An Algorithm for Solving a Polynomic Congruence, and its Application to Error-Correcting Codes

By M. H. McAndrew

1. Introduction. The solution of $f(x) = 0$ in the p-adic field may be calculated by the Newton-Raphson process, the iteration of the transformation: $x \to x - f(x)/f'(x)$; as in the real field the formula cannot be applied successfully unless we have an initial approximation sufficiently close to a root for the subsequent iteration to converge. (In the p-adic field, "sufficiently close" is equivalent to "congruent to a sufficiently high power of p.") In this paper we deduce a simple criterion to ensure that the initial approximation is suitable and we develop a procedure for calculating the roots of $f(x) \equiv 0 \pmod{p^k}$ for any value of k, using the above process where applicable and a single-stepping procedure elsewhere. In §6 we apply this algorithm to investigate solutions of a congruence connected with the existence of close-packed error-correcting binary codes. We deduce that for $n < 2^{70}$ and $2 \leqq r \leqq 20$ there are no such codes other than the trivial codes and the Golay code. This result complements results of Shapiro and Slotnick [5] and Selfridge [4] which show that there are no codes for $r = 2$, or r an odd integer less than 135, or $n < 10^8$.

2. Notation. p is a prime and $f(x)$ a polynomial with integer coefficients; $f'(x)$ is the formal derivative of $f(x)$. We use the notation $p^a \| B$ for "$p^a \mid B$ and $p^{a+1} \nmid B$." Define $l(x)$ by $p^l \| f'(x)$. Define

$$b(m, x) = \text{Max}\left\{\left[\frac{m+1}{2}\right], m - l(x)\right\}.$$

We write $l, l_1, l_2, \cdots$ for $l(x), l(x_1), l(x_2), \cdots$; similarly, for $b, b_1, b_2, \cdots$ where the relevant value of m is clear from the context. We say x is a *solution of type* A mod p^m if

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

and $m \geqq 2l + 1$. We say x is a *solution of type* B mod p^m if (1) holds and $m \leqq 2l$.

3. Properties of Solution-Sets.

Lemma 1. (i) *If x is a solution of type* A mod p^m, *then $b = m - l$ and $2b \geqq m + 1 \geqq 2l + 2$.*

(ii) *If x is a solution of type* B mod p^m *then $b = [(m + 1)/2]$ and $b \leqq l$.*

Proof. These results follow directly from the definition of solution type.

Lemma 2. *If $f(x) \equiv 0 \pmod{p^m}$ and $x_1 \equiv x \pmod{p^b}$, then*

(i) *x_1 is a solution* mod p^m *of the same type as x.*

(ii) $b_1 = b$.

(iii) *If x is of type* A mod p^m *then $l_1 = l$.*

Proof. By hypothesis, $x_1 = x + up^b$ for integral u; hence,

$$f(x_1) = f(x) + up^b f'(x) + vp^{2b}, \tag{2}$$

Received September 30, 1963. Revised June 24, 1964.

$$(3) \qquad f'(x_1) = f'(x_1) + wp^b,$$

for integral v and w, by Taylor's theorem for polynomials. Now $p^m \mid f(x)$ and, by definition of $b, b + l \geqq m$ and $2b \geqq m$; hence in (2)

$$(4) \qquad f(x_1) \equiv 0 \pmod{p^m}.$$

To complete the proof we distinguish two cases.

(a) If x is a solution of type A mod p^m then, by Lemma 1 (i), $b \geqq l + 1$; hence, in (3), $p^l \parallel f'(x_1)$, i.e., $l_1 = l$. Therefore $2l_1 + 1 = 2l + 1 \leqq m$, x_1 is a solution of type A mod p^m, and $b_1 = m - l_1 = m - l = b$.

(b) If x is a solution of type B mod p^m then, by Lemma 1 (ii), $b \leqq l$; hence, in (3), $l_1 \geqq b = [(m + 1)/2]$, i.e., $2l_1 \geqq m$. Hence x_1 is a solution of type B mod p^m and $b_1 = [(m + 1)/2] = b$, by Lemma 1 (ii).

This concludes the proof of Lemma 2.

