ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE DIRECT®

Journal of Number Theory 102 (2003) 41–89

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Cubic and quartic congruences modulo a prime

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College, Huaian, Jiangsu 223001, People's Republic of China

Received 5 March 2002; revised 25 November 2002

Communicated by W. Duke

Abstract

Let $p>3$ be a prime, and $N_p(f(x))$ denote the number of solutions of the congruence $f(x)\equiv 0 \pmod p$. In this paper, using the third-order recurring sequences we determine the values of $N_p(x^3+a_1x^2+a_2x+a_3)$ and $N_p(x^4+ax^2+bx+c)$, and construct the solutions of the corresponding congruences, where a_1,a_2,a_3,a,b,c are integers.

MSC: Primary 11A07; Secondary 11B39, 11B50, 11A15

Keywords: Cubic congruence; Quartic congruence; Recurring sequence

1. Introduction

Let p be a prime greater than 3, and let $\mathbb{Z}$ be the set of integers. In this paper we study the general cubic congruence $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$ and the quartic congruence $x^4+ax^2+bx+c\equiv 0 \pmod p$, where $a_1,a_2,a_3,a,b,c\in\mathbb{Z}$.

Denote the number of solutions of the congruence $f(x)\equiv 0 \pmod p$ by $N_p(f(x))$. Let $(\frac{d}{p})$ be the Legendre symbol, and let $D=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$ be the discriminant of the cubic polynomial $x^3+a_1x^2+a_2x+a_3$ (cf. [17]). According to Stickelberger [5,14], Dickson [6] and Skolem [9,11] we have

E-mail address: hyzhsun@public.hy.js.cn.

0022-314X/03/$ - see front matter
doi:10.1016/S0022-314X(03)00067-2

Theorem 1.1. *If $p>3$ is a prime, $a_1,a_2,a_3\in\mathbb{Z}$ and $p\nmid D$, then*

$$N_p(x^3+a_1x^2+a_2x+a_3)=\begin{cases}0 \text{ or } 3 & \text{if } (\frac{D}{p})=1,\\ 1 & \text{if } (\frac{D}{p})=-1.\end{cases}$$

In 1829 Cauchy (cf. [4,18]) proved

Theorem 1.2. *Let $A,B\in\mathbb{Z}$, and let $p>3$ be a prime such that $p\nmid AB$ and $(\frac{-4A^3-27B^2}{p})=1$. If $\{v_n\}$ is defined by $v_0=2$, $v_1=B$ and $v_{n+1}=Bv_n+(\frac{A}{3})^3v_{n-1}(n\geqslant 1)$, then*

$$N_p(x^3+Ax-B)=\begin{cases}3 & \text{if } v_{(p-(\frac{p}{3}))/3}\equiv 2(\frac{p}{3})(\frac{A}{3})^{(1-(\frac{p}{3}))/2}\pmod p,\\ 0 & \text{if } v_{(p-(\frac{p}{3}))/3}\equiv -(\frac{p}{3})(\frac{A}{3})^{(1-(\frac{p}{3}))/2}\pmod p.\end{cases}$$

In 1992 Spearman and Williams [12,13] revealed the connection between cubic congruences and binary quadratic forms. They established the following result.

Theorem 1.3. *Let a_1,a_2,a_3 be integers such that $x^3+a_1x^2+a_2x+a_3$ is irreducible over the field of rational numbers and has a non-square discriminant D. Let $H(D)$ denote the form class group of classes of primitive, integral binary quadratic forms of discriminant D. Then there is a unique subgroup $J(a_1,a_2,a_3)$ of index 3 in $H(D)$ such that if p is any prime >3 with $(\frac{D}{p})=1$, then $N_p(x^3+a_1x^2+a_2x+a_3)=3$ if and only if p is represented by one of the classes in $J(a_1,a_2,a_3)$.*

From the above we know that solving cubic and quartic congruences has a long history. For more results along this line one may consult [1–3,7,18,19].

For integers a_1,a_2,a_3 let $\{u_n\}$ and $\{s_n\}$ be the third-order recurring sequences defined by

$$u_{-2}=u_{-1}=0,\quad u_0=1,\quad u_{n+3}+a_1u_{n+2}+a_2u_{n+1}+a_3u_n=0\ \ (n\geqslant -2)$$

and

$$s_0=3,\quad s_1=-a_1,\quad s_2=a_1^2-2a_2,\quad s_{n+3}+a_1s_{n+2}+a_2s_{n+1}+a_3s_n=0\ \ (n\geqslant 0).$$

In the paper we mainly determine the values of $s_{p+1},s_{p+2},u_{p-2},\ u_{p-1},u_p$ modulo p. As applications, we introduce new types of pseudoprimes, obtain the formulas for $N_p(x^3+a_1x^2+a_2x+a_3)$ and $N_p(x^4+ax^2+bx+c)$, and construct the solutions of cubic and quartic congruences in terms of $\{s_n\}$ as well. As examples we have the following typical results on cubic and quartic congruences.

(1.1) Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$, $a=(a_1^2-3a_2)^3$, $b=-2a_1^3+9a_1a_2-27a_3$ and $D=-\frac{1}{27}(b^2-4a)=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$. If $p\nmid ab$, then

$$N_p(x^3+a_1x^2+a_2x+a_3)=\begin{cases}3 & \text{if } Du_{p-2}^2\equiv 0\ (\mathrm{mod}\ p),\\ 0 & \text{if } Du_{p-2}^2\equiv (a_1^2-3a_2)^2\ (\mathrm{mod}\ p),\\ 1 & \text{if } Du_{p-2}^2\not\equiv 0,\ (a_1^2-3a_2)^2\ (\mathrm{mod}\ p).\end{cases}$$

Moreover, if $N_p(x^3+a_1x^2+a_2x+a_3)=1$, then the unique solution is given by

$$x\equiv\frac{(-a_1^2a_2+6a_2^2-9a_1a_3)u_{p-2}+a_1^3-6a_1a_2+27a_3}{-bu_{p-2}+3(a_1^3-3a_2)}\ (\mathrm{mod}\ p).$$

(1.2) Let $p>3$ be a prime, and $a_1,a_2,a_3\in\mathbb{Z}$. If $p\nmid a_1^2-3a_2$, we have

$$N_p(x^3+a_1x^2+a_2x+a_3)=\begin{cases}3 & \text{if } s_{p+1}\equiv a_1^2-2a_2\ (\mathrm{mod}\ p),\\ 0 & \text{if } s_{p+1}\equiv a_2\ (\mathrm{mod}\ p),\\ 1 & \text{if } s_{p+1}\not\equiv a_2,\ a_1^2-2a_2\ (\mathrm{mod}\ p).\end{cases}$$

Moreover, if $N_p(x^3+a_1x^2+a_2x+a_3)=1$, then the unique solution of the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0\ (\mathrm{mod}\ p)$ is given by $x\equiv(2a_1a_2-9a_3-a_1s_{p+1})/(-2a_1^2+3a_2+3s_{p+1})\ (\mathrm{mod}\ p)$; if $N_p(x^3+a_1x^2+a_2x+a_3)=0$ and $p\nmid a_1^2-3a_2$, then $(2s_{p+2}+a_1a_2-3a_3)^2\equiv D\ (\mathrm{mod}\ p)$; if $N_p(x^3+a_1x^2+a_2x+a_3)=3$, $p\nmid D$ and $x_0=\frac{1}{2}((\frac{-a_3}{p})s_{\frac{p+1}{2}}-a_1)\not\equiv -a_1\ (\mathrm{mod}\ p)$, then

$$x\equiv x_0,\quad \frac{1}{2}\left(-a_1-x_0\pm\frac{d}{3x_0^2+2a_1x_0+a_2}\right)\ (\mathrm{mod}\ p)$$

are the three solutions of the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0\ (\mathrm{mod}\ p)$, where D is given by (1.1) and d is an integer such that $d^2\equiv D\ (\mathrm{mod}\ p)$.

(1.3) Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$, and let $\{S_n\}$ be given by $S_0=3$, $S_1=-2a$, $S_2=2a^2+8c$ and $S_{n+3}=-2aS_{n+2}+(4c-a^2)S_{n+1}+b^2S_n$ $(n\geqslant 0)$. If $p\nmid a^2+12c$, then $N_p(x^4+ax^2+bx+c)=1$ if and only if $S_{p+1}\equiv a^2-4c\ (\mathrm{mod}\ p)$. If $N_p(x^4+ax^2+bx+c)=1$, then the unique solution of the congruence $x^4+ax^2+bx+c\equiv 0(\mathrm{mod}\ p)$ is given by $x\equiv(a^2-4c-S_{(p+1)/2}^2)/(4b)\ (\mathrm{mod}\ p)$.

(1.4) Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$ and $p\nmid(a^2+12c)b((4a^3+27b^2)b^2-16c(a^4+9ab^2-8a^2c+16c^2))$. Then the congruence $x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)$ has four solutions if and only if $S_{(p-1)/2}\equiv 3\ (\mathrm{mod}\ p)$ and $S_{p+1}\equiv 2a^2+8c\ (\mathrm{mod}\ p)$, where $\{S_n\}$ is the sequence as in (1.3).

(1.5) Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$, $D(a,b,c)=-(4a^3+27b^2)b^2+16c(a^4+9ab^2-8a^2c+16c^2)$ and $p\nmid bD(a,b,c)$. Then

$$N_p(x^4+ax^2+bx+c)=1+\sum_y\left(\frac{y}{p}\right),$$

where y runs over the solutions of the congruence $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\pmod p$.

We remark that (1.1) and (1.2) are better than Cauchy's result since we do not need to compute the Legendre symbol $(\frac{D}{p})$. The proofs of (1.1) and (1.2) are based on [15], and the proofs of (1.3)–(1.5) depend on (1.2). (1.5) is the basic result for quartic congruences, which improves Skolem's result (see [7,10]). Although the methods used are elementary, our results seem simple and useful, and are not easy consequences of Galois' theory. For example, using Galois' theory we do not know why (1.3) is true.

Throughout this paper we use the following notations:

$[x]$—the greatest integer not exceeding x, $(\frac{x}{p})$—the Legendre symbol, $N_p(f(x))$—the number of solutions of the congruence $f(x)\equiv 0\pmod p$, $C_0(p)$, $C_1(p)$, $C_2(p)$—the sets defined by Sun [15, Definition 2.1], $D(a,b,c)=-(4a^3+27b^2)b^2+16c(a^4+9ab^2-8a^2c+16c^2)$, $\omega=(-1+\sqrt{-3})/2$.

2. Connections between Lucas sequences and cubic congruences

For $a,b\in\mathbb{Z}$ the Lucas sequences $\{u_n(a,b)\}$ and $\{v_n(a,b)\}$ are defined by

$$u_0(a,b)=0,\quad u_1(a,b)=1\quad\text{and}\quad u_{n+1}(a,b)=bu_n(a,b)-au_{n-1}(a,b)(n\geqslant 1)\qquad(2.1)$$

and

$$v_0(a,b)=2,\quad v_1(a,b)=b\quad\text{and}\quad v_{n+1}(a,b)=bv_n(a,b)-av_{n-1}(a,b)(n\geqslant 1).\qquad(2.2)$$

It is well known that

$$u_n(a,b)=\frac{1}{\sqrt{b^2-4a}}\left\{\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n-\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n\right\}\quad(b^2-4a\neq 0)$$

and

$$v_n(a,b)=\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n+\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n.\qquad(2.3)$$

When p is an odd prime such that $p\nmid a$, we have the following congruences (see [8]):

$$u_{p-(\frac{b^2-4a}{p})}(a,b)\equiv 0\ (\mathrm{mod}\ p)\quad\text{and}\quad u_p(a,b)\equiv\left(\frac{b^2-4a}{p}\right)\ (\mathrm{mod}\ p).\tag{2.4}$$

Lemma 2.1. *Let $a,b\in\mathbb{Z}$, $u_n=u_n(a,b)$ and $v_n=v_n(a,b)$. Then*

(i) $v_{3n}=v_n^3-3a^nv_n$.

(ii) *If p is an odd prime such that $p\nmid a(b^2-4a)$ and $\varepsilon=(\frac{b^2-4a}{p})$, then*

$$v_{p-\varepsilon}\equiv 2a^{\frac{1-\varepsilon}{2}}\ (\mathrm{mod}\ p)\quad\text{and}\quad v_{p+\varepsilon}\equiv a^{\frac{\varepsilon-1}{2}}(b^2-2a)\ (\mathrm{mod}\ p).$$

Proof. Set $t=\frac{1}{2}(b+\sqrt{b^2-4a})$ and $u=\frac{1}{2}(b-\sqrt{b^2-4a})$. Then we find $tu=a$ and $v_m=t^m+u^m$ for $m\geqslant 0$. Thus,

$$v_{3n}=t^{3n}+u^{3n}=(t^n+u^n)^3-3(tu)^n(t^n+u^n)=v_n^3-3a^nv_n.$$

This proves (i).

Now consider (ii). One can easily check that

$$v_n=\frac{b}{a}u_{n+2}-\frac{b^2-2a}{a}u_{n+1}=2u_{n+1}-bu_n=bu_n-2au_{n-1}=(b^2-2a)u_{n-1}-abu_{n-2}.$$

Thus applying (2.4) we see that

$$v_{p-\varepsilon}=\varepsilon(2a^{(1-\varepsilon)/2}u_p-bu_{p-\varepsilon})\equiv 2a^{(1-\varepsilon)/2}\ (\mathrm{mod}\ p)$$

and

$$v_{p+\varepsilon}=\varepsilon(a^{(\varepsilon-1)/2}(b^2-2a)u_p-a^{\varepsilon}bu_{p-\varepsilon})\equiv a^{(\varepsilon-1)/2}(b^2-2a)\ (\mathrm{mod}\ p).$$

This proves (ii) and hence the proof is complete. □

In [15] we point out the following basic result without proof.

Lemma 2.2. *Let $p>3$ be a prime, $a,b\in\mathbb{Z}$ and $p\nmid a$. Then $N_p(x^3-3ax-ab)=1$ if and only if $(\frac{-3(b^2-4a)}{p})=-1$. Moreover, if $(\frac{-3(b^2-4a)}{p})=-1$, then the unique solution of the congruence $x^3-3ax-ab\equiv 0\ (\mathrm{mod}\ p)$ is given by*

$$x\equiv a^{\frac{p-(\frac{p}{3})}{3}}v_{(p+2(\frac{p}{3}))/3}(a,b)\equiv\frac{b}{a^{[p/3]}v_{(p-(\frac{p}{3}))/3}(a,b)-1}\ (\mathrm{mod}\ p).$$

Proof. If $p \mid b$, then clearly $N_p(x^3-3ax-ab)=1$ if and only if $(\frac{-3(b^2-4a)}{p})=(\frac{3a}{p})=1$. Since $v_{(p+2(\frac{p}{3}))/3}(a,b)\equiv(\sqrt{-a})^{(p+2(\frac{p}{3}))/3}+(-\sqrt{-a})^{(p+2(\frac{p}{3}))/3}=0\pmod p$ and $v_{(p-(\frac{p}{3}))/3}(a,b)\equiv 2(\sqrt{-a})^{(p-(\frac{p}{3}))/3}=2(-a)^{(p-(\frac{p}{3}))/6}\pmod p$ by (2.3), we see that the result is true when $p \mid b$.

If $p \mid b^2-4a$, then $(\frac{-3(b^2-4a)}{p})=0\neq -1$ and $N_p(x^3-3ax-ab)=3\neq 1$ since $x^3-3ax-ab\equiv(x-b)(x+b/2)^2\pmod p$. So the result is true when $p \mid b^2-4a$.

