(x) = 2$, then $\mathbb{R}[x]/(p(x)) \cong \mathbb{C}$. In this case $y(x)^m \equiv g(x) \pmod{p(x)}$ admits a nonzero solution and this solution can be lifted to a solution modulo $p(x)^k$.

Assume next that $p(x) \mid g(x)$. If $\deg p(x)$ is 1 or 2 then (2) admits a solution if and only if the conditions imposed by Lemma 2 are satisfied. We summarise our results in the following theorem:

Theorem 4. *In $\mathbb{R}[x]$ the congruence (1) admits a solution if and only if the following holds for every (real or complex) root α of $f(x)$: if l denotes the multiplicity of α in $g(x)$ and k the multiplicity of α in $f(x)$, then either*

(i) $k \leqslant l$, *or*

(ii) $m \mid l$, *and whenever α is real either $\left(g/p^l\right)(\alpha) > 0$ or else m is odd.*

5. Finite fields

When K is a finite field there is an easy criterion to decide if an element a has an m^{th} root in it, namely let $e := (|K| - 1)/(m, |K| - 1)$ and test if a^e is equal to 1 or not: in the first case a has exactly $(m, |K| - 1)$ roots in the field, in the second case it has no roots. We summarise our results in the following theorem:

Theorem 5. *Let F be a finite field of characteristic q. Write m as $q^t r$ with $q \not| r$. In $F[x]$ the congruence (1) admits a solution if and only if the following holds for every irreducible factor $p(x)$ of $f(x)$: if $d := \deg p(x)$, $e := \left(|F|^d - 1\right)/\left(r, |F|^d - 1\right)$, l is equal to the highest exponent to which $p(x)$ divides $g(x)$ and k is equal to the highest exponent to which $p(x)$ divides $f(x)$, then either*

(i) $k \leqslant l$, *or*

(ii) $m \mid l$ *and* $\left(g(x)/p(x)^l\right)^e \equiv 1 \pmod{p(x)}$.

We would like to add the fact that when F is a finite field there are very efficient algorithms for factoring polynomials over F [1, 5], for computing the roots of polynomials over F [7, 5] and for taking m^{th} roots of elements of F [8].

https://doi.org/10.1017/S0004972700013782 Published online by Cambridge University Press

References

[1] E.R. Berlekamp, 'Factoring polynomials over large finite fields', *Math. Comp.* **24** (1970), 713–735.

[2] N. Koblitz, *p-adic numbers, p-adic analysis and zeta functions*, (second edition) (Springer-Verlag, Berlin, Heidelberg, New York, 1984).

[3] J.B. Miller, 'Power roots of polynomials', *Bull. Austral. Math. Soc. Vol.* **47** (1993), 163–168.

[4] S. Lang, *Algebra*, (third edition) (Addison-Wesley, Reading, Mass., 1993).

[5] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Math. and its Applications 20, (Addison-Wesley, Reading, Mass., 1983).

[6] R.S. Pierce, *Associative algebras* (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

[7] M.O. Rabin, 'Probabilistic algorithms in finite fields', *SIAM J. Comput.* **9** (1980), 273–280.

[8] K.S. Williams and K. Hardy, 'A refinement of H.C. Williams' q-th root algorithm', *Math. Comput.* **61** (1993), 475–483.

School of Computer Science
Carelton University
Ottawa, Ontario K1S 5B6
Canada