A CRITERION FOR POLYNOMIALS TO BE CONGRUENT TO THE PRODUCT OF LINEAR POLYNOMIALS (mod p)

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College, Huaian, Jiangsu 223001, P.R. China
e-mail: hyzhsun@public.hy.js.cn

(Submitted November 2004-Final Revision February 2005)

ABSTRACT

Let $\{u_n\}$ be defined by $u_{1-m} = \cdots = u_{-1} = 0, u_0 = 1$ and $u_n + a_1u_{n-1} + \cdots + a_mu_{n-m} = 0$ $(m \geq 2,\ n \geq 1)$. In this paper we show that the congruence $x^m + a_1x^{m-1} + \cdots + a_m \equiv 0 \pmod p$ has m distinct solutions if and only if $u_{p-m} \equiv \cdots \equiv u_{p-2} \equiv 0 \pmod p$ and $u_{p-1} \equiv 1 \pmod p$, where p is a prime such that $p > m$ and $p \not| a_m$.

1. INTRODUCTION

In [2] the author extended Lucas series to general linear recurring sequences by defining $\{u_n(a_1, \ldots, a_m)\}$ as follows:

$$\begin{aligned} &u_{1-m} = \cdots = u_{-1} = 0,\ u_0 = 1, \\ &u_n + a_1u_{n-1} + \cdots + a_mu_{n-m} = 0 \quad (n = 1, 2, 3, \ldots), \end{aligned} \tag{1}$$

where $m \geq 2$ and $a_1, \ldots, a_m$ are complex numbers.

Let $\mathbb{Z}$ be the set of integers. In this paper we establish the following result.

Theorem 1: *Let $m \geq 2,\ m, a_1, \ldots, a_m \in \mathbb{Z}$, $u_n = u_n(a_1, \ldots, a_m)$, and let p be a prime such that $p > m$ and $p \not| a_m$. Then the congruence $x^m + a_1x^{m-1} + \cdots + a_m \equiv 0 \pmod p$ has m distinct solutions if and only if*

$$u_{p-m} \equiv \cdots \equiv u_{p-2} \equiv 0 \pmod p \quad \textit{and} \quad u_{p-1} \equiv 1 \pmod p. \tag{2}$$

The famous Chebotarev density theorem implies that (see for example [4]) if the polynomial $x^m + a_1x^{m-1} + \cdots + a_m$ $(a_1, \ldots, a_m \in \mathbb{Z})$ is irreducible over $\mathbb{Z}(x)$, then the set S of primes p such that $x^m + a_1x^{m-1} + \cdots + a_m \equiv 0 \pmod p$ has m solutions has a positive density $d(S)$, that is,

$$d(S) = \lim_{x \to +\infty} \frac{|\{p :\ p \leq x,\ p \in S\}|}{|\{p :\ p \leq x,\ p \text{ is a prime}\}|} > 0.$$

Thus, by Theorem 1 we have

Corollary 1: *Let $m \geq 2,\ a_1, \ldots, a_m \in \mathbb{Z}$ and $u_n = u_n(a_1, \ldots, a_m)$. If $x^m + a_1x^{m-1} + \cdots + a_m$ is irreducible over $\mathbb{Z}(x)$, then there are infinitely many prime p satisfying (2).*

2. PROOF OF THEOREM 1

Let $f(x) = x^m + a_1x^{m-1} + \cdots + a_m$. If $f(x) \equiv 0 \pmod p$ has m distinct solutions $b_1, \ldots, b_m$, then we have $f(x) \equiv (x - b_1) \cdots (x - b_m) \pmod p$ and $b_i \not\equiv b_j \pmod p$ for $i \neq j$ (see [1, Theorem 108]). Suppose $(x - b_1) \cdots (x - b_m) = x^m + A_1x^{m-1} + \cdots + A_m$. Then

$\sum_{i=1}^{m}(a_i - A_i)x^{m-i} \equiv 0 \pmod p$ for any integer x. Since $p > m$, by [1, Theorem 107] or Lagrange's theorem we must have $a_i \equiv A_i \pmod p$ for $i = 1, 2, \dots, m$. By the definition of $\{u_n\}$, it is evident that $u_n \equiv u_n(A_1, \dots, A_m) \pmod p$ for all $n \ge 1 - m$. Since $p \not| a_m$ we see that $p \not| b_1 \cdots b_m$. Hence, applying [2, Theorem 2.3] and Fermat's little theorem we obtain

$$\begin{aligned} u_{n+p-1} &\equiv u_{n+p-1}(A_1, \dots, A_m) = \sum_{i=1}^{m} \frac{b_i^{n+p-1+m-1}}{\prod_{\substack{j=1 \\ j \ne i}}^{m} (b_i - b_j)} \equiv \sum_{i=1}^{m} \frac{b_i^{n+m-1}}{\prod_{\substack{j=1 \\ j \ne i}}^{m} (b_i - b_j)} \\ &= u_n(A_1, \dots, A_m) \equiv u_n \pmod p \quad (n \ge 1 - m). \end{aligned}$$

Note that $u_{1-m} = \cdots = u_{-1} = 0$ and $u_0 = 1$. So (2) holds.