Now assume that $p\nmid b(b^2-4a)$. If the congruence $x^3-3ax-ab\equiv 0\pmod p$ has a solution $x\equiv x_0\pmod p$, then clearly $x_0\not\equiv 0,-b/2,-b/3\pmod p$ and

$$\begin{aligned}x^3-3ax-ab&\equiv(x-x_0)(x^2+x_0x+ab/x_0)\\&\equiv(x-x_0)\left(\left(x+\frac{x_0}{2}\right)^2-\frac{3a(x_0-b)}{4x_0}\right)\pmod p.\end{aligned}$$

Observing that

$$x_0^2-4ab/x_0=(x_0^3-4ab)/x_0\equiv 3a(x_0-b)/x_0\pmod p$$

and

$$b^2-4a\equiv b^2-\frac{4x_0^3}{3x_0+b}=\frac{-(x_0-b)(2x_0+b)^2}{3x_0+b}\equiv\frac{-a(x_0-b)(2x_0+b)^2}{x_0^3}\pmod p$$

we obtain

$$\left(\frac{-3(b^2-4a)}{p}\right)=\left(\frac{3a(x_0-b)}{p}\right)\left(\frac{x_0}{p}\right).$$

Hence

$$N_p(x^3-3ax-ab)=2+\left(\frac{4x_0\cdot 3a(x_0-b)}{p}\right)=2+\left(\frac{-3(b^2-4a)}{p}\right).$$

So $N_p(x^3-3ax-ab)=1$ implies that $(\frac{-3(b^2-4a)}{p})=-1$.

Now suppose $(\frac{-3(b^2-4a)}{p})=-1$. Then $(\frac{b^2-4a}{p})=-(\frac{-3}{p})=-(\frac{p}{3})$. By the above, $N_p(x^3-3ax-ab)=1$ if and only if $N_p(x^3-3ax-ab)>0$. Let $v_n=v_n(a,b)$. Using

Lemma 2.1(i) and Fermat's little theorem we see that

$$\begin{aligned}&(a^{(p-(\frac{p}{3}))/3}v_{(p+2(\frac{p}{3}))/3})^3-3a\cdot a^{(p-(\frac{p}{3}))/3}v_{(p+2(\frac{p}{3}))/3}\\&=a^{p-(\frac{p}{3})}(v_{p+2(\frac{p}{3})}+3a^{(p+2(\frac{p}{3}))/3}v_{(p+2(\frac{p}{3}))/3})-3a^{1+(p-(\frac{p}{3}))/3}v_{(p+2(\frac{p}{3}))/3}\\&\equiv a^{1-(\frac{p}{3})}v_{p+2(\frac{p}{3})}=a^{1+(\frac{b^2-4a}{p})}v_{p-2(\frac{b^2-4a}{p})}\pmod p.\end{aligned}$$

Set $\varepsilon=(\frac{b^2-4a}{p})$. It is easily seen that

$$v_{p-2\varepsilon}=\frac{b^2-a}{b}a^{-(1+\varepsilon)/2}v_{p-\varepsilon}-\frac{a^{(1-3\varepsilon)/2}}{b}v_{p+\varepsilon}.$$

Thus applying Lemma 2.1(ii) we obtain

$$v_{p-2\varepsilon}\equiv\frac{b^2-a}{b}a^{-(1+\varepsilon)/2}\cdot 2a^{(1-\varepsilon)/2}-\frac{a^{(1-3\varepsilon)/2}}{b}\cdot a^{(\varepsilon-1)/2}(b^2-2a)=a^{-\varepsilon}b\pmod p.$$

So we have

$$(a^{(p-(\frac{p}{3}))/3}v_{(p+2(\frac{p}{3}))/3})^3-3a\cdot a^{(p-(\frac{p}{3}))/3}v_{(p+2(\frac{p}{3}))/3}\equiv a^{1+\varepsilon}v_{p-2\varepsilon}\equiv ab\pmod p.$$

Hence $x\equiv a^{(p-(\frac{p}{3}))/3}v_{(p+2(\frac{p}{3}))/3}\pmod p$ is a solution of the congruence $x^3-3ax-ab\equiv 0\pmod p$. This shows that $N_p(x^3-3ax-ab)>0$ and so $N_p(x^3-3ax-ab)=1$.

Let $y=a^{[\frac{p}{3}]+1}v_{(p-(\frac{p}{3}))/3}$. Using Lemma 2.1 we see that

$$\begin{aligned}y^3&=a^{3[\frac{p}{3}]+3}(3a^{\frac{p-(\frac{p}{3})}{3}}v_{(p-(\frac{p}{3}))/3}+v_{p-(\frac{p}{3})})\\&\equiv a^{3[\frac{p}{3}]+3}(3a^{\frac{p-(\frac{p}{3})}{3}-[\frac{p}{3}]-1}y+a^{-\frac{1+(\frac{p}{3})}{2}}(b^2-2a))\equiv 3a^2y+a^2(b^2-2a)\pmod p.\end{aligned}$$

It then follows that $y\not\equiv a\pmod p$ since $p\nmid ab$. So we have

$$\begin{aligned}&\left(\frac{b}{a^{[p/3]}v_{(p-(\frac{p}{3}))/3}-1}\right)^3-3a\cdot\frac{b}{a^{[p/3]}v_{(p-(\frac{p}{3}))/3}-1}-ab\\&=\left(\frac{ab}{y-a}\right)^3-3a\cdot\frac{ab}{y-a}-ab=-\frac{ab}{(y-a)^3}(y^3-3a^2y-a^2(b^2-2a))\equiv 0\pmod p.\end{aligned}$$

Since $N_p(x^3-3ax-ab)=1$ we must have

$$a^{\frac{p-(\frac{p}{3})}{3}}v_{(p+2(\frac{p}{3}))/3}\equiv\frac{b}{a^{[p/3]}v_{(p-(\frac{p}{3}))/3}-1}\pmod p.$$

This completes the proof. □

Theorem 2.1. *Let $p>3$ be a prime, $a,b\in\mathbb{Z}$, $p\nmid a$ and $(\frac{-3(b^2-4a)}{p})=-1$, and let $x(a,b)$ denote the unique solution of the congruence $x^3-3ax-ab\equiv 0\pmod p$. Then*

$$u_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\frac{1}{b^2-4a}\left(\frac{-3a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}-1}(-bx^2(a,b)+2ax(a,b)+2ab)\pmod p$$

and

$$v_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\left(\frac{a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}-1}(x^2(a,b)-2a)\pmod p.$$

Proof. Let $u_n=u_n(a,b)$ and $v_n=v_n(a,b)$. From Lemma 2.2 we know that

$$x(a,b)\equiv a^{\frac{p-(\frac{p}{3})}{3}}v_{(p+2(\frac{p}{3}))/3}\equiv\frac{b}{a^{[p/3]}v_{(p-(\frac{p}{3}))/3}-1}\pmod p.$$

Thus,

$$v_{\frac{p-(\frac{p}{3})}{3}}\equiv a^{-[\frac{p}{3}]}\left(1+\frac{b}{x(a,b)}\right)\equiv a^{-[\frac{p}{3}]-1}(x^2(a,b)-2a)\pmod p.$$

It is easy to verify that

$$(b^2-4a)u_n=2v_{n+1}-bv_n=bv_n-2av_{n-1}.$$

So we have

$$(b^2-4a)\left(\frac{p}{3}\right)u_{(p-(\frac{p}{3}))/3}=-bv_{(p-(\frac{p}{3}))/3}+2a^{(1-(\frac{p}{3}))/2}v_{(p+2(\frac{p}{3}))/3}.\tag{2.5}$$

From this and the above we obtain

$$\begin{aligned}u_{\frac{p-(\frac{p}{3})}{3}}&\equiv\frac{1}{b^2-4a}\left(\frac{p}{3}\right)(-a^{-[p/3]-1}b(x^2(a,b)-2a)+2a^{(1-(\frac{p}{3}))/2-(p-(\frac{p}{3}))/3}x(a,b))\\&=\frac{1}{a^{[p/3]+1}(b^2-4a)}\left(\frac{p}{3}\right)(-bx^2(a,b)+2ax(a,b)+2ab)\pmod p.\end{aligned}$$

To complete the proof, we note that

$$a^{-[\frac{p}{3}]}=a^{\frac{p-(\frac{p}{3})}{6}-\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}}\pmod p.\qquad\square\tag{2.6}$$

Corollary 2.1. *Let $p>3$ be a prime, $a,b\in\mathbb{Z}$, $p\nmid a$ and $(\frac{-3(b^2-4a)}{p})=-1$. Then*

$$u_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\begin{cases}-(\frac{-2}{p})a^{(p-(\frac{p}{3}))/6-1}b\pmod p & \text{if } p\mid b^2-2a,\\ \frac{1}{b^2-4a}(\frac{-3a}{p})a^{(p-(\frac{p}{3}))/6-1}t(a,b)\pmod p & \text{if } p\nmid b^2-2a\end{cases}$$

and

$$v_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\begin{cases}2(\frac{3}{p})a^{(p-(\frac{p}{3}))/6}\pmod p & \text{if } p\mid b,\\ (\frac{a}{p})a^{(p-(\frac{p}{3}))/6-1}y(a,b)\pmod p & \text{if } p\nmid b,\end{cases}$$

where $t(a,b)\pmod p$ is the unique solution of the congruence $t^3+3a^2(b^2-4a)t+a^2b(b^2-4a)^2\equiv 0\pmod p$, and $y(a,b)\pmod p$ is the unique solution of the congruence $y^3-3a^2y-a^2(b^2-2a)\equiv 0\pmod p$.

Proof. Let $x(a,b)\pmod p$ denote the unique solution of the congruence $x^3-3ax-ab\equiv 0\pmod p$, and $t=-bx^2(a,b)+2ax(a,b)+2ab$. Using the fact that $x^3(a,b)\equiv 3ax(a,b)+ab\pmod p$ one can easily check that $t^3-3a't-a'b'\equiv 0\pmod p$, where $a'=-a^2(b^2-4a)$ and $b'=b(b^2-4a)$. Since $p\nmid a'$ and $b'^2-4a'=(b^2-2a)^2(b^2-4a)$, using Lemma 2.2 we see that $N_p(x^3-3a'x-a'b')=1$ provided $p\nmid b^2-2a$. Hence, if $p\nmid b^2-2a$ we have $t\equiv t(a,b)\pmod p$. So, by Theorem 2.1 and (2.6),

$$u_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\frac{1}{a^{[p/3]+1}(b^2-4a)}\left(\frac{p}{3}\right)t(a,b)\equiv\frac{1}{b^2-4a}\left(\frac{-3a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}-1}t(a,b)\pmod p.$$

If $p\mid b^2-2a$, then clearly $x(a,b)\equiv -b\pmod p$ and $(\frac{-3a}{p})=-(\frac{-2}{p})$. Hence, by Theorem 2.1, (2.6) and the fact that $b^2-4a\equiv -b^2\pmod p$ we have

$$u_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\frac{1}{a^{[p/3]+1}(b^2-4a)}\left(\frac{p}{3}\right)(-b^3)\equiv-\left(\frac{-2}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}-1}b\pmod p.$$

If $p\mid b$, then clearly $x(a,b)\equiv 0\pmod p$ and $(\frac{3a}{p})=-1$. By Theorem 2.1 and (2.6) we get

$$v_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv a^{-\frac{p}{3}]-1}\cdot(-2a)\equiv 2\left(\frac{3}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}}\pmod p.$$

If $p\nmid b$, then $N_p(x^3-3a^2x-a^2(b^2-2a))=1$ by Lemma 2.2. From the proof of Lemma 2.2 we know that $y=a^{[p/3]+1}v_{(p-(\frac{p}{3}))/3}(a,b)$ satisfies the congruence $y^3\equiv 3a^2y+a^2(b^2-2a)\pmod p$. Thus $y\equiv y(a,b)\pmod p$ and hence $v_{(p-(\frac{p}{3}))/3}(a,b)\equiv a^{-[p/3]-1}y(a,b)\equiv(\frac{a}{p})a^{(p-(\frac{p}{3}))/6-1}y(a,b)\pmod p$. This completes the proof. □

For given positive integer p let D_p be the set of those rational numbers whose denominator is prime to p. When $3\nmid p$, in [15] the author defined

$$C_i(p)=\left\{k\,\middle|\,\left(\frac{k+1+2\omega}{p}\right)_3=\omega^i,\ k\in D_p\right\}\quad\text{for } i=0,1,2, \tag{2.7}$$

where $(\frac{\cdot}{p})_3$ is the cubic Jacobi symbol.

According to [15], if $k\in D_p$, then $k\in C_0(p)\cup C_1(p)\cup C_2(p)$ if and only if the numerator of k^2+3 is prime to p, and $k\in C_2(p)$ if and only if $-k\in C_1(p)$. Also, from Theorem 6.1 of [15] we have

Theorem 2.2. *Let $p>3$ be a prime, $a,b\in D_p$, $p\nmid a$, $(\frac{-3(b^2-4a)}{p})=1$ and $k^2\equiv -3(b^2-4a)\pmod p$. Then*

$$u_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\begin{cases}0\pmod p & \text{if } 3b/k\in C_0(p),\\ \pm\frac{k}{b^2-4a}(\frac{-3a}{p})a^{(p-(\frac{p}{3}))/6}\pmod p & \text{if } \pm 3b/k\in C_1(p)\end{cases}$$

and

$$v_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\begin{cases}2(\frac{a}{p})a^{(p-(\frac{p}{3}))/6}\pmod p & \text{if } 3b/k\in C_0(p),\\ -(\frac{a}{p})a^{(p-(\frac{p}{3}))/6}\pmod p & \text{if } 3b/k\notin C_0(p).\end{cases}$$

Proof. If $p\mid b$, then $(\frac{-a}{p})=(\frac{-3}{p})(\frac{-3(b^2-4a)}{p})=(\frac{p}{3})$. Clearly we have

$$u_{\frac{p-(\frac{p}{3})}{3}}(a,b)=\frac{1}{\sqrt{b^2-4a}}\left\{\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^{\frac{p-(\frac{p}{3})}{3}}-\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^{\frac{p-(\frac{p}{3})}{3}}\right\}\equiv 0\pmod p$$

and

$$v_{\frac{p-(\frac{p}{3})}{3}}(a,b)=\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^{\frac{p-(\frac{p}{3})}{3}}+\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^{\frac{p-(\frac{p}{3})}{3}}$$
$$\equiv 2(\sqrt{-a})^{(p-(\frac{p}{3}))/3}=2(-a)^{(p-(\frac{p}{3}))/6}=2\left(\frac{a}{p}\right)a^{(p-(\frac{p}{3}))/6}\ (\mathrm{mod}\ p).$$

Since $0\in C_0(p)$ by Sun [15, Proposition 2.1], we see that $3b/k\in C_0(p)$. So the result holds when $p\mid b$.

If $p\nmid b$, it follows from [15, Proposition 2.2] that $3b/k\in C_i(p)$ if and only if $-k/b\in C_i(p)$. Notice that

$$\frac{3}{-k}\equiv\frac{k}{b^2-4a}\ (\mathrm{mod}\ p),\quad (-1)^{[\frac{p}{3}]}=\left(\frac{-3}{p}\right)\quad\text{and}\quad a^{-[\frac{p}{3}]}\equiv\left(\frac{a}{p}\right)a^{(p-(\frac{p}{3}))/6}\ (\mathrm{mod}\ p)$$

by (2.6). Putting $s=-k$ in [15, Theorem 6.1] we obtain the result. □

Lemma 2.3. *Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$, $a=(a_1^2-3a_2)^3$, $b=-2a_1^3+9a_1a_2-27a_3$ and $D=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$. Then*

(i) $b^2-4a=-27D$.