In view of Lemma 2, we define a *solution-set* mod p^m as the set of all x_1 with $x_1 \equiv x \pmod{p^b}$, where x is a solution of (1) and $b = b(m, x)$. We use the notation (x, b, m) for such a solution-set and say x is a *representative* of it. By Lemma 2 (ii), the value of b is independent of the choice of representative and, by Lemma 2 (i), we may define unambiguously the type of a solution-set as the type of any representative. Let $S(m)$ be the totality of solution-sets mod p^m.

We define an *extension to* mod p^{m+r} of the solution-set (x, b, m) as a solution-set $(x_1, b_1, m + r)$ with $x_1 \equiv x \pmod{p^b}$. Clearly $S(m + r)$ consists of just all extensions to mod p^{m+r} of the solution-sets of $S(m)$.

THEOREM 1. (i) *If (x, b, m) is a solution-set of type* A, *then it has a unique extension, $(x_1, b_1, m + 1)$ to* mod p^{m+1}; *this extension is also of type* A *with $l_1 = l$ and $b_1 = b + 1$.*

(ii) *If (x, b, m) is a solution-set of type* B, *then* (a) *if m is odd either $(x, b, m + 1)$ is the unique extension of (x, b, m) to* mod p^{m+1} or there is no extension to mod p^{m+1}; (b) *if m is even, the extensions to* mod p^{m+1} *are just those $(x + sp^b, b + 1, m + 1)$ for which $0 \leqq s < p$ and $f(x + sp^b) \equiv 0 \pmod{p^{m+1}}$.*

Proof. For any integral s,

$$(5) \qquad f(x + sp^b) = f(x) + sp^bf'(x) + vp^{2b},$$

for integral v.

(i) If x is a solution of type A then, by Lemma 1 (i), $b = m - l$ and $2b \geqq m + 1$; hence, from (5), $f(x + sp^b) \equiv 0 \pmod{p^{m+1}}$ if and only if

$$(6) \qquad p^{-m}f(x) + sp^{-l}f'(x) \equiv 0 \pmod{p}.$$

Since $p \nmid p^{-l}f'(x)$, (6) has a unique solution mod p for s, s_0 say. Let $x_1 = x + s_0p^b$; then the unique extension of (x, b, m) to mod p^{m+1} is clearly $(x_1, b_1, m + 1)$. Further, $l_1 = l$, by Lemma 2 (iii); hence $m + 1 > 2l_1 + 1$ and so $(x_1, b_1, m + 1)$ is of type A with $b_1 = m + 1 - l_1 = m + 1 - l = b + 1$.

(ii) In this case, by Lemma 1 (ii), $b = [(m + 1)/2]$. (a) If m is odd, then $b = (m + 1)/2$; hence $b + l = (m + 1)/2 + l \geqq (m + 1)/2 + m/2 > m$. Therefore in (5) $f(x + sp^b) \equiv f(x) \pmod{p^{m+1}}$. Hence if $f(x) \not\equiv 0 \pmod{p^{m+1}}$, then (x, b, m) has no extension to mod p^{m+1}; if $f(x) \equiv 0 \pmod{p^{m+1}}$ then, since $m + 1 \leqq 2l$, x is a solution of type B mod p^{m+1} with

$$b(m+1, x) = \left[\frac{m+1+1}{2}\right], \quad \text{by Lemma 1 (ii)}$$

$$= \frac{m+1}{2}, \quad \text{since } m \text{ is odd}$$

$$= b(m, x),$$

i.e., in this case $(x, b, m+1)$ is the unique extension. (b) If m is even, then $b = m/2$. For any s, $x + sp^b$ is a solution of type B mod p^m, by Lemma 2 (i), i.e., $l' = l(x + sp^b) \geqq m/2$. If $f(x + sp^b) \equiv 0 \pmod{p^{m+1}}$ then

$$b(m+1, x+sp^b) = \operatorname{Max}\left(\left[\frac{m+1+1}{2}\right], m+1-l'\right)$$

$$= \operatorname{Max}\left(\frac{m+2}{2}, m+1-l'\right)$$

$$= \frac{m+2}{2}, \quad \text{since } l' \geqq \frac{m}{2},$$

$$= b + 1.$$

I.e., the solution-set mod p^{m+1} containing $x + sp^b$ is just $(x + sp^b, b+1, m+1)$. This completes the proof of Theorem 1.