Conversely, suppose (2) is true. Let

$$a_0 = 1,\ g(x) = \sum_{j=0}^{p-1-m} u_j x^{p-1-m-j} \quad \text{and} \quad f(x)g(x) = \sum_{k=0}^{p-1} c_k x^k.$$

Then we see that

$$c_k = \sum_{\substack{0 \leqslant i \leqslant m \\ 0 \leqslant j \leqslant p-1-m \\ i+j=p-1-k}} a_i u_j = \sum_{max\{0,m-k\} \leqslant i \leqslant min\{m,p-1-k\}} a_i u_{p-1-k-i} \ (0 \le k \le p-1),$$

where $max\{a, b\}$ and $min\{a, b\}$ denote the maximum and minimum elements in the set $\{a, b\}$ respectively. Clearly we have $c_{p-1} = a_0 u_0 = 1$ and

$$\begin{aligned} c_0 &= a_m u_{p-1-m} \equiv (a_0 u_{p-1} + a_1 u_{p-2} + \cdots + a_m u_{p-1-m}) - a_0 u_{p-1} \\ &= -u_{p-1} \equiv -1 \pmod p. \end{aligned}$$

For $k \in \{1, 2, \dots, p-2\}$ we claim that

$$c_k = \sum_{max\{0,m-k\} \leqslant i \leqslant m} a_i u_{p-1-k-i}. \tag{3}$$

If $p - 1 - k \geqslant m$, then clearly (3) holds. If $1 \leqslant p - 1 - k < m$ and for $p - k \leqslant i \leqslant m$ we have $1 - m \leqslant p - 1 - k - i \leqslant -1$ and so $u_{p-1-k-i} = 0$. Thus, $\sum_{i=p-k}^{m} a_i u_{p-1-k-i} = 0$ and hence, (3) is also true.

If $m \leqslant k \leqslant p-2$, from (1) and (3) we see that $c_k = \sum_{i=0}^{m} a_i u_{p-1-k-i} = 0$. If $1 \leqslant k \leqslant m-1$, by (1), (3) and the fact that $u_{p-m} \equiv \cdots \equiv u_{p-2} \equiv 0 \pmod p$ we get

$$\begin{aligned} c_k &= \sum_{m-k \leqslant i \leqslant m} a_i u_{p-1-k-i} = \sum_{0 \leqslant i \leqslant m} a_i u_{p-1-k-i} - \sum_{0 \leqslant i \leqslant m-k-1} a_i u_{p-1-k-i} \\ &= -\sum_{0 \leqslant i \leqslant m-k-1} a_i u_{p-1-k-i} \equiv 0 \pmod p. \end{aligned}$$

Therefore, $c_k \equiv 0 \pmod p$ for $k = 1, 2, \dots, p-2$.

Now, putting the above together we obtain

$$f(x)g(x) = \left(\sum_{i=0}^{m} a_i x^{m-i}\right)\left(\sum_{j=0}^{p-1-m} u_j x^{p-1-m-j}\right) = \sum_{k=0}^{p-1} c_k x^k \equiv x^{p-1} - 1 \pmod p. \qquad (4)$$

Since $x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \pmod p$ by Lagrange's theorem (see [1, Theorem 112]), we see that $f(x)$ is congruent to the product of distinct linear polynomials (mod p). This completes the proof of Theorem 1.

3. APPLICATION TO CUBIC CONGRUENCES

Theorem 2: *Let $a_1, a_2, a_3 \in \mathbb{Z}$, $u_n = u_n(a_1, a_2, a_3)$, $a = (a_1^2 - 3a_2)^3$, $b = -2a_1^3 + 9a_1a_2 - 27a_3$, and let $p > 3$ be a prime such that $p \not| \, aba_3(b^2 - 4a)$. Then the following statements are equivalent:*

(i) $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$ *has three solutions,*

(ii) $u_{p-1+n} \equiv u_n \pmod p$ *for all* $n \geq -2$,

(iii) $u_{p-3} \equiv u_{p-2} \equiv 0 \pmod p$ *and* $u_{p-1} \equiv 1 \pmod p$,

(iv) $u_{p-2} \equiv 0 \pmod p$,

(v) $U_{\frac{p-(\frac{p}{3})}{3}} \equiv 0 \pmod p$,

(vi) $s_{p+1} \equiv a_1^2 - 2a_2 \pmod p$,

(vii) $V_{\frac{p-(\frac{p}{3})}{3}} \equiv 2(a_1^2 - 3a_2)^{\frac{1-(\frac{p}{3})}{2}} \pmod p$,