(ii) *If $p\nmid a_1^2-3a_2$ and $X=(a_1^2-3a_2)(3x+a_1)$, then $x^3+a_1x^2+a_2x+a_3=(X^3-3aX-ab)/(27a)$ and so $N_p(x^3+a_1x^2+a_2x+a_3)=N_p(x^3-3ax-ab)$.*

(iii) $N_p(x^3+a_1x^2+a_2x+a_3)=1$ *if and only if* $(\frac{D}{p})=-1$.

Proof. One can easily check that $b^2-4a=-27D$. So (i) holds.

Now consider (ii). It is clear that

$$x^3+a_1x^2+a_2x+a_3=\tfrac{1}{27}((3x+a_1)^3-3(a_1^2-3a_2)(3x+a_1)-b).\qquad(2.8)$$

Thus, if $p\nmid a_1^2-3a_2$ and $X=(a_1^2-3a_2)(3x+a_1)$, we have

$$x^3+a_1x^2+a_2x+a_3=\frac{1}{27a}(X^3-3aX-ab).$$

Hence $N_p(x^3+a_1x^2+a_2x+a_3)=N_p(x^3-3ax-ab)$. This proves (ii).

Finally consider (iii). If $p\nmid a_1^2-3a_2$, using Lemma 2.2 and the above we see that

$$N_p(x^3+a_1x^2+a_2x+a_3)=N_p(x^3-3ax-ab)=1$$
$$\Leftrightarrow\left(\frac{D}{p}\right)=\left(\frac{-3(b^2-4a)}{p}\right)=-1.$$

If $p \mid a_1^2 - 3a_2$, it follows from (2.8) that $N_p(x^3 + a_1x^2 + a_2x + a_3) = N_p(x^3 - b)$. But,

$$N_p(x^3 - b) = 1 \iff p \nmid b \quad \text{and} \quad p \equiv 2 \pmod 3 \iff \left(\frac{D}{p}\right) = \left(\frac{-3(b^2-4a)}{p}\right) = -1.$$

So $N_p(x^3 + a_1x^2 + a_2x + a_3) = 1$ if and only if $(\frac{D}{p}) = -1$. This proves (iii) and hence the proof is complete. □

Theorem 2.3. *Let $p > 3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}$, $a = (a_1^2 - 3a_2)^3$, $b = -2a_1^3 + 9a_1a_2 - 27a_3$, $p \nmid ab(b^2 - 4a)$ and $x_0 = \frac{1}{3}((a_1^2 - 3a_2)^{-(\frac{p}{3})} v_{(p+2(\frac{p}{3}))/3}(a, b) - a_1)$. Then the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$ has one and only one solution if and only if $x \equiv x_0 \pmod p$ is a solution of the congruence.*

Proof. Let $X_0 = a^{(p-(\frac{p}{3}))/3} v_{(p+2(\frac{p}{3}))/3}(a, b)$. Since $a^{(p-(\frac{p}{3}))/3} = (a_1^2 - 3a_2)^{p-(\frac{p}{3})} \equiv (a_1^2 - 3a_2)^{1-(\frac{p}{3})} \pmod p$ we see that

$$X_0 \equiv (a_1^2 - 3a_2)^{1-(\frac{p}{3})} v_{(p+2(\frac{p}{3}))/3}(a, b) = (a_1^2 - 3a_2)(3x_0 + a_1) \pmod p.$$

Applying Lemma 2.3 we get

$$x_0^3 + a_1x_0^2 + a_2x_0 + a_3 \equiv \frac{1}{27a}(X_0^3 - 3aX_0 - ab) \pmod p.$$

If $(\frac{D}{p}) = -1$, then $(\frac{-3(b^2-4a)}{p}) = (\frac{D}{p}) = -1$ since $b^2 - 4a = -27D$. In view of Lemma 2.2 we have $X_0^3 - 3aX_0 - ab \equiv 0 \pmod p$. So $x_0^3 + a_1x_0^2 + a_2x_0 + a_3 \equiv 0 \pmod p$ by the above.

If $(\frac{D}{p}) = 1$, then $(\frac{-3(b^2-4a)}{p}) = (\frac{D}{p}) = 1$. Suppose $k^2 \equiv -3(b^2 - 4a) \pmod p$ for $k \in \mathbb{Z}$. From (2.5) and Theorem 2.2 we see that

$$\begin{aligned} &2a^{(1-(\frac{p}{3}))/2} v_{(p+2(\frac{p}{3}))/3}(a, b) \\ &\quad = (b^2 - 4a)\left(\frac{p}{3}\right) u_{(p-(\frac{p}{3}))/3}(a, b) + b v_{(p-(\frac{p}{3}))/3}(a, b) \\ &\quad \equiv \begin{cases} 2(\frac{a}{p}) a^{(p-(\frac{p}{3}))/6} b \pmod p & \text{if } \frac{3b}{k} \in C_0(p), \\ (\pm k - b)(\frac{a}{p}) a^{(p-(\frac{p}{3}))/6} \pmod p & \text{if } \pm\frac{3b}{k} \in C_1(p). \end{cases} \end{aligned}$$

Observing that $a = (a_1^2 - 3a_2)^3$ and so

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

we then get

$$v_{\frac{p+2(\frac{p}{3})}{3}}(a,b)\equiv\begin{cases}(a_1^2-3a_2)^{(\frac{p}{3})-1}b\ (\mathrm{mod}\,p) & \text{if } \frac{3b}{k}\in C_0(p),\\ \frac{\pm k-b}{2}(a_1^2-3a_2)^{(\frac{p}{3})-1}\ (\mathrm{mod}\,p) & \text{if } \pm\frac{3b}{k}\in C_1(p).\end{cases}\tag{2.9}$$

Thus

$$X_0\equiv(a_1^2-3a_2)^{1-(\frac{p}{3})}v_{(p+2(\frac{p}{3}))/3}(a,b)\equiv b\quad\text{or}\quad(\pm k-b)/2\ (\mathrm{mod}\,p).$$

From this one can easily check that $X_0^3-3aX_0\equiv b^3-3ab\ (\mathrm{mod}\,p)$ and so $X_0^3-3aX_0-ab\equiv b(b^2-4a)\not\equiv 0\ (\mathrm{mod}\,p)$. Hence $x_0^3+a_1x_0^2+a_2x_0+a_3\not\equiv 0\ (\mathrm{mod}\,p)$.

By the above, $(\frac{D}{p})=-1$ if and only if $x_0^3+a_1x_0^2+a_2x_0+a_3\equiv 0\ (\mathrm{mod}\,p)$. This together with Lemma 2.3(iii) yields the result. □

3. Congruences for the third-order recurring sequences

Let $p>3$ be a prime, and $a_1,a_2,a_3\in\mathbb{Z}$. In this section we will determine $s_{p+1},s_{p+2},u_{p-2},u_{p-1},u_p\ (\mathrm{mod}\,p)$, where $\{s_n\}$ and $\{u_n\}$ are the third-order recurring sequences defined as below.

Definition 3.1. For $a_1,a_2,a_3\in\mathbb{Z}$ define the third-order linear recursive sequences $\{u_n(a_1,a_2,a_3)\}$ and $\{s_n(a_1,a_2,a_3)\}$ by

$$u_{-2}=u_{-1}=0,\quad u_0=1,\quad u_{n+3}+a_1u_{n+2}+a_2u_{n+1}+a_3u_n=0\ \ (n\geqslant -2)$$

and

$$s_0=3,\quad s_1=-a_1,\quad s_2=a_1^2-2a_2,\quad s_{n+3}+a_1s_{n+2}+a_2s_{n+1}+a_3s_n=0\ \ (n\geqslant 0).$$

Let $\{s_n\}$ and $\{u_n\}$ be given by the above, and let $x^3+a_1x^2+a_2x+a_3=(x-x_1)(x-x_2)(x-x_3)$. Then clearly

$$\begin{aligned}&\sum_{i=1}^3 x_i^{n+3}+a_1\sum_{i=1}^3 x_i^{n+2}+a_2\sum_{i=1}^3 x_i^{n+1}+a_3\sum_{i=1}^3 x_i^n\\&\quad=\sum_{i=1}^3 x_i^n(x_i^3+a_1x_i^2+a_2x_i+a_3)=0.\end{aligned}$$

Since $x_1^0+x_2^0+x_3^0=3$, $x_1+x_2+x_3=-a_1$ and

$$x_1^2+x_2^2+x_3^2=(x_1+x_2+x_3)^2-2(x_1x_2+x_1x_3+x_2x_3)=a_1^2-2a_2,$$

we see that

$$s_n = x_1^n + x_2^n + x_3^n \quad (n \geqslant 0). \tag{3.1}$$

From this and [16] we have

$$\sum_{k=1}^{n} s_k u_{n-k} = nu_n \quad \text{and} \quad s_n = -(a_1 u_{n-1} + 2a_2 u_{n-2} + 3a_3 u_{n-3}). \tag{3.2}$$

Lemma 3.1. *Let $p>3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}$, $a = (a_1^2 - 3a_2)^3$, $b = -2a_1^3 + 9a_1a_2 - 27a_3$, and let $s_n = s_n(a_1, a_2, a_3)$. Then*

$$s_{p+1} \equiv \frac{a_1^2}{3} + \frac{1}{3}(a_1^2 - 3a_2)^{\frac{1+(\frac{p}{3})}{2}} v_{\frac{p-(\frac{p}{3})}{3}}(a, b) \pmod p$$

and

$$s_{p+2} \equiv \frac{1}{9}\Big\{ 6a_1a_2 - 3a_1^3 + (a_1^2 - 3a_2)^{1-(\frac{p}{3})} v_{\frac{p+2(\frac{p}{3})}{3}}(a, b) - 2a_1(a_1^2 - 3a_2)^{\frac{1+(\frac{p}{3})}{2}} v_{\frac{p-(\frac{p}{3})}{3}}(a, b) \Big\} \pmod p.$$

Proof. Let x_1, x_2 and x_3 be the three roots of the equation $x^3 + a_1x^2 + a_2x + a_3 = 0$. Then $s_n = x_1^n + x_2^n + x_3^n$ $(n \geqslant 0)$ by (3.1). For $i = 1, 2, 3$ set $y_i = 3x_i + a_1$. Then y_1, y_2 and y_3 are the roots of the equation $y^3 - 3(a_1^2 - 3a_2)y - b = 0$ by (2.8), and

$$s_n = x_1^n + x_2^n + x_3^n = \frac{1}{3^n}\{(y_1 - a_1)^n + (y_2 - a_1)^n + (y_3 - a_1)^n\}.$$

Since y_1, y_2 and y_3 are algebraic integers we see that

$$(y_i - a_1)^p \equiv y_i^p - a_1^p \equiv y_i^p - a_1 \pmod p \quad \text{for } i = 1, 2, 3.$$

Hence, for $i = 1, 2, 3$ we have

$$(y_i - a_1)^{p+1} \equiv (y_i - a_1)(y_i^p - a_1) = y_i^{p+1} - a_1y_i^p - a_1y_i + a_1^2 \pmod p$$

and

$$\begin{aligned}(y_i - a_1)^{p+2} &\equiv (y_i^2 - 2a_1y_i + a_1^2)(y_i^p - a_1) \\ &= y_i^{p+2} - 2a_1y_i^{p+1} + a_1^2y_i^p - a_1y_i^2 + 2a_1^2y_i - a_1^3 \pmod p.\end{aligned}$$

Observing that

$$y_1+y_2+y_3=0,\quad y_1^p+y_2^p+y_3^p\equiv(y_1+y_2+y_3)^p=0\ (\mathrm{mod}\ p)$$

and

$$\begin{aligned}y_1^2+y_2^2+y_3^2&=(y_1+y_2+y_3)^2-2(y_1y_2+y_1y_3+y_2y_3)\\&=0-2\cdot(-3(a_1^2-3a_2))=6(a_1^2-3a_2),\end{aligned}$$

by the above we get

$$\begin{aligned}s_{p+1}&=\frac{1}{3^{p+1}}\sum_{i=1}^3(y_i-a_1)^{p+1}\\&\equiv\frac{1}{9}\left(\sum_{i=1}^3y_i^{p+1}-a_1\sum_{i=1}^3y_i^p-a_1\sum_{i=1}^3y_i+3a_1^2\right)\\&\equiv\frac{1}{9}(y_1^{p+1}+y_2^{p+1}+y_3^{p+1}+3a_1^2)\ (\mathrm{mod}\ p)\end{aligned}$$

and so

$$\begin{aligned}s_{p+2}&=\frac{1}{3^{p+2}}\sum_{i=1}^3(y_i-a_1)^{p+2}\\&\equiv\frac{1}{27}\sum_{i=1}^3(y_i^{p+2}-2a_1y_i^{p+1}+a_1^2y_i^p-a_1y_i^2+2a_1^2y_i-a_1^3)\\&\equiv\frac{1}{27}(y_1^{p+2}+y_2^{p+2}+y_3^{p+2}-2a_1(9s_{p+1}-3a_1^2)-\ 6a_1(a_1^2-3a_2)-3a_1^3)\\&=\frac{1}{27}(y_1^{p+2}+y_2^{p+2}+y_3^{p+2}-18a_1s_{p+1}+18a_1a_2-3a_1^3)\ (\mathrm{mod}\ p).\end{aligned}$$

Let $t=(b+\sqrt{b^2-4a})/2$ and $u=(b-\sqrt{b^2-4a})/2$. Then $t+u=b$ and $tu=a=-\frac{1}{27}(-3(a_1^2-3a_2))^3$. From the theory of cubic equations we know that $\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k}$ $(k=0,1,2)$ are the three roots of the equation $y^3-3(a_1^2-3a_2)y-b=0$. So, by the above,

$$s_{p+1}\equiv\frac{1}{9}(y_1^{p+1}+y_2^{p+1}+y_3^{p+1}+3a_1^2)=\frac{a_1^2}{3}+\frac{1}{9}\sum_{k=0}^2(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^{p+1}\ (\mathrm{mod}\ p)$$

and

$$s_{p+2}\equiv\frac{1}{27}\left(\sum_{k=0}^{2}(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^{p+2}-18a_1s_{p+1}+18a_1a_2-3a_1^3\right)\pmod p.$$

Since $\sqrt[3]{t}, \sqrt[3]{t}\omega, \sqrt[3]{t}\omega^2, \sqrt[3]{u}, \sqrt[3]{u}\omega, \sqrt[3]{u}\omega^2$ are the roots of the equation $x^6-bx^3+a=0$, we see that they are all algebraic integers. Hence,

$$\begin{aligned}&(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^{p+1}\\&\quad\equiv(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})((\sqrt[3]{t}\omega^k)^p+(\sqrt[3]{u}\omega^{2k})^p)\\&\quad=(\sqrt[3]{t})^{p+1}\omega^{k(p+1)}+(\sqrt[3]{u})^{p+1}\omega^{2k(p+1)}\\&\qquad+\sqrt[3]{tu}((\sqrt[3]{t})^{p-1}\omega^{k(p-1)}+(\sqrt[3]{u})^{p-1}\omega^{2k(p-1)})\pmod p\end{aligned}$$

and

$$\begin{aligned}&(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^{p+2}\\&\quad\equiv(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^2((\sqrt[3]{t}\omega^k)^p+(\sqrt[3]{u}\omega^{2k})^p)\\&\quad=(\sqrt[3]{t})^{p+2}\omega^{k(p+2)}+2\sqrt[3]{tu}(\sqrt[3]{t})^p\omega^{kp}+(\sqrt[3]{t})^p(\sqrt[3]{u})^2\omega^{k(p+1)}\\&\qquad+(\sqrt[3]{t})^2(\sqrt[3]{u})^p\omega^{2k(p+1)}+2\sqrt[3]{tu}(\sqrt[3]{u})^p\omega^{2kp}+(\sqrt[3]{u})^{p+2}\omega^{2k(p+2)}\pmod p.\end{aligned}$$