THEOREM 2. *If* (x, b, m) *is a solution-set of type* A *then*

$$f(x) + uf'(x) \equiv 0 \pmod{p^{2m-2l}} \tag{7}$$

has a solution u, *unique* mod p^{m-2l}, *and* $(x+u, 2m-3l, 2m-2l)$ *is the unique extension to* mod p^{2m-2l} *of* (x, b, m).

Proof. Since (x, b, m) is a solution-set of type A, $m > 2l$. Hence, since $p^m \mid f(x)$ and $p^l \parallel f'(x)$, equation (7) has a solution for u, unique mod p^{2m-3l}. Further $p^{m-l} \mid u$ since, from (7), $uf'(x) \equiv 0 \pmod{p^m}$. By Taylor's theorem,

$$f(x+u) \equiv f(x) + uf'(x) \pmod{p^{2m-2l}}$$

$$\equiv 0 \pmod{p^{2m-2l}}, \quad \text{by (7)}.$$

Therefore $x + u$ is a solution mod p^{2m-2l} and, since $p^b = p^{m-l} \mid u$, $x + u \in (x, b, m)$. By Theorem 1 (i) the solution-set (x, b, m) has a unique extension $(x_1, b+1, m+1)$ to mod p^{m+1}, also of type A; by induction it has a unique extension $(x_{m-2l}, b+m-2l, 2m-2l)$ to mod $2m-2l$. Since $x+u$ is a solution mod p^{2m-2l} this concludes the proof of the theorem.

4. Description of the Algorithm. The solution-sets of an integral polynomial $f(x)$ mod p^m form a tree with extension as the connective. For example, the solution-sets of $f(x) = (x+1)(x^2 - x + 6) \pmod{2^m}$ are depicted in Figure 1. We can construct all the solution-sets by starting with the unique solution-set mod p^0, namely, $(0, 0, 0)$, and calculate the solution-sets mod p^{m+1} as the extensions of the solution-sets mod p^m. For a solution-set of type A we may construct its extension to mod p^N in about $\log_2 N$ steps by the algorithm of Theorem 2. For solution-sets of type B mod p^m we construct the solution-sets mod p^{m+1} by means of the criteria of Theorem 1.

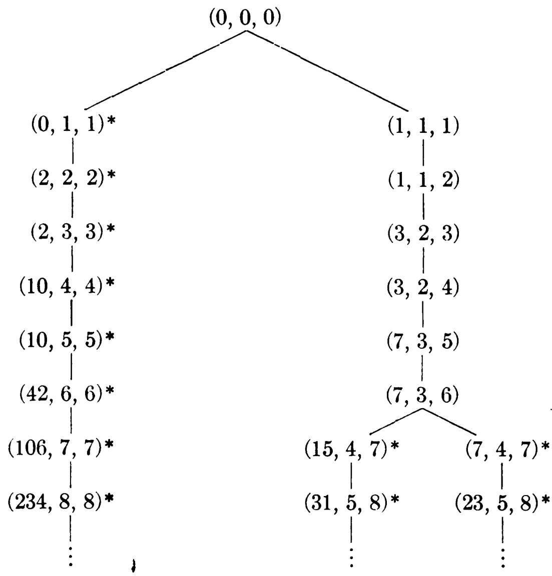

FIG. 1. Solution-sets of $(x + 1)(x^2 - x + 6) = 0 \pmod{2^m}$. The solution-sets of type A are indicated by *.

5. Interpretation in the p-adic Field. The solutions of $f(x) \equiv 0$ to arbitrary high powers of p correspond to the solution of $f(x) = 0$ in the p-adic field. In this interpretation a solution-set (x, b, m) corresponds to an interval in which $f(x)$ is small in the p-adic valuation; specifically, $|f(y)|_p \leqq p^{-m}$ for $|y - x|_p \leqq p^{-b}$. The relevance of the definition of type of solution-sets is indicated by Theorem 1. If (x, b, m) is a solution-set of type A then, by induction of Theorem 1 (i), there is a unique solution y of $f(y) = 0$ in $|y - x|_p \leqq p^{-b}$. On the other hand, if (x, b, m) is a solution-set of type B then although $|f(y)|_p$ is "small" in the range $|y - x|_p \leqq p^{-b}$ there may be no solutions of $f(y) = 0$ in this range, or one or more solutions. Theorem 2 exhibits the operation of the Newton-Raphson algorithm. The computation of $-f(x)/f'(x)$ corresponds to solving equation (7) to modulus p^∞. For computational purposes we must be satisfied with solving the equation to modulus some suitably high power of p. Restriction of the algorithm to solution-sets of type A both guarantees that the iteration converges (in the p-adic topology) and indicates the "right" modulus in which to solve equation (7), namely p^{2m-2l}. By "right" we mean that no greater modulus will guarantee a smaller value of $|f(x')|_p$ for the next iterate x'.