(viii) *if* $(\frac{a}{p}) = 1$, *then* $p \mid U_{\frac{p-(\frac{p}{3})}{6}}$; *if* $(\frac{a}{p}) = -1$, *then* $p \mid V_{\frac{p-(\frac{p}{3})}{6}}$,

where $(\frac{n}{m})$ *is the Legendre symbol, and* $\{U_n\}$, $\{V_n\}$, $\{s_n\}$ *are given by*

$$\begin{aligned}
&U_0 = 0,\ U_1 = 1,\ U_{n+1} = bU_n - aU_{n-1} \quad (n \geq 1),\\
&V_0 = 2,\ V_1 = b,\ V_{n+1} = bV_n - aV_{n-1} \quad (n \geq 1),\\
&s_0 = 3,\ s_1 = -a_1,\ s_2 = a_1^2 - 2a_2,\ s_{n+3} + a_1s_{n+2} + a_2s_{n+1} + a_3s_n = 0\ (n \geq 0).
\end{aligned}$$

Proof: From the definition of u_n we see that (ii) is equivalent to (iii). As $p \not| \, b^2 - 4a$ and $-\frac{b^2-4a}{27}$ is the discriminant of $x^3 + a_1x^2 + a_2x + a_3$, the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$ has no multiple solutions. By Theorem 1, (i) and (iii) are equivalent. According to [3, Theorem 4.3], (i) is equivalent to (iv). By [3, Theorem 3.2(i)], (iv) and (v) are equivalent. From [3, Theorem 4.1] we know that (i) is equivalent to (vi). By [3, Lemma 3.1], (vi) is equivalent to (vii). It is well known that (see [5])

$$U_{2n} = U_nV_n, \quad V_{2n} = V_n^2 - 2a^n \quad \text{and} \quad V_n^2 - (b^2 - 4a)U_n^2 = 4a^n.$$

Thus, we have

$$V_{\frac{p-(\frac{p}{3})}{3}} = V^2_{\frac{p-(\frac{p}{3})}{6}} - 2a^{\frac{p-(\frac{p}{3})}{6}} \equiv V^2_{\frac{p-(\frac{p}{3})}{6}} - 2\left(\frac{a_1^2 - 3a_2}{p}\right)(a_1^2 - 3a_2)^{\frac{1-(\frac{p}{3})}{2}} \pmod p.$$

Therefore, (vii) is equivalent to

$$V^2_{\frac{p-(\frac{p}{3})}{6}} \equiv 2\left(1+\left(\frac{a_1^2-3a_2}{p}\right)\right)(a_1^2-3a_2)^{\frac{1-(\frac{p}{3})}{2}} \pmod p.$$

As $V_n^2-(b^2-4a)U_n^2=4a^n$, the above congruence is equivalent to

$$(b^2-4a)U^2_{\frac{p-(\frac{p}{3})}{6}} \equiv 2\left(1-\left(\frac{a_1^2-3a_2}{p}\right)\right)(a_1^2-3a_2)^{\frac{1-(\frac{p}{3})}{2}} \pmod p.$$

Thus, (vii) and (viii) are equivalent and the theorem is proved.

Remark 1: Let $a_1, a_2, a_3 \in \mathbb{Z}$ be such that $x^3+a_1x^2+a_2x+a_3$ is irreducible in $\mathbb{Z}[x]$. From Theorem 2 and Chebotarev density theorem we know that there are infinitely many primes p satisfying (i)-(viii) in Theorem 2.

Let p be a prime such that $p>3$ and $p\nmid a_1^2-3a_2$. From [3, Theorem 4.1 and 4.2] and [3, Lemma 3.1] we know that

$$\begin{aligned}&x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p \quad \text{has no solutions}\\ &\iff s_{p+1}\equiv a_2 \pmod p \iff V_{\frac{p-(\frac{p}{3})}{3}} \equiv -(a_1^2-3a_2)^{\frac{1-(\frac{p}{3})}{2}} \pmod p\end{aligned}$$

and

$$\begin{aligned}&x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p \quad \text{has one and only one solution}\\ &\iff s_{p+1}\not\equiv a_2, a_1^2-2a_2 \pmod p\\ &\iff V_{\frac{p-(\frac{p}{3})}{3}} \not\equiv -(a_1^2-3a_2)^{\frac{1-(\frac{p}{3})}{2}},\ 2(a_1^2-3a_2)^{\frac{1-(\frac{p}{3})}{2}} \pmod p.\end{aligned}$$

By Chebotarev density theorem, there are also infinitely many primes satisfying one of the above conditions in terms of $\{s_n\}$ or $\{V_n\}$.

REFERENCES

[1] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* (5th edition), Oxford Univ. Press, Oxford, 1981, 84-86.

[2] Z.H. Sun. “Linear Recursive Sequences and Powers of Matrices.” *Fibonacci Quart.* **39** (2001): 339-351.

[3] Z.H. Sun. “Cubic and Quartic Congruences Modulo a Prime.” *J. Number Theory* **102** (2003): 41-89.

[4] D. Terr. *Chebotarev Density Theorem.* http://mathworld.wolfram.com/ChebotarevDensityTheorem.html.

[5] H.C. Williams. *Édouard Lucas and Primality Testing.* Canadian Mathematical Society Series of Monographs and Advanced Texts (Vol. 22), Wiley, New York, 1998, p. 74.

AMS Classification Numbers: 11A07, 11B39, 11B50, 11T06

✠ ✠ ✠