Observing that $\sqrt[3]{tu}=\sqrt[3]{a}=a_1^2-3a_2$, $t^n+u^n=v_n(a,b)$ and $1+\omega+\omega^2=0$, by the above we obtain

$$\begin{aligned}&\sum_{k=0}^{2}(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^{p+1}\\&\quad\equiv((\sqrt[3]{t})^{p+1}+(\sqrt[3]{u})^{p+1})(1+\omega^{p+1}+\omega^{2(p+1)})\\&\qquad+(a_1^2-3a_2)((\sqrt[3]{t})^{p-1}+(\sqrt[3]{u})^{p-1})(1+\omega^{p-1}+\omega^{2(p-1)})\\&\quad=3(a_1^2-3a_2)^{(1+(\frac{p}{3}))/2}((\sqrt[3]{t})^{p-(\frac{p}{3})}+(\sqrt[3]{u})^{p-(\frac{p}{3})})\\&\quad=3(a_1^2-3a_2)^{(1+(\frac{p}{3}))/2}v_{\frac{p-(\frac{p}{3})}{3}}(a,b)\pmod p\end{aligned}$$

and

$$\begin{aligned}
&\sum_{k=0}^{2}(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^{p+2}\\
&\quad\equiv\sum_{k=0}^{2}\{(\sqrt[3]{t})^{p+2}\omega^{k(p+2)}+(\sqrt[3]{u})^{p+2}\omega^{2k(p+2)}\\
&\qquad+(\sqrt[3]{tu})^2((\sqrt[3]{u})^{p-2}\omega^{k(2p+2)}+(\sqrt[3]{t})^{p-2}\omega^{k(p+1)})\}\\
&\quad=3(a_1^2-3a_2)^{1-(\frac{p}{3})}((\sqrt[3]{t})^{p+2(\frac{p}{3})}+(\sqrt[3]{u})^{p+2(\frac{p}{3})})\\
&\quad=3(a_1^2-3a_2)^{1-(\frac{p}{3})}v_{\frac{p+2(\frac{p}{3})}{3}}(a,b)\pmod p.
\end{aligned}$$

Therefore

$$\begin{aligned}
s_{p+1}&\equiv\frac{a_1^2}{3}+\frac{1}{9}\sum_{k=0}^{2}(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^{p+1}\\
&\equiv\frac{a_1^2}{3}+\frac{1}{3}(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}v_{\frac{p-(\frac{p}{3})}{3}}(a,b)\pmod p
\end{aligned}$$

and so

$$\begin{aligned}
s_{p+2}&\equiv\frac{1}{27}\left(\sum_{k=0}^{2}(\sqrt[3]{t}\omega^k+\sqrt[3]{u}\omega^{2k})^{p+2}-18a_1s_{p+1}+18a_1a_2-3a_1^3\right)\\
&\equiv\frac{1}{9}\left\{(a_1^2-3a_2)^{1-(\frac{p}{3})}v_{\frac{p+2(\frac{p}{3})}{3}}(a,b)-2a_1(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}v_{\frac{p-(\frac{p}{3})}{3}}(a,b)\right.\\
&\qquad\left.+6a_1a_2-3a_1^3\right\}\pmod p.
\end{aligned}$$

This completes the proof. □

Now we can prove

Theorem 3.1. *Let* $p>3$ *be a prime,* $a_1,a_2,a_3\in\mathbb{Z}$, $a=(a_1^2-3a_2)^3$, $b=-2a_1^3+9a_1a_2-27a_3$, $D=-\frac{1}{27}(b^2-4a)=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$, *and* $s_n=s_n(a_1,a_2,a_3)$. *Then*

(i) $s_p\equiv-a_1\pmod p$.

(ii) *If* $(\frac{D}{p})=-1$ *and so* $x^3+a_1x^2+a_2x+a_3\equiv 0\,(\mathrm{mod}\,p)$ *for some integer* x, *then*

$$s_{p+1}\equiv 3x^2+2a_1x+2a_2\,(\mathrm{mod}\,p)\quad\text{and}\quad s_{p+2}\equiv -2a_1x^2-(a_1^2+a_2)x-a_1a_2\,(\mathrm{mod}\,p).$$

(iii) *If* $(\frac{D}{p})=0$ *or* 1 *and so* $d^2\equiv D\,(\mathrm{mod}\,p)$ *for some* $d\in\mathbb{Z}$, *then*

$$s_{p+1}\equiv\begin{cases}a_1^2-2a_2\,(\mathrm{mod}\,p) & \text{if } p\mid D \text{ or } \frac{b}{3d}\in C_0(p),\\ a_2\,(\mathrm{mod}\,p) & \text{if } p\nmid D \text{ and } \frac{b}{3d}\notin C_0(p)\end{cases}$$

and

$$s_{p+2}\equiv\begin{cases}-a_1^3+3a_1a_2-3a_3\,(\mathrm{mod}\,p) & \text{if } p\mid D \text{ or } \frac{b}{3d}\in C_0(p),\\ \frac{1}{2}(\pm d-a_1a_2+3a_3)\,(\mathrm{mod}\,p) & \text{if } p\nmid aD \text{ and } \pm\frac{b}{3d}\in C_1(p),\\ \frac{1}{9}(-a_1^3+b^{\frac{p+2}{3}})\,(\mathrm{mod}\,p) & \text{if } p\mid a \text{ and } p\nmid D.\end{cases}$$

Proof. Suppose $x^3+a_1x^2+a_2x+a_3=(x-x_1)(x-x_2)(x-x_3)$. From (3.1) we know that $s_n=x_1^n+x_2^n+x_3^n$ for $n\geqslant 0$. Since x_1,x_2,x_3 are all algebraic integers and $x_1+x_2+x_3=-a_1$ we see that

$$s_p=x_1^p+x_2^p+x_3^p\equiv(x_1+x_2+x_3)^p=(-a_1)^p\equiv -a_1\,(\mathrm{mod}\,p).$$

This proves (i).

Now consider (ii). Suppose $(\frac{D}{p})=-1$. Then $N_p(x^3+a_1x^2+a_2x+a_3)=1$ by Lemma 2.3. Let x be an integer such that $x^3+a_1x^2+a_2x+a_3\equiv 0\,(\mathrm{mod}\,p)$. We claim that $(a_1^2-3a_2)^{(1+(\frac{p}{3}))/2}\,v_{(p-(\frac{p}{3}))/3}(a,b)\equiv 9x^2+6a_1x-a_1^2+6a_2\,(\mathrm{mod}\,p)$. If $p\nmid a$ and $X=(a_1^2-3a_2)(3x+a_1)$, then $X^3-3aX-ab\equiv 0\,(\mathrm{mod}\,p)$ by Lemma 2.3. Using Theorem 2.1 we see that

$$\begin{aligned}&(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}\,v_{(p-(\frac{p}{3}))/3}(a,b)\\ &\quad\equiv(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}\cdot\left(\frac{a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}-1}(X^2-2a)\\ &\quad\equiv(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}(a_1^2-3a_2)^{\frac{-5-(\frac{p}{3})}{2}}((a_1^2-3a_2)^2(3x+a_1)^2-2(a_1^2-3a_2)^3)\\ &\quad\equiv(3x+a_1)^2-2(a_1^2-3a_2)=9x^2+6a_1x-a_1^2+6a_2\,(\mathrm{mod}\,p).\end{aligned}$$

If $p\mid a$, then $v_n(a,b)\equiv b^n\,(\mathrm{mod}\,p)$ by (2.3). Since $(\frac{p}{3})=(\frac{-3}{p})=-(\frac{-27D}{p})=-(\frac{b^2-4a}{p})=-(\frac{b^2}{p})=-1$ we find $p\equiv 2\,(\mathrm{mod}\,3)$. Using (2.8) we see that $(3x+a_1)^3\equiv b\,(\mathrm{mod}\,p)$

and hence $x\equiv(b^{\frac{2p-1}{3}}-a_1)/3 \pmod p$. From this we get

$$\begin{aligned}&9x^2+6a_1x-a_1^2+6a_2\\&\quad\equiv 9x^2+6a_1x+3a_2\\&\quad\equiv (b^{\frac{2p-1}{3}}-a_1)^2+2a_1(b^{\frac{2p-1}{3}}-a_1)+3a_2\\&\quad\equiv b^{\frac{4p-2}{3}}\equiv b^{\frac{p+1}{3}}\equiv v_{(p+1)/3}(a,b)\pmod p.\end{aligned}$$

So the claim is also true when $p\mid a$.

Now, by the claim and Lemma 3.1 we have

$$\begin{aligned}s_{p+1}&\equiv\tfrac13(a_1^2+(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}v_{(p-(\frac{p}{3}))/3}(a,b))\\&\equiv\tfrac13(a_1^2+9x^2+6a_1x-a_1^2+6a_2)=3x^2+2a_1x+2a_2\pmod p.\end{aligned}$$

On the other hand, if $p\nmid a$, it follows from Lemma 2.2 that

$$\begin{aligned}&(a_1^2-3a_2)^{1-(\frac{p}{3})}v_{\frac{p+2(\frac{p}{3})}{3}}(a,b)\\&\quad\equiv(a_1^2-3a_2)^{1-(\frac{p}{3})}\cdot a^{-(p-(\frac{p}{3}))/3}X\\&\quad=(a_1^2-3a_2)^{1-(\frac{p}{3})-(p-(\frac{p}{3}))}\cdot(a_1^2-3a_2)(3x+a_1)\\&\quad\equiv(a_1^2-3a_2)(3x+a_1)\pmod p.\end{aligned}$$

This is also true when $p\mid a$ since $p\equiv 2 \pmod 3$. So, by Lemma 3.1 and the above we get

$$\begin{aligned}s_{p+2}&\equiv\tfrac19\{(a_1^2-3a_2)^{1-(\frac{p}{3})}v_{\frac{p+2(\frac{p}{3})}{3}}(a,b)\\&\quad-2a_1(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}v_{\frac{p-(\frac{p}{3})}{3}}(a,b)+6a_1a_2-3a_1^3\}\\&\equiv\tfrac19\{(a_1^2-3a_2)(3x+a_1)-2a_1(9x^2+6a_1x-a_1^2+6a_2)+6a_1a_2-3a_1^3\}\\&=-(2a_1x^2+(a_1^2+a_2)x+a_1a_2)\pmod p.\end{aligned}$$

This proves (ii).

Let us consider (iii). Suppose $d^2 \equiv D \pmod p$ for $d \in \mathbb{Z}$. If $p \mid D$, then $b^2 \equiv 4a \pmod p$ and so $(\frac{a}{p}) = 0$ or 1 since $b^2 - 4a = -27D$. Using (2.3) we see that

$$\begin{aligned} v_n(a,b) &\equiv 2\left(\frac{b}{2}\right)^n \\ &= \begin{cases} (\frac{b^2}{4})^{(n-1)/2} b \equiv a^{(n-1)/2} b \pmod p & \text{if } 2 \nmid n, \\ 2(\frac{b^2}{4})^{n/2} \equiv 2a^{n/2} \pmod p & \text{if } 2 \mid n. \end{cases} \end{aligned}$$

Thus, by Lemma 3.1 we have

$$\begin{aligned} s_{p+1} &\equiv \frac{1}{3}\left(a_1^2 + (a_1^2 - 3a_2)^{\frac{1+(\frac{p}{3})}{2}} \cdot 2a^{\frac{p-(\frac{p}{3})}{6}}\right) \\ &= \frac{1}{3}(a_1^2 + 2(a_1^2 - 3a_2)^{\frac{p+1}{2}}) \\ &\equiv \frac{1}{3}\left(a_1^2 + 2(a_1^2 - 3a_2)\left(\frac{a}{p}\right)\right) \equiv a_1^2 - 2a_2 \pmod p \end{aligned}$$

and

$$\begin{aligned} s_{p+2} &\equiv \frac{1}{9}\{(a_1^2 - 3a_2)^{1-(\frac{p}{3})} a^{\frac{p+2(\frac{p}{3})-3}{6}} b \\ &\quad - 2a_1(a_1^2 - 3a_2)^{\frac{1+(\frac{p}{3})}{2}} \cdot 2a^{\frac{p-(\frac{p}{3})}{6}}\} + \frac{2a_1a_2 - a_1^3}{3} \\ &= \frac{1}{9}(b - 4a_1(a_1^2 - 3a_2))(a_1^2 - 3a_2)^{\frac{p-1}{2}} + \frac{1}{3}(2a_1a_2 - a_1^3) \\ &\equiv \frac{1}{3}\left\{(-2a_1^3 + 7a_1a_2 - 9a_3)\left(\frac{a}{p}\right) + 2a_1a_2 - a_1^3\right\} \\ &\equiv -a_1^3 + 3a_1a_2 - 3a_3 \pmod p. \end{aligned}$$

(noting that $p \mid b$ when $p \mid a$).

If $p \mid a$ and $p \nmid D$, then $(\frac{p}{3}) = (\frac{-3}{p}) = (\frac{-27D}{p}) = (\frac{b^2-4a}{p}) = (\frac{b^2}{p}) = 1$ and so $p \equiv 1 \pmod 3$. Since $v_n(a,b) \equiv b^n \pmod p$ by (2.3), it follows from Lemma 3.1 that

$$s_{p+1} \equiv \frac{1}{3}\{a_1^2 + (a_1^2 - 3a_2)v_{\frac{p-1}{3}}(a,b)\} \equiv \frac{a_1^2}{3} \equiv a_2 \pmod p$$

and

$$s_{p+2} \equiv \tfrac{1}{9}\{v_{\frac{p+2}{3}}(a,b) + 6a_1a_2 - 3a_1^3\} \equiv \tfrac{1}{9}(b^{\frac{p+2}{3}} - a_1^3) \pmod p.$$

If $p\nmid aD$, then $(\frac{b}{3d})^2+3\equiv\frac{b^2+27D}{9D}=\frac{4a}{9D}\not\equiv 0\pmod p$. Thus, $b/(3d)\in C_0(p)\cup C_1(p)\cup C_2(p)$. Since $(9d)^2\equiv 81D\equiv -3(b^2-4a)\pmod p$ we see that $(\frac{-3(b^2-4a)}{p})=1$.