From the p-adic interpretation it also follows that there are no type B solutions for some sufficiently large modulus, unless the *rational* polynomial $f(x)$ has a repeated factor. For if (x_n, b, n) is a convergent sequence of type B solution-sets then $|f(x_n)|_p \leqq p^{-n}$ and $|f'(x_n)|_p \leqq p^{-l} \leqq p^{-n/2}$. Hence $\lim_n x_n$ is a root of both $f(x)$ and $f'(x)$. Further, the existence of a common root of $f(x)$ and $f'(x)$ in the p-adic field implies a repeated factor of the rational polynomial $f(x)$ since the two discriminants are formally the same.

6. The Search for Close-Packed Codes. The existence of a close-packed error-correcting binary code [2] requires integers x, r with

$$f_r(x) \equiv r!\left\{1 + x + \binom{x}{2} + \cdots + \binom{x}{r}\right\} = 2^k. \tag{8}$$

The algorithm described in §4 was programmed for the IBM 704 to search for solutions of $f_r(x) \equiv 0 \pmod{2^m}$. For all m, r with $2 \leqq r \leqq 20$ and $0 \leqq m \leqq 139$ the least value of x with

$$\begin{aligned} &0 \leqq x < 2^{70}, \\ &f_r(x) \equiv 0 \pmod{2^m} \end{aligned} \tag{9}$$

and

$$f_r(x) \not\equiv 0 \pmod{2^{m+1}}$$

was printed and also an indication of whether or not

$$x < r \cdot 2^{[(m+r-1)/r]}. \tag{10}$$

Finally it was determined for each value of r that there were no solutions of $f_r(x) \equiv 0 \pmod{2^{140}}$ with $0 \leqq x < 2^{70}$. Now if $f_r(x) = (r!) \cdot 2^k$ with $0 \leqq x < 2^{70}$ then either $k + s \geqq 140$ (where $2^s \parallel r!$) or equations (9) hold with $m = k + s$. In the latter case inequality (10) must also be satisfied. For if not, then $x \geqq r \cdot 2^{m/r}$ and hence $f_r(x) \geqq (x - r)^r \geqq r^r(2^{m/r} - 1)^r \geqq r^r(3 \cdot 2^{m/r}/4)^r = (3r/4)^r \cdot 2^m > (r!) \cdot 2^m > (r!) \cdot 2^k$.

The only solutions of (9) and (10) found for $2 \leqq r \leqq 20$ and $2r + 1 < x$ were $x = 90$, $r = 2$ and $x = 23$, $r = 3$. Hence there are no solutions of $f_r(x) = (r!) \cdot 2^k$ for $2 \leqq r \leqq 20$ and $0 \leqq x < 2^{70}$ other than

(i) $0 \leqq x \leqq r$ for arbitrary r; these do not correspond to close-packed codes.

(ii) $x = 2r + 1$ for arbitrary r; these correspond to the trivial r error-correcting codes of two code points of length $2r + 1$.

(iii) $x = 90$, $r = 2$; this does not correspond to a close-packed code as shown in [1].

(iv) $x = 23$, $r = 3$; this corresponds to the Golay-Paige code of 2^{12} code points of length 23 [1, 3].

IBM Watson Research Center
Yorktown Heights, New York

1. M. J. E. Golay, "Notes on digital coding," *Proc. IRE*, v. 37, 1949, p. 657.
2. R. W. Hamming, "Error detecting and error correcting codes," *Bell Systems Tech. J.*, v. 24, 1950, p. 147–160. MR **12**, 35.
3. Lowell J. Paige, "A note on the Mathieu groups," *Canad. J. Math.* v. 9, 1957, p. 15–18. MR **18**, 871.
4. J. L. Selfridge, Private Communication.
5. H. S. Shapiro & D. L. Slotnick, "On the mathematical theory of error-correcting codes," *IBM J. Res. Develop.*, v. 3, 1959, p. 25–34. MR **20** #5092.