Noting that $(a_1^2-3a_2)^{(1+(\frac{p}{3}))/2}(\frac{a}{p})a^{\frac{p-(\frac{p}{3})}{6}}=(\frac{a_1^2-3a_2}{p})(a_1^2-3a_2)^{\frac{p+1}{2}}\equiv a_1^2-3a_2\pmod p$ and then applying Theorem 2.2 we get

$$(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}v_{\frac{p-(\frac{p}{3})}{3}}(a,b)\equiv\begin{cases}2(a_1^2-3a_2)\pmod p & \text{if } \frac{b}{3d}\in C_0(p),\\ -(a_1^2-3a_2)\pmod p & \text{if } \frac{b}{3d}\notin C_0(p).\end{cases}$$

So, by Lemma 3.1 we have

$$s_{p+1}\equiv\begin{cases}\frac{1}{3}\{a_1^2+2(a_1^2-3a_2)\}=a_1^2-2a_2\pmod p & \text{if } \frac{b}{3d}\in C_0(p),\\ \frac{1}{3}\{a_1^2-(a_1^2-3a_2)\}=a_2\pmod p & \text{if } \frac{b}{3d}\notin C_0(p).\end{cases}$$

On the other hand, putting $k=9d$ in (2.9) we find

$$v_{\frac{p+2(\frac{p}{3})}{3}}(a,b)\equiv\begin{cases}(a_1^2-3a_2)^{(\frac{p}{3})-1}b\pmod p & \text{if } \frac{b}{3d}\in C_0(p),\\ \frac{\pm 9d-b}{2}(a_1^2-3a_2)^{(\frac{p}{3})-1}(\mathrm{mod}\ p) & \text{if } \pm\frac{b}{3d}\in C_1(p).\end{cases}$$

Thus, by the above and Lemma 3.1 we obtain

$$\begin{aligned}s_{p+2}\equiv&\frac{1}{9}\{(a_1^2-3a_2)^{1-(\frac{p}{3})}v_{\frac{p+2(\frac{p}{3})}{3}}(a,b)\\&-2a_1(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}v_{\frac{p-(\frac{p}{3})}{3}}(a,b)+6a_1a_2-3a_1^3\}\\\equiv&\begin{cases}\frac{1}{9}\{b-2a_1\cdot 2(a_1^2-3a_2)+6a_1a_2-3a_1^3\}\pmod p & \text{if } \frac{b}{3d}\in C_0(p),\\ \frac{1}{9}\{\frac{\pm 9d-b}{2}+2a_1(a_1^2-3a_2)+6a_1a_2-3a_1^3\}\pmod p & \text{if } \pm\frac{b}{3d}\in C_1(p)\end{cases}\\\equiv&\begin{cases}-a_1^3+3a_1a_2-3a_3\pmod p & \text{if } \frac{b}{3d}\in C_0(p),\\ \frac{\pm d-a_1a_2+3a_3}{2}\pmod p & \text{if } \pm\frac{b}{3d}\in C_1(p).\end{cases}\end{aligned}$$

This completes the proof. □

Lemma 3.2. *For $a_1,a_2,a_3\in\mathbb{Z}$ let $D=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$, $u_n=u_n(a_1,a_2,a_3)$ and $s_n=s_n(a_1,a_2,a_3)$.*

(i) *For $n\geqslant -2$ we have*

$$Du_n=(2a_1^2-6a_2)s_{n+4}+(2a_1^3-7a_1a_2+9a_3)s_{n+3}+(a_1^2a_2-4a_2^2+3a_1a_3)s_{n+2}.$$

(ii) *For $n\geqslant -1$ we have*

$$Du_n=(9a_3-a_1a_2)s_{n+3}+(-a_1^2a_2+2a_2^2+3a_1a_3)s_{n+2}+(-2a_1^2a_3+6a_2a_3)s_{n+1}.$$

(iii) *For* $n\geqslant 0$ *we have*

$$Du_n=(2a_2^2-6a_1a_3)s_{n+2}+(a_1a_2^2-2a_1^2a_3-3a_2a_3)s_{n+1}+(a_1a_2a_3-9a_3^2)s_n.$$

Proof. For $n\geqslant -2$ let $U_n=Du_n$ and

$$U_n'=(2a_1^2-6a_2)s_{n+4}+(2a_1^3-7a_1a_2+9a_3)s_{n+3}+(a_1^2a_2-4a_2^2+3a_1a_3)s_{n+2}.$$

Then clearly

$$U_{n+3}+a_1U_{n+2}+a_2U_{n+1}+a_3U_n=0\quad\text{and}$$

$$U'_{n+3}+a_1U'_{n+2}+a_2U'_{n+1}+a_3U'_n=0.$$

Since

$$u_{-2}=u_{-1}=0,\quad u_0=1,\quad s_0=3,\quad s_1=-a_1,\quad s_2=a_1^2-2a_2,$$

$$s_3=-a_1^3+3a_1a_2-3a_3\quad\text{and}\quad s_4=a_1^4-4a_1^2a_2+2a_2^2+4a_1a_3,$$

one can easily verify the following facts:

$$U'_{-2}=0=U_{-2},\quad U'_{-1}=0=U_{-1},\quad U'_0=D=U_0.$$

So $U_n=U_n'$ for $n\geqslant -2$. This proves (i).

Now consider (ii). Since $s_{n+4}=-(a_1s_{n+3}+a_2s_{n+2}+a_3s_{n+1})$, replacing s_{n+4} by $-(a_1s_{n+3}+a_2s_{n+2}+a_3s_{n+1})$ in (i) we get (ii).

Part (iii) follows from (ii) and the fact that $s_{n+3}=-(a_1s_{n+2}+a_2s_{n+1}+a_3s_n)$. □

Theorem 3.2. *Let* $p>3$ *be a prime*, $a_1,a_2,a_3\in\mathbb{Z}$, $a=(a_1^2-3a_2)^3$, $b=-2a_1^3+9a_1a_2-27a_3$ *and* $D=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3\not\equiv 0\pmod p$. *Then*

(i) $u_{p-2}(a_1,a_2,a_3)\equiv 3(3a_2-a_1^2)^{(1+(\frac{p}{3}))/2}u_{(p-(\frac{p}{3}))/3}(a,b)\pmod p$.

(ii) *If* $(\frac{D}{p})=-1$, *then*

$$u_{p-2}(a_1,a_2,a_3)\equiv\begin{cases}-3b/(a_1^2-3a_2)^2\pmod p & \text{if } p\mid b^2-2a,\\ x\pmod p & \text{if } p\nmid b^2-2a,\end{cases}$$

where $x\pmod p$ *is the unique solution of the congruence* $Dx^3-(a_1^2-3a_2)^2x+b\equiv 0\pmod p$.

(iii) *If* $(\frac{D}{p})=1$ *and so* $d^2\equiv D\pmod p$ *for some integer* d, *then*

$$u_{p-2}(a_1,a_2,a_3)\equiv\begin{cases}0\pmod p & \text{if } p\mid a \text{ or } \frac{b}{3d}\in C_0(p),\\ \pm\frac{a_1^2-3a_2}{d}\pmod p & \text{if } \pm\frac{b}{3d}\in C_1(p).\end{cases}$$

Proof. Let $s_n = s_n(a_1, a_2, a_3)$ and $v_n = v_n(a, b)$. It follows from Lemma 3.2 that

$$u_{p-2}(a_1, a_2, a_3)$$
$$= \frac{1}{D}\{2(a_1^2 - 3a_2)s_{p+2} + (2a_1^3 - 7a_1a_2 + 9a_3)s_{p+1} + (a_1^2a_2 - 4a_2^2 + 3a_1a_3)s_p\}. \quad (3.3)$$

Since $b^2 - 4a = -27D$ and $s_p \equiv -a_1 \pmod p$ by Theorem 3.1, using (3.3), Lemma 3.1 and (2.5) we obtain

$$\begin{aligned} u_{p-2}(a_1, a_2, a_3) &\equiv \frac{1}{9D}\left\{2(a_1^2 - 3a_2)^{2-(\frac{p}{3})}v_{\frac{p+2(\frac{p}{3})}{3}} - (a_1^2 - 3a_2)^{\frac{1+(\frac{p}{3})}{2}}bv_{\frac{p-(\frac{p}{3})}{3}}\right\} \\ &= \frac{1}{9D}(a_1^2 - 3a_2)^{\frac{1+(\frac{p}{3})}{2}}(b^2 - 4a)\left(\frac{p}{3}\right)u_{\frac{p-(\frac{p}{3})}{3}}(a, b) \\ &= 3(3a_2 - a_1^2)^{\frac{1+(\frac{p}{3})}{2}}u_{\frac{p-(\frac{p}{3})}{3}}(a, b) \pmod p. \end{aligned}$$

This proves (i).

Now consider (ii). Suppose $(\frac{D}{p}) = -1$. Since $a = (a_1^2 - 3a_2)^3$ it is easy to see that

$$(3a_2 - a_1^2)^{\frac{1+(\frac{p}{3})}{2}} \cdot \left(\frac{-3a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}} \equiv -(a_1^2 - 3a_2) \pmod p. \quad (3.4)$$

If $p \mid b^2 - 2a$, then $p \nmid ab$ since $b^2 - 4a = -27D \not\equiv 0 \pmod p$. From (i), Corollary 2.1 and (3.4) we see that

$$\begin{aligned} u_{p-2}(a_1, a_2, a_3) &\equiv 3(3a_2 - a_1^2)^{(1+(\frac{p}{3}))/2} \cdot \left(\frac{-3a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}-1}b \\ &\equiv -\frac{3b}{(a_1^2 - 3a_2)^2} \pmod p. \end{aligned}$$

If $p \nmid a(b^2 - 2a)$, by (i), Corollary 2.1 and (3.4) we have

$$\begin{aligned} &u_{p-2}(a_1, a_2, a_3) \\ &\equiv 3(3a_2 - a_1^2)^{(1+(\frac{p}{3}))/2} \cdot \left(\frac{-3a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}-1}(b^2 - 4a)^{-1}t(a, b) \\ &\equiv -\frac{3t(a, b)}{(a_1^2 - 3a_2)^2(b^2 - 4a)} = \frac{t(a, b)}{9D(a_1^2 - 3a_2)^2} \pmod p, \end{aligned}$$

where $t(a,b) \pmod p$ is the unique solution of the congruence $t^3+3a^2(b^2-4a)t+a^2b(b^2-4a)^2 \equiv 0 \pmod p$. Let $t=9D(a_1^2-3a_2)^2x$. Using the fact that $b^2-4a=-27D$ we find $t^3+3a^2(b^2-4a)t+a^2b(b^2-4a)^2=(27aD)^2(Dx^3-(a_1^2-3a_2)^2x+b)$. So $z \equiv t(a,b)/(9D(a_1^2-3a_2)^2) \equiv u_{p-2}(a_1,a_2,a_3) \pmod p$ is the unique solution of the congruence $Dx^3-(a_1^2-3a_2)^2x+b \equiv 0 \pmod p$.

If $p \mid a$, then $p \nmid b$ and $(\frac{p}{3})=(\frac{-3}{p})=-(\frac{-27D}{p})=-(\frac{b^2-4a}{p})=-(\frac{b^2}{p})=-1$. So $p \equiv 2 \pmod 3$ and hence $N_p(Dx^3-(a_1^2-3a_2)^2x+b)=N_p(Dx^3+b)=1$. From (i) and the fact that $b^2-4a \equiv b^2 \pmod p$ we see that

$$u_{p-2}(a_1,a_2,a_3) \equiv 3u_{\frac{p+1}{3}}(a,b) \equiv \frac{3}{b}\left\{\left(\frac{b+b}{2}\right)^{\frac{p+1}{3}}-\left(\frac{b-b}{2}\right)^{\frac{p+1}{3}}\right\}$$
$$=3b^{\frac{p-2}{3}} \pmod p.$$

This together with the fact that $27D=4a-b^2 \equiv -b^2 \pmod p$ yields

$$D(u_{p-2}(a_1,a_2,a_3))^3+b \equiv D(3b^{\frac{p-2}{3}})^3+b \equiv b-b^p \equiv 0 \pmod p.$$

So $x \equiv u_{p-2}(a_1,a_2,a_3) \pmod p$ is also the unique solution of the congruence $Dx^3-(a_1^2-3a_2)^2x+b \equiv 0 \pmod p$ when $p \mid a$.

By the above, (ii) is true. Now consider (iii). Suppose $(\frac{D}{p})=1$ and $d^2 \equiv D \pmod p$. Since $b^2-4a=-27D$ we have $(9d)^2 \equiv 81D=-3(b^2-4a) \pmod p$. If $p \mid a$, then $(\frac{p}{3})=(\frac{-3}{p})=(\frac{-27D}{p})=(\frac{b^2-4a}{p})=(\frac{b^2}{p})=1$ and so $p \equiv 1 \pmod 3$. Thus $u_{p-2}(a_1,a_2,a_3) \equiv 0 \pmod p$ by (i). If $p \nmid a$, using (i), (3.4) and taking $k=9d$ in Theorem 2.2 we get

$$u_{p-2}(a_1,a_2,a_3)$$
$$\equiv 3(3a_2-a_1^2)^{(1+(\frac{p}{3}))/2}u_{(p-(\frac{p}{3}))/3}(a,b)$$
$$\equiv \begin{cases} 0 \pmod p & \text{if } \frac{b}{3d} \in C_0(p), \\ 3(3a_2-a_1^2)^{\frac{1+(\frac{p}{3})}{2}} \cdot \frac{+9d}{-27D}(\frac{-3a}{p})a^{\frac{p-(\frac{p}{3})}{6}} \equiv \pm\frac{a_1^2-3a_2}{d} \pmod p & \text{if } \pm\frac{b}{3d} \in C_1(p). \end{cases}$$

This proves (iii) and hence the proof is complete.

Using Lemma 3.2 and Theorem 3.1 one can easily prove

Theorem 3.3. *Let $p>3$ be a prime, $a_1,a_2,a_3 \in \mathbb{Z}$, $a=(a_1^2-3a_2)^3$, $b=-2a_1^3+9a_1a_2-27a_3$ and $D=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3 \not\equiv 0 \pmod p$.*

(i) *If $(\frac{D}{p})=-1$, then*

$$u_{p-1}(a_1,a_2,a_3) \equiv \frac{1}{D}\{(-a_1^2a_2+6a_2^2-9a_1a_3)x^2-(a_1^3a_2-5a_1a_2^2+3a_1^2a_3+9a_2a_3)x$$
$$-a_1^2a_2^2+4a_2^3+2a_1^3a_3-9a_1a_2a_3\} \pmod p$$

and

$$u_p(a_1,a_2,a_3)\equiv\frac{1}{D}\{(-a_1a_2^2+6a_1^2a_3-9a_2a_3)x^2+(-2a_2^3+2a_1^3a_3)x + a_1^2a_2a_3+9a_1a_3^2-6a_2^2a_3\}\ (\mathrm{mod}\ p),$$

where $x\ (\mathrm{mod}\ p)$ *is the unique solution of the congruence* $x^3+a_1x^2+a_2x+a_3\equiv 0\ (\mathrm{mod}\ p)$.

(ii) If $(\frac{D}{p})=1$ *and so* $d^2\equiv D\ (\mathrm{mod}\ p)$ *for some integer* d, *then*

$$u_{p-1}(a_1,a_2,a_3)\equiv\begin{cases} b^{\frac{p-1}{3}}\ (\mathrm{mod}\ p) & \text{if } p\mid a,\\ 1\ (\mathrm{mod}\ p) & \text{if } \frac{b}{3d}\in C_0(p),\\ \frac{-d\pm(9a_3-a_1a_2)}{2d}\ (\mathrm{mod}\ p) & \text{if } \pm\frac{b}{3d}\in C_1(p)\end{cases}$$

and

$$u_p(a_1,a_2,a_3)\equiv\begin{cases} -\frac{a_1}{3}\,(1+2b^{\frac{p-1}{3}})\ (\mathrm{mod}\ p) & \text{if } p\mid a,\\ -a_1\ (\mathrm{mod}\ p) & \text{if } \frac{b}{3d}\in C_0(p),\\ \pm\frac{a_2^2-3a_1a_3}{d}\ (\mathrm{mod}\ p) & \text{if } \pm\frac{b}{3d}\in C_1(p).\end{cases}$$

From Theorems 3.1–3.3 we have the following result.

Theorem 3.4. *For given integer* k *let* $p>3$ *be a prime such that* $p\nmid k^2+3$. *Then*

(a) $$u_{p-2}(-3k,-9,3k)\equiv\begin{cases}0\ (\mathrm{mod}\ p) & \text{if } k\in C_0(p),\\ \frac{p\pm1}{2}\ (\mathrm{mod}\ p) & \text{if } \pm k\in C_1(p),\end{cases}$$

(b) $$u_{p-1}(-3k,-9,3k)\equiv\begin{cases}1\ (\mathrm{mod}\ p) & \text{if } k\in C_0(p),\\ \frac{p-1}{2}\ (\mathrm{mod}\ p) & \text{if } \pm k\in C_1(p),\end{cases}$$

(c) $$u_p(-3k,-9,3k)\equiv\begin{cases}3k\ (\mathrm{mod}\ p) & \text{if } k\in C_0(p),\\ \frac{p\pm3}{2}\ (\mathrm{mod}\ p) & \text{if } \pm k\in C_1(p),\end{cases}$$

(d) $$s_{p+1}(-3k,-9,3k)\equiv\begin{cases}9k^2+18\ (\mathrm{mod}\ p) & \text{if } k\in C_0(p),\\ -9\ (\mathrm{mod}\ p) & \text{if } \pm k\in C_1(p),\end{cases}$$

(e) $$s_{p+2}(-3k,-9,3k)\equiv\begin{cases}27k^3+72k\ (\mathrm{mod}\ p) & \text{if } k\in C_0(p),\\ \pm9(k^2+3)-9k\ (\mathrm{mod}\ p) & \text{if } \pm k\in C_1(p).\end{cases}$$

Proof. Let $a_1=-3k$, $a_2=-9$ and $a_3=3k$. Then

$$a_1^2-3a_2=9(k^2+3),\quad -2a_1^3+9a_1a_2-27a_3=54k(k^2+3),$$

$$a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3=(18(k^2+3))^2.$$

So the result follows immediately from Theorems 3.1–3.3. □

Corollary 3.1. *Let p be a prime greater than* 3. *Then*

$$\text{(a)}\quad u_{p-2}(-3,-9,3)\equiv\begin{cases}0\pmod p & \text{if } p\equiv\pm1\pmod 9,\\ \frac{p+1}{2}\pmod p & \text{if } p\equiv\pm4\pmod 9,\\ \frac{p-1}{2}\pmod p & \text{if } p\equiv\pm2\pmod 9,\end{cases}$$

$$\text{(b)}\quad u_{p-1}(-3,-9,3)\equiv\begin{cases}1\pmod p & \text{if } p\equiv\pm1\pmod 9,\\ \frac{p-1}{2}\pmod p & \text{if } p\equiv\pm2,\pm4\pmod 9,\end{cases}$$

$$\text{(c)}\quad u_{p}(-3,-9,3)\equiv\begin{cases}3\pmod p & \text{if } p\equiv\pm1\pmod 9,\\ \frac{p+3}{2}\pmod p & \text{if } p\equiv\pm4\pmod 9,\\ \frac{p-3}{2}\pmod p & \text{if } p\equiv\pm2\pmod 9,\end{cases}$$

$$\text{(d)}\quad s_{p+1}(-3,-9,3)\equiv\begin{cases}27\pmod p & \text{if } p\equiv\pm1\pmod 9,\\ -9\pmod p & \text{if } p\equiv\pm2,\pm4\pmod 9.\end{cases}$$

Proof. Let $(\frac{\alpha}{\pi})_3$ be the cubic Jacobi symbol. It is well known that [15, (1.1)] $(\frac{\omega}{p})_3=\omega^{(1-(\frac{p}{3})p)/3}$. So

$$\left(\frac{1+1+2\omega}{p}\right)_3=\left(\frac{-2\omega^2}{p}\right)_3=\left(\frac{\omega}{p}\right)_3^2=\omega^{\frac{2(1-(\frac{p}{3})p)}{3}}=\begin{cases}1 & \text{if } p\equiv\pm1\pmod 9,\\ \omega & \text{if } p\equiv\pm4\pmod 9,\\ \omega^2 & \text{if } p\equiv\pm2\pmod 9.\end{cases}$$

Therefore,

$$1\in C_0(p)\ \Leftrightarrow\ p\equiv\pm1\pmod 9,\quad 1\in C_1(p)\ \Leftrightarrow\ p\equiv\pm4\pmod 9$$

and

$$-1\in C_1(p)\ \Leftrightarrow\ 1\in C_2(p)\ \Leftrightarrow\ p\equiv\pm2\pmod 9.$$

Now putting $k=1$ in Theorem 3.4 we get the result. □

Inspired by Theorem 3.4, we now introduce new types of pseudoprimes.

Definition 3.2. Let a_1, a_2, a_3 be integers such that $D = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3 = d^2$ for some integer d. If p is composite prime to $6d$ and the congruence in Theorem 3.2(iii) holds, we say that p is a $u_{p-2}(a_1, a_2, a_3)$ pseudoprime. Similarly, we may define $s_{p+1}(a_1, a_2, a_3), s_{p+2}(a_1, a_2, a_3), u_{p-1}(a_1, a_2, a_3)$ and $u_p(a_1, a_2, a_3)$ pseudoprimes according to Theorems 3.1 and 3.3. Let $k \in \mathbb{Z}$, and let p be a composite number prime to $6(k^2+3)$. We say that p is a u_{p-2}, u_{p-1}, u_p or s_{p+1} pseudoprime with parameter k if p satisfies the congruence (a), (b), (c), or (d) in Theorem 3.4, respectively.

In the special case $k = 1$, a composite number p prime to 6 belongs to a new type of pseudoprimes with parameter 1 if and only if one of the congruences in Corollary 3.1 is true for p.

According to the computations with computer, we list u_{p-2}, u_{p-1}, u_p, s_{p+1} pseudoprimes with parameter 1 up to 10^5 as follows:

u_{p-2} pseudoprimes : $49 = 7^2,\ 3481 = 59^2,\ 16\,469 = 43 \cdot 383.$

u_{p-1} pseudoprimes : $91 = 7 \cdot 13,\ 217 = 7 \cdot 31,\ 961 = 31^2,\ 1681 = 41^2,$

$19\,771 = 17 \cdot 1163.$

u_p pseudoprimes : $1469 = 13 \cdot 113,\ 5041 = 71^2.$

s_{p+1} pseudoprimes : $121 = 11^2,\ 245 = 5 \cdot 7^2,\ 625 = 5^4,\ 6289 = 13 \cdot 331.$

Here we make some comments on new types of pseudoprimes. For each type of the above pseudoprimes, do there exist infinitely many such pseudoprimes? From the search result we see that each type of the above pseudoprimes should be very rare, and more less than Carmichael numbers or Lucas pseudoprimes (there are 16 Carmichael numbers and 25 Lucas pseudoprimes below 10^5). Another observation is that many of the above pseudoprimes are of the form q^2, where q is an odd prime. Is this true? How to interpret it?

Now we introduce another type of pseudoprimes.

Definition 3.3. Let $m, a_1, a_2, \ldots, a_m$ be integers, and let $\{s_n\}$ be given by

$$s_0 = m, \quad s_1 = -a_1, \quad s_k = -(a_1s_{k-1} + a_2s_{k-2} + \cdots + a_{k-1}s_1 + ka_k) \ \ (2 \leqslant k < m),$$

$$s_n + a_1s_{n-1} + \cdots + a_ms_{n-m} = 0 \quad (n \geqslant m).$$

If p is an odd composite number such that $s_p \equiv -a_1 \pmod p$, we say that p is a s_p pseudoprime with parameters $a_1, a_2, \ldots, a_m$, or say that p is a $s_p(a_1, \ldots, a_m)$ pseudoprime.

Let $x^m + a_1x^{m-1} + \cdots + a_m = (x - x_1)\cdots(x - x_m)$. By Newton's formula (cf. [17]) we have $s_n = x_1^n + \cdots + x_m^n$ $(n \geqslant 0)$. Since $x_1, x_2, \ldots, x_m$ are all algebraic integers, using Fermat's little theorem we see that if p is a prime, then

$$s_p = x_1^p + \cdots + x_m^p \equiv (x_1 + \cdots + x_m)^p = (-a_1)^p \equiv -a_1 \pmod p.$$

So $s_p(a_1, \ldots, a_m)$ pseudoprimes are well defined.

For example, an odd composite number p is a $s_p(-3, -9, 3)$ pseudoprime if and only if $s_p(-3, -9, 3) \equiv 3 \pmod p$. All the $s_p(-3, -9, 3)$ pseudoprimes below 50 000 are $25 = 5^2$, $289 = 17^2$, $615 = 3 \cdot 5 \cdot 41$, $2703 = 3 \cdot 17 \cdot 53$, $11\,951 = 17 \cdot 19 \cdot 37$, $41\,393 = 11 \cdot 53 \cdot 71$.

Clearly $s(a_1, \ldots, a_m)$ pseudoprimes include pseudoprimes to base a and Lucas pseudoprimes. For given integers $a_1, \ldots, a_m$ we conjecture that there are infinitely many $s(a_1, \ldots, a_m)$ pseudoprimes.

4. The cubic congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$

Let $a_1, a_2, a_3 \in \mathbb{Z}$. The discriminant D of the cubic polynomial $x^3 + a_1x^2 + a_2x + a_3 = (x - x_1)(x - x_2)(x - x_3)$ is given by (cf. [17,12])

$$D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3. \quad (4.1)$$

When $p > 3$ is a prime such that $p \nmid D$, it follows from Lemma 2.3 that

$$N_p(x^3 + a_1x^2 + a_2x + a_3) = \begin{cases} 0 \text{ or } 3 & \text{if } (\frac{D}{p}) = 1, \\ 1 & \text{if } (\frac{D}{p}) = -1. \end{cases} \quad (4.2)$$

This is a well-known result mentioned in Section 1.

Lemma 4.1. *Let $p > 3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}$, and $D = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3 \equiv 0 \pmod p$. Then $N_p(x^3 + a_1x^2 + a_2x + a_3) = 3$. Moreover,*

$$x \equiv \begin{cases} -\frac{a_1}{3}, \ -\frac{a_1}{3}, \ -\frac{a_1}{3} \pmod p & \text{if } p \mid a_1^2 - 3a_2, \\ -a_1 + \frac{a_1a_2 - 9a_3}{a_1^2 - 3a_2}, \ -\frac{a_1a_2 - 9a_3}{2(a_1^2 - 3a_2)}, \ -\frac{a_1a_2 - 9a_3}{2(a_1^2 - 3a_2)} \pmod p & \text{if } p \nmid a_1^2 - 3a_2 \end{cases}$$

are the three solutions of the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$.

Proof. Let $a = (a_1^2 - 3a_2)^3$ and $b = -2a_1^3 + 9a_1a_2 - 27a_3$. Then $b^2 - 4a = -27D \equiv 0 \pmod p$ by Lemma 2.3.

If $p \mid a_1^2 - 3a_2$, then $p \mid a$ and so $p \mid b$. Hence, by (2.8) we get $x^3 + a_1x^2 + a_2x + a_3 \equiv (x + a_1/3)^3 \pmod p$. So the result holds in this case.

If $p\nmid a_1^2-3a_2$, clearly $X^3-3aX-ab\equiv 0\pmod p$ has the three solutions $X\equiv b,-b/2,-b/2\pmod p$. So, using Lemma 2.3(ii) we see that

$$x\equiv\frac{1}{3}\left(\frac{b}{a_1^2-3a_2}-a_1\right),\ \frac{1}{3}\left(-\frac{b}{2(a_1^2-3a_2)}-a_1\right),\ \frac{1}{3}\left(-\frac{b}{2(a_1^2-3a_2)}-a_1\right)\pmod p$$

are the three solutions of the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0\pmod p$. To see the result, we note that

$$\frac{1}{3}\left(\frac{b}{a_1^2-3a_2}-a_1\right)=-a_1+\frac{a_1a_2-9a_3}{a_1^2-3a_2}$$

and

$$\frac{1}{3}\left(-\frac{b}{2(a_1^2-3a_2)}-a_1\right)=-\frac{a_1a_2-9a_3}{2(a_1^2-3a_2)}.\qquad\square$$

Lemma 4.2. *Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$, $a=(a_1^2-3a_2)^3$, $b=-2a_1^3+9a_1a_2-27a_3$, $D=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$, and $p\nmid aD$. Then $N_p(x^3+a_1x^2+a_2x+a_3)=3$ if and only if there is an integer d such that $d^2\equiv D\pmod p$ and $b/(3d)\in C_0(p)$, and $N_p(x^3+a_1x^2+a_2x+a_3)=0$ if and only if there is an integer d such that $d^2\equiv D\pmod p$ and $b/(3d)\notin C_0(p)$.*

Proof. In view of (4.2) we may assume $(\frac{D}{p})=1$ and $d^2\equiv D\pmod p$ $(d\in\mathbb{Z})$. If $p\mid b$, then $3a\equiv 81D/4\pmod p$ since $b^2-4a=-27D$. So we have $(\frac{3a}{p})=1$ and therefore $N_p(x^3+a_1x^2+a_2x+a_3)=N_p(x^3-3ax-ab)=3$ by Lemma 2.3. On the other hand, we have $b/(3d)\in C_0(p)$ since $0\in C_0(p)$. So the result is true when $p\mid b$.

Now assume $p\nmid b$. Clearly $(-9d)^2\equiv 81D=-3(b^2-4a)\pmod p$. So, using Theorem 4.1 of [15] we find that

$$N_p(x^3-3ax-ab)=\begin{cases}3 & \text{if } -9d/b\in C_0(p),\\ 0 & \text{if } -9d/b\notin C_0(p).\end{cases}$$

Since $N_p(x^3+a_1x^2+a_2x+a_3)=N_p(x^3-3ax-ab)$ by Lemma 2.3 and $b/(3d)\in C_0(p)$ if and only if $-9d/b\in C_0(p)$ by Sun [15, Proposition 2.2], we obtain

$$N_p(x^3+a_1x^2+a_2x+a_3)=\begin{cases}3 & \text{if } b/(3d)\in C_0(p),\\ 0 & \text{if } b/(3d)\notin C_0(p).\end{cases}$$

This finishes the proof. $\square$

Now we can prove

Theorem 4.1. *Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$ and $p\nmid a_1^2-3a_2$. Then $N_p(x^3+a_1x^2+a_2x+a_3)=0$ if and only if $s_{p+1}(a_1,a_2,a_3)\equiv a_2 \pmod p$, and $N_p(x^3+a_1x^2+a_2x+a_3)=3$ if and only if $s_{p+1}(a_1,a_2,a_3)\equiv a_1^2-2a_2 \pmod p$.*

Proof. Let $a=(a_1^2-3a_2)^3$, $b=-2a_1^3+9a_1a_2-27a_3$, $D=-\frac{1}{27}(b^2-4a)=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$, and $s_n=s_n(a_1,a_2,a_3)$. We show the result by considering the following three cases.

Case 1: $p\mid D$. In this case $N_p(x^3+a_1x^2+a_2x+a_3)=3$ by Lemma 4.1. On the other hand, using Theorem 3.1(iii) we see that $s_{p+1}\equiv a_1^2-2a_2 \pmod p$. So the result is true when $p\mid D$.

Case 2: $(\frac{D}{p})=1$. Suppose $d^2\equiv D \pmod p$ for $d\in\mathbb{Z}$. From Theorem 3.1 and Lemma 4.2 we see that

$$s_{p+1}\equiv\begin{cases} a_1^2-2a_2 \pmod p & \text{if } N_p(x^3+a_1x^2+a_2x+a_3)=3,\\ a_2 \pmod p & \text{if } N_p(x^3+a_1x^2+a_2x+a_3)=0.\end{cases}$$

Case 3: $(\frac{D}{p})=-1$. In this case we have $N_p(x^3+a_1x^2+a_2x+a_3)=1$ and $(\frac{-3(b^2-4a)}{p})=-1$ by (4.2) and the fact that $b^2-4a=-27D$. From Lemma 3.1 and Corollary 2.1 we see that

$$s_{p+1}\equiv\frac{1}{3}\left\{a_1^2+(a_1^2-3a_2)^{\frac{1+(\frac{p}{3})}{2}}\cdot\left(\frac{a}{p}\right)a^{\frac{p-(\frac{p}{3})}{6}-1}y\right\}\equiv\frac{1}{3}\{a_1^2+(a_1^2-3a_2)^{-2}y\} \pmod p,$$

where $y\in\mathbb{Z}$ satisfies the congruence $y^3-3a^2y-a^2(b^2-2a)\equiv 0 \pmod p$. Since $p\nmid a(b^2-4a)$ we must have $y\not\equiv -a,\ 2a \pmod p$ and so $s_{p+1}\not\equiv a_2, a_1^2-2a_2 \pmod p$.

Summarizing the above we get the assertion. □

Corollary 4.1. *Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$, $p\nmid a_1^2-3a_2$ and $s_n=s_n(a_1,a_2,a_3)$. If $s_{p+1}\equiv a_2 \pmod p$, then $(\frac{D}{p})=1$ and $(2s_{p+2}+a_1a_2-3a_3)^2\equiv D \pmod p$, where $D=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$.*

Proof. Let $a=(a_1^2-3a_2)^3$ and $b=-2a_1^3+9a_1a_2-27a_3$. From Theorem 4.1 and Lemma 4.1 we see that $N_p(x^3+a_1x^2+a_2x+a_3)=0$ and so $p\nmid D$. It then follows from Lemma 4.2 that there is an integer d such that $d^2\equiv D \pmod p$ and $b/(3d)\notin C_0(p)$. Since $(\frac{b}{3d})^2+3\equiv\frac{b^2+27D}{9D}=\frac{4a}{9D}\not\equiv 0 \pmod p$ we see that $b/(3d)\in$

$C_1(p)\cup C_2(p)$. Hence applying Theorem 3.1(iii) we get $s_{p+2}\equiv\frac{1}{2}(\pm d-a_1a_2+3a_3)\pmod p$ and so $(2s_{p+2}+a_1a_2-3a_3)^2\equiv(\pm d)^2\equiv D\pmod p$. This proves the corollary. □

Lemma 4.3. *Let $a_1,a_2,a_3,A,B,C,x,y\in\mathbb{Z}$, $x^3+a_1x^2+a_2x+a_3\equiv 0\pmod p$ and $y\equiv Ax^2+Bx+C\pmod p$. If $Ay-a_1AB+a_2A^2+B^2-AC\not\equiv 0\pmod p$ or $(a_1a_2-a_3)A^3-(a_1^2+a_2)A^2B+2a_1AB^2-B^3\not\equiv 0\pmod p$, then we have*

$$x\equiv\frac{(B-a_1A)y+a_1AC-a_3A^2-BC}{Ay-a_1AB+a_2A^2+B^2-AC}\pmod p.$$

Proof. If $p\mid A$, then $p\nmid B$ and $y\equiv Bx+C\pmod p$. So $x\equiv(y-C)/B=(By-BC)/B^2\pmod p$. This shows that the result is true when $p\mid A$.

Now assume $p\nmid A$. It is easily seen that

$$\begin{aligned}(Ax+a_1A-B)y&\equiv(Ax+a_1A-B)(Ax^2+Bx+C)\\&=A^2(x^3+a_1x^2)+(a_1AB-B^2+AC)x+a_1AC-BC\\&\equiv -A^2(a_2x+a_3)+(a_1AB-B^2+AC)x+a_1AC-BC\\&=(a_1AB-B^2+AC-a_2A^2)x+a_1AC-BC-a_3A^2\pmod p.\end{aligned}$$

That is,

$$(Ay-a_1AB+B^2-AC+a_2A^2)x\equiv(B-a_1A)y+a_1AC-BC-a_3A^2\pmod p.$$

If $Ay-a_1AB+B^2-AC+a_2A^2\equiv 0\pmod p$, we must have $y\equiv(a_1AB-B^2+AC-a_2A^2)/A\pmod p$ and $(B-a_1A)y+a_1AC-BC-a_3A^2\equiv 0\pmod p$ by the above. So

$$\begin{aligned}&(B-a_1A)(a_1AB-B^2+AC-a_2A^2)+A(a_1AC-BC-a_3A^2)\\&\quad=(a_1a_2-a_3)A^3-(a_1^2+a_2)A^2B+2a_1AB^2-B^3\equiv 0\pmod p.\end{aligned}$$

This is a contradiction. Therefore $Ay-a_1AB+B^2-AC+a_2A^2\not\equiv 0\pmod p$ and hence $x\equiv((B-a_1A)y+a_1AC-BC-a_3A^2)/(Ay-a_1AB+a_2A^2+B^2-AC)\pmod p$. This completes the proof. □

Theorem 4.2. *Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$, and $s_n=s_n(a_1,a_2,a_3)$. Then $N_p(x^3+a_1x^2+a_2x+a_3)=1$ if and only if $s_{p+1}\not\equiv a_2,a_1^2-2a_2\pmod p$. Moreover, if*

$s_{p+1}\not\equiv a_2, a_1^2-2a_2 \pmod p$, *then the unique solution of the congruence* $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$ *is given by*

$$x\equiv\frac{-a_1s_{p+1}+2a_1a_2-9a_3}{3s_{p+1}-2a_1^2+3a_2}$$
$$\equiv\begin{cases}-a_1/3 \pmod p & \text{if } p\mid b,\\ (3s_{p+1}^2-(a_1^2+3a_2)s_{p+1}+2a_1^2a_2-6a_2^2+9a_1a_3)/b \pmod p & \text{if } p\nmid b,\end{cases}$$

where $b=-2a_1^3+9a_1a_2-27a_3$.

Proof. Let $a=(a_1^2-3a_2)^3$. If $p\mid a$, then $a_1^2-2a_2\equiv a_2 \pmod p$ and $x^3+a_1x^2+a_2x+a_3\equiv\frac{1}{27}((3x+a_1)^3-b) \pmod p$ by (2.8). Hence $N_p(x^3+a_1x^2+a_2x+a_3)=1$ if and only if $p\equiv 2 \pmod 3$ and $p\nmid b$. Next, using Lemma 3.1 we see that

$$s_{p+1}\equiv\begin{cases}\frac{a_1^2}{3}\equiv a_2 \pmod p & \text{if } p\equiv 1 \pmod 3,\\ \frac{a_1^2}{3}+\frac{1}{3}v_{\frac{p+1}{3}}(a,b)\equiv a_2+\frac{1}{3}b^{\frac{p+1}{3}} \pmod p & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

Thus,

$$N_p(x^3+a_1x^2+a_2x+a_3)=1 \iff p\equiv 2 \pmod 3 \text{ and } p\nmid b \iff s_{p+1}\not\equiv a_2 \pmod p.$$

If $p\nmid a$, using Theorem 4.1 and the fact that $N_p(x^3+a_1x^2+a_2x+a_3)=0, 1$ or 3 we see that $N_p(x^3+a_1x^2+a_2x+a_3)=1$ if and only if $s_{p+1}\not\equiv a_2, a_1^2-2a_2 \pmod p$.

Now assume $s_{p+1}\not\equiv a_2, a_1^2-2a_2 \pmod p$. Then $N_p(x^3+a_1x^2+a_2x+a_3)=1$ by the above. Applying Lemma 2.3 we find $(\frac{D}{p})=-1$, where $D=-\frac{1}{27}(b^2-4a)$. Let x be an integer such that $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$. By Theorem 3.1 we have $s_{p+1}\equiv 3x^2+2a_1x+2a_2 \pmod p$. Now putting $A=3$, $B=2a_1$ and $C=2a_2$ in Lemma 4.3 we find $(a_1a_2-a_3)A^3-(a_1^2+a_2)A^2B+2a_1AB^2-B^3=b$ and so

$$x\equiv\frac{-a_1s_{p+1}+2a_1a_2-9a_3}{3s_{p+1}-2a_1^2+3a_2} \pmod p \tag{4.3}$$

provided $p\nmid b$. Since $s_{p+1}\equiv 3x^2+2a_1x+2a_2 \pmod p$ and $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$, one can also check that

$$s_{p+1}^2\equiv(a_1^2+3a_2)x^2+(5a_1a_2-9a_3)x+4a_2^2-3a_1a_3 \pmod p$$

and so

$$3s_{p+1}^2-(a_1^2+3a_2)s_{p+1}+2a_1^2a_2-6a_2^2+9a_1a_3\equiv bx \pmod p.$$

Thus the result holds in the case $p\nmid b$.

When $p \mid b$, clearly $p \nmid a$ since $b^2 - 4a = -27D \not\equiv 0 \pmod p$. By (2.8) we have $x \equiv -a_1/3 \pmod p$. Thus, applying Theorem 3.1 we find $s_{p+1} \equiv 3x^2 + 2a_1x + 2a_2 \equiv -a_1^2/3 + 2a_2 \pmod p$ and so $3s_{p+1} - 2a_1^2 + 3a_2 \equiv -3(a_1^2 - 3a_2) \not\equiv 0 \pmod p$. Thus we also have (4.3) by Lemma 4.3. This completes the proof. □

Corollary 4.2. *Let $p>3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}$, and $D = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3$. Then $(\frac{D}{p}) = -1$ if and only if $s_{p+1}(a_1, a_2, a_3) \not\equiv a_2, a_1^2 - 2a_2 \pmod p$.*

Proof. This is immediate from Lemma 2.3(iii) and Theorem 4.2. □

Corollary 4.3. *Let $p>3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}$, and $s_n = s_n(a_1, a_2, a_3)$. If $s_{p+1} \not\equiv a_2, a_1^2 - 2a_2 \pmod p$, then*

$$s_{p+2} \equiv \frac{-2a_1s_{p+1}^2 + a_1^3s_{p+1} - a_1a_2^2 - 3a_1^2a_3 + 9a_2a_3}{3s_{p+1} - 2a_1^2 + 3a_2} \pmod p.$$

Proof. From Theorem 4.2 and Corollary 4.2 we know that

$$N_p(x^3 + a_1x^2 + a_2x + a_3) = 1 \ \Leftrightarrow\ s_{p+1} \not\equiv a_2, \quad a_1^2 - 2a_2 \pmod p \ \Leftrightarrow\ \left(\frac{D}{p}\right) = -1,$$

where $D = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3$.

Let x be an integer such that $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$. From Theorem 3.1 we see that

$$s_{p+1} \equiv 3x^2 + 2a_1x + 2a_2 \pmod p \quad \text{and} \quad s_{p+2} \equiv -2a_1x^2 - (a_1^2 + a_2)x - a_1a_2 \pmod p.$$

Thus

$$2a_1s_{p+1} + 3s_{p+2} \equiv (a_1^2 - 3a_2)x + a_1a_2 \pmod p.$$

Hence applying Theorem 4.2 we get

$$\begin{aligned} s_{p+2} &\equiv \frac{1}{3}\{(a_1^2 - 3a_2)x + a_1a_2 - 2a_1s_{p+1}\} \\ &\equiv \frac{1}{3}\left\{(a_1^2 - 3a_2)\frac{-a_1s_{p+1} + 2a_1a_2 - 9a_3}{3s_{p+1} - 2a_1^2 + 3a_2} + a_1a_2 - 2a_1s_{p+1}\right\} \\ &= \frac{-2a_1s_{p+1}^2 + a_1^3s_{p+1} - a_1a_2^2 - 3a_1^2a_3 + 9a_2a_3}{3s_{p+1} - 2a_1^2 + 3a_2} \pmod p. \end{aligned}$$

This proves the corollary. □

Remark 4.1. Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$, $u_n=u_n(a_1,a_2,a_3)$ and $s_n=s_n(a_1,a_2,a_3)$. If $s_{p+1}\not\equiv a_2, a_1^2-2a_2 \pmod p$, using Theorems 3.3 and 4.2 one can obtain similar congruences for u_{p-1} and $u_p \pmod p$ in terms of s_{p+1}.

Theorem 4.3. *Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$, $a=(a_1^2-3a_2)^3$, $b=-2a_1^3+9a_1a_2-27a_3$, $D=-\frac{1}{27}(b^2-4a)=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$ and $u_n=u_n(a_1,a_2,a_3)$. If $p\nmid ab$, then*

$$N_p(x^3+a_1x^2+a_2x+a_3)=\begin{cases}3 & \text{if } Du_{p-2}^2\equiv 0 \pmod p,\\ 0 & \text{if } Du_{p-2}^2\equiv (a_1^2-3a_2)^2 \pmod p,\\ 1 & \text{if } Du_{p-2}^2\not\equiv 0,(a_1^2-3a_2)^2 \pmod p.\end{cases} \tag{4.4}$$

Moreover, if $N_p(x^3+a_1x^2+a_2x+a_3)=1$, then the unique solution of the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$ is given by

$$x\equiv\frac{(-a_1^2a_2+6a_2^2-9a_1a_3)u_{p-2}+a_1^3-6a_1a_2+27a_3}{-bu_{p-2}+3(a_1^2-3a_2)} \pmod p.$$

Proof. If $p\mid D$, then $N_p(x^3+a_1x^2+a_2x+a_3)=3$ by Lemma 4.1. Now suppose $p\nmid D$. If $(\frac{D}{p})=-1$, it follows from Theorem 3.2 that $Du_{p-2}^3-(a_1^2-3a_2)^2u_{p-2}+b\equiv 0 \pmod p$. Since $p\nmid b$ we see that $Du_{p-2}^2\not\equiv 0,(a_1^2-3a_2)^2 \pmod p$. If $(\frac{D}{p})=1$ and $d^2\equiv D \pmod p$, by Theorem 3.2 we have $Du_{p-2}^2\equiv 0$ or $(a_1^2-3a_2)^2 \pmod p$ according as $b/(3d)\in C_0(p)$ or $b/(3d)\notin C_0(p)$. Thus, $Du_{p-2}^2\equiv 0 \pmod p$ if and only if there is an integer d such that $d^2\equiv D \pmod p$ and $b/(3d)\in C_0(p)$, and $Du_{p-2}^2\equiv (a_1^2-3a_2)^2 \pmod p$ if and only if there is an integer d such that $d^2\equiv D \pmod p$ and $b/(3d)\notin C_0(p)$. This together with Lemma 4.2 gives (4.4).

Now suppose $N_p(x^3+a_1x^2+a_2x+a_3)=1$. Then $(\frac{D}{p})=-1$ by Lemma 2.3. Let $s_n=s_n(a_1,a_2,a_3)$. From Theorem 3.1 we know that

$$s_p\equiv -a_1 \pmod p,\quad s_{p+1}\equiv 3x^2+2a_1x+2a_2 \pmod p,$$

$$s_{p+2}\equiv -2a_1x^2-(a_1^2+a_2)x-a_1a_2 \pmod p.$$

Thus, by (3.3) we have

$$\begin{aligned}Du_{p-2}\equiv &-bx^2+(2a_1^4-10a_1^2a_2+6a_2^2+18a_1a_3)x+a_1^3a_2\\ &-4a_1a_2^2-3a_1^2a_3+18a_2a_3 \pmod p.\end{aligned}$$

Setting $y = Du_{p-2}$, $A = -b$, $B = 2a_1^4 - 10a_1^2a_2 + 6a_2^2 + 18a_1a_3$ and $C = a_1^3a_2 - 4a_1a_2^2 - 3a_1^2a_3 + 18a_2a_3$ we find

$$\begin{aligned}(B - a_1A)y + a_1AC - a_3A^2 - BC&\\ = (-a_1^2a_2 + 6a_2^2 - 9a_1a_3)Du_{p-2} + (a_1^3 - 6a_1a_2 + 27a_3)D&\end{aligned}$$

and

$$Ay - a_1AB + a_2A^2 + B^2 - AC = -bDu_{p-2} + 3(a_1^2 - 3a_2)D.$$

If $p \mid b$, then $p \nmid a$ since $b^2 - 4a = -27D \not\equiv 0 \pmod p$. So $Ay - a_1AB + a_2A^2 + B^2 - AC \not\equiv 0 \pmod p$. If $p \mid b^2 - 2a$, then $p \nmid a$ and $u_{p-2} \equiv -3b/(a_1^2 - 3a_2)^2 \pmod p$ by Theorem 3.2. So

$$\begin{aligned}Ay - a_1AB + a_2A^2 + B^2 - AC &\equiv D(3b^2(a_1^2 - 3a_2)^{-2} + 3(a_1^2 - 3a_2))\\ &\equiv 9D(a_1^2 - 3a_2) \not\equiv 0 \pmod p.\end{aligned}$$

If $p \nmid b(b^2 - 2a)$, it follows from Theorem 3.2 that $Du_{p-2}^3 - (a_1^2 - 3a_2)^2u_{p-2} + b \equiv 0 \pmod p$. Thus $u_{p-2} \not\equiv 3(a_1^2 - 3a_2)/b \pmod p$ since $p \nmid b^2 - 2a$. Hence $Ay - a_1AB + a_2A^2 + B^2 - AC \not\equiv 0 \pmod p$.

Now, by the above and Lemma 4.3 we see that the unique solution of the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$ is given by

$$\begin{aligned}x &\equiv \frac{(B - a_1A)y + a_1AC - a_3A^2 - BC}{Ay - a_1AB + a_2A^2 + B^2 - AC}\\ &\equiv \frac{(-a_1^2a_2 + 6a_2^2 - 9a_1a_3)u_{p-2} + a_1^3 - 6a_1a_2 + 27a_3}{-bu_{p-2} + 3(a_1^2 - 3a_2)} \pmod p.\end{aligned}$$

This completes the proof. □

Lemma 4.4. *Let $p > 3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}$, and $s_n = s_n(a_1, a_2, a_3)$.*

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

$$s_{\frac{p+1}{2}}^4 - 2(a_1^2 - 2a_2)s_{\frac{p+1}{2}}^2 + 8a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}} + a_1^4 - 4a_1^2a_2 + 8a_1a_3 \equiv 0 \pmod p.$$

(ii) *If the congruence* $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$ *is unsolvable, then*

$$s_{\frac{p+1}{2}}^4-2a_2s_{\frac{p+1}{2}}^2+8a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}}+a_2^2-4a_1a_3\equiv 0 \pmod p.$$

Proof. Let $x^3+a_1x^2+a_2x+a_3=(x-x_1)(x-x_2)(x-x_3)$. Then $s_n=x_1^n+x_2^n+x_3^n$ for all $n=0,1,2\ldots$. On setting $z_1=x_2x_3,\ z_2=x_1x_3$ and $z_3=x_1x_2$ we find

$$s_{\frac{p+1}{2}}^2-s_{p+1}=(x_1^{\frac{p+1}{2}}+x_2^{\frac{p+1}{2}}+x_3^{\frac{p+1}{2}})^2-(x_1^{p+1}+x_2^{p+1}+x_3^{p+1})=2(z_1^{\frac{p+1}{2}}+z_2^{\frac{p+1}{2}}+z_3^{\frac{p+1}{2}}).$$

Thus

$$(s_{\frac{p+1}{2}}^2-s_{p+1})^2=4\{z_1^{p+1}+z_2^{p+1}+z_3^{p+1}+2((z_1z_2)^{\frac{p+1}{2}}+(z_1z_3)^{\frac{p+1}{2}}+(z_2z_3)^{\frac{p+1}{2}})\}.$$

Since

$$\begin{aligned}(z_1z_2)^{\frac{p+1}{2}}+(z_1z_3)^{\frac{p+1}{2}}+(z_2z_3)^{\frac{p+1}{2}}&=(x_1x_2x_3)^{\frac{p+1}{2}}(x_1^{\frac{p+1}{2}}+x_2^{\frac{p+1}{2}}+x_3^{\frac{p+1}{2}})\\&=(-a_3)^{\frac{p+1}{2}}s_{\frac{p+1}{2}}\equiv -a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}} \pmod p,\end{aligned}$$

we get

$$(s_{\frac{p+1}{2}}^2-s_{p+1})^2\equiv 4(z_1^{p+1}+z_2^{p+1}+z_3^{p+1})-8a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}} \pmod p.$$

Observing that

$$z_1+z_2+z_3=x_2x_3+x_1x_3+x_1x_2=a_2,\quad z_1z_2z_3=(x_1x_2x_3)^2=a_3^2$$

and

$$z_1z_2+z_1z_3+z_2z_3=(x_1+x_2+x_3)x_1x_2x_3=(-a_1)(-a_3)=a_1a_3$$

we see that $z_1,\ z_2$ and z_3 are the three roots of the equation $z^3-a_2z^2+a_1a_3z-a_3^2=0$. Hence $s_n(-a_2,a_1a_3,-a_3^2)=z_1^n+z_2^n+z_3^n$. So, by the above we have

$$(s_{\frac{p+1}{2}}^2-s_{p+1})^2+8a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}}\equiv 4s_{p+1}(-a_2,a_1a_3,-a_3^2) \pmod p.$$

That is,

$$s_{\frac{p+1}{2}}^4 - 2s_{p+1}s_{\frac{p+1}{2}}^2 + 8a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}} + s_{p+1}^2 - 4s_{p+1}(-a_2, a_1a_3, -a_3^2) \equiv 0 \pmod p. \quad (4.5)$$

Now we claim that $N_p(z^3 - a_2z^2 + a_1a_3z - a_3^2) = 0$ or 3 according as $N_p(x^3 + a_1x^2 + a_2x + a_3) = 0$ or 3. If $N_p(x^3 + a_1x^2 + a_2x + a_3) = 3$, we also have $N_p(z^3 - a_2z^2 + a_1a_3z - a_3^2) = 3$ since $z_1 = x_2x_3$, $z_2 = x_1x_3$ and $z_3 = x_1x_2$. If $N_p(x^3 + a_1x^2 + a_2x + a_3) = 0$ and $z^3 - a_2z^2 + a_1a_3z - a_3^2 \equiv 0 \pmod p$ for some integer z, then $p \nmid a_3$ and so $p \nmid z$. It is easily seen that

$$\left(-\frac{a_3}{z}\right)^3 + a_1\left(-\frac{a_3}{z}\right)^2 + a_2\left(-\frac{a_3}{z}\right) + a_3 = \frac{a_3}{z^3}(z^3 - a_2z^2 + a_1a_3z - a_3^2) \equiv 0 \pmod p.$$

This contradicts the condition $N_p(x^3 + a_1x^2 + a_2x + a_3) = 0$. So $N_p(x^3 + a_1x^2 + a_2x + a_3) = 0$ implies $N_p(z^3 - a_2z^2 + a_1a_3z - a_3^2) = 0$. Hence the claim is true.

If $N_p(x^3 + a_1x^2 + a_2x + a_3) = 3$, then $N_p(z^3 - a_2z^2 + a_1a_3z - a_3^2) = 3$ by the above. From Theorems 4.1 and 3.1 we see that

$$s_{p+1} \equiv a_1^2 - 2a_2 \pmod p \quad \text{and} \quad s_{p+1}(-a_2, a_1a_3, -a_3^2) \equiv a_2^2 - 2a_1a_3 \pmod p.$$

Thus, by (4.5) we have

$$s_{\frac{p+1}{2}}^4 - 2(a_1^2 - 2a_2)s_{\frac{p+1}{2}}^2 + 8a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}} + a_1^4 - 4a_1^2a_2 + 8a_1a_3 \equiv 0 \pmod p.$$

If $N_p(x^3 + a_1x^2 + a_2x + a_3) = 0$, then $N_p(z^3 - a_2z^2 + a_1a_3z - a_3^2) = 0$ by the claim. Using Theorems 4.1 and 3.1 we see that

$$s_{p+1} \equiv a_2 \pmod p \quad \text{and} \quad s_{p+1}(-a_2, a_1a_3, -a_3^2) \equiv a_1a_3 \pmod p.$$

Thus, by (4.5) we get

$$s_{\frac{p+1}{2}}^4 - 2a_2s_{\frac{p+1}{2}}^2 + 8a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}} + a_2^2 - 4a_1a_3 \equiv 0 \pmod p.$$

We are done. □

Theorem 4.4. *Let $p > 3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}$, and $s_n = s_n(a_1, a_2, a_3)$. If the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$ has three solutions and $x_0 = \frac{1}{2}((\frac{-a_3}{p})s_{\frac{p+1}{2}} - a_1) \not\equiv -a_1 \pmod p$, then $x \equiv x_0 \pmod p$ is one of the three solutions of the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$. Furthermore, if $D = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3 \not\equiv 0 \pmod p$, then $d^2 \equiv D \pmod p$ for some integer d and the*

other two solutions of the above congruence are given by

$$x \equiv \pm\frac{1}{2d}((2a_1^2-6a_2)x_0^2+(2a_1^3-7a_1a_2+9a_3\mp d)x_0 + a_1^2a_2-4a_2^2+3a_1a_3\mp a_1d)\ (\mathrm{mod}\ p).$$

Proof. Since $s_{\frac{p+1}{2}}=(\frac{-a_3}{p})(2x_0+a_1)$ we find

$$\begin{aligned} &s_{\frac{p+1}{2}}^4-2(a_1^2-2a_2)s_{\frac{p+1}{2}}^2+8a_3\left(\frac{-a_3}{p}\right)s_{\frac{p+1}{2}}+a_1^4-4a_1^2a_2+8a_1a_3\\ &\quad=(2x_0+a_1)^4-2(a_1^2-2a_2)(2x_0+a_1)^2\\ &\qquad+8a_3(2x_0+a_1)+a_1^4-4a_1^2a_2+8a_1a_3\\ &\quad=16(x_0^4+2a_1x_0^3+(a_1^2+a_2)x_0^2+(a_1a_2+a_3)x_0+a_1a_3)\\ &\quad=16(x_0+a_1)(x_0^3+a_1x_0^2+a_2x_0+a_3). \end{aligned}$$

Thus, by Lemma 4.4 we obtain $(x_0+a_1)(x_0^3+a_1x_0^2+a_2x_0+a_3)\equiv 0\ (\mathrm{mod}\ p)$ and so $x_0^3+a_1x_0^2+a_2x_0+a_3\equiv 0\ (\mathrm{mod}\ p)$ since $x_0\not\equiv -a_1\ (\mathrm{mod}\ p)$.

Now assume $p\nmid D$. Since $N_p(x^3+a_1x^2+a_2x+a_3)=3$ we must have $(\frac{D}{p})=1$ and so $d^2\equiv D\ (\mathrm{mod}\ p)$ for some integer d. Suppose that $x\equiv x_0,x_1,x_2(\mathrm{mod}\ p)$ are the three solutions of the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0\ (\mathrm{mod}\ p)$. Then clearly $x_0+x_1+x_2\equiv -a_1\ (\mathrm{mod}\ p)$ and $x_0x_1+x_0x_2+x_1x_2\equiv a_2\ (\mathrm{mod}\ p)$. So we have $x_1+x_2\equiv -a_1-x_0\ (\mathrm{mod}\ p)$ and therefore

$$\begin{aligned}(x_0-x_1)(x_0-x_2)&=x_0x_1+x_0x_2+x_1x_2+x_0^2-2x_0(x_1+x_2)\\ &\equiv a_2+x_0^2+2x_0(a_1+x_0)=3x_0^2+2a_1x_0+a_2\ (\mathrm{mod}\ p).\end{aligned}$$

Observing that $((x_0-x_1)(x_0-x_2)(x_1-x_2))^2\equiv D\equiv d^2\ (\mathrm{mod}\ p)$ by (4.1), we get $(x_0-x_1)(x_0-x_2)(x_1-x_2)\equiv\pm d\ (\mathrm{mod}\ p)$ and so

$$x_1-x_2\equiv\pm\frac{d}{(x_0-x_1)(x_0-x_2)}\equiv\pm\frac{d}{3x_0^2+2a_1x_0+a_2}\ (\mathrm{mod}\ p).$$

This together with the fact that $x_1+x_2\equiv -a_1-x_0\ (\mathrm{mod}\ p)$ yields

$$x_1\equiv\frac{1}{2}\left(-a_1-x_0\pm\frac{d}{3x_0^2+2a_1x_0+a_2}\right)\ (\mathrm{mod}\ p)$$

and

$$x_2 \equiv \frac{1}{2}\left(-a_1 - x_0 \mp \frac{d}{3x_0^2 + 2a_1x_0 + a_2}\right) \pmod p.$$

Since $x_0^3 \equiv -(a_1x_0^2 + a_2x_0 + a_3) \pmod p$ and so $x_0^4 \equiv (a_1^2 - a_2)x_0^2 + (a_1a_2 - a_3)x_0 + a_1a_3 \pmod p$ one can easily verify that

$$(3x_0^2 + 2a_1x_0 + a_2)((2a_1^2 - 6a_2)x_0^2 + (2a_1^3 - 7a_1a_2 + 9a_3)x_0 + a_1^2a_2 - 4a_2^2 + 3a_1a_3)$$
$$\equiv D \pmod p.$$

Thus

$$\frac{d}{3x_0^2 + 2a_1x_0 + a_2}$$
$$\equiv \frac{(2a_1^2 - 6a_2)x_0^2 + (2a_1^3 - 7a_1a_2 + 9a_3)x_0 + a_1^2a_2 - 4a_2^2 + 3a_1a_3}{d} \pmod p.$$

Now putting the above together we obtain the result. □

From Lemmas 2.3, 4.2 and [15, Theorem 4.1] one can easily prove

Theorem 4.5. *Let p be a prime such that $p \equiv 1 \pmod 3$, $a_1, a_2, a_3 \in \mathbb{Z}$, $a = (a_1^2 - 3a_2)^3$ and $b = -2a_1^3 + 9a_1a_2 - 27a_3$ with $p \nmid a(b^2 - 4a)$. Then the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$ has three solutions if and only if there is an integer y such that $y^2 \equiv b^2 - 4a \pmod p$ and $4(b - y)$ is a cubic residue of p. Moreover, if $y^2 \equiv b^2 - 4a \pmod p$ and $z \equiv z_1, z_2, z_3 \pmod p$ are the three solutions of the congruence $z^3 \equiv 4(b - y) \pmod p$, then*

$$x \equiv \frac{(z_i - a_1)^2 + 3(a_1^2 - 4a_2)}{6z_i} \pmod p \quad (i = 1, 2, 3)$$

are the three solutions of the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$.

We remark that Theorem 4.5 can also be deduced from the theory of cubic equations.

5. The quartic congruence $x^4 + ax^2 + bx + c \equiv 0 \pmod p$

Let p be an odd prime. In the section we discuss the general quartic congruence $x^4 + ax^2 + bx + c \equiv 0 \pmod p$.

For the general quartic polynomial $x^4+a_1x^3+a_2x^2+a_3x+a_4$ let

$$a=a_2-\frac{3a_1^2}{8},\quad b=a_3-\frac{a_1a_2}{2}+\frac{a_1^3}{8},\quad c=a_4-\frac{a_1a_3}{4}+\frac{a_1^2a_2}{16}-\frac{3a_1^4}{256}$$

and $y=x+a_1/4$. Then we find

$$x^4+a_1x^3+a_2x^2+a_3x+a_4=y^4+ay^2+by+c.$$

So we only need to study the congruence $x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)$.

For $a,b,c\in\mathbb{Z}$ define

$$D(a,b,c)=-(4a^3+27b^2)b^2+16c(a^4+9ab^2-8a^2c+16c^2). \tag{5.1}$$

Then clearly

$$\begin{aligned}a^2D(a,b,c)=&\,2ab^2(a^2+12c)^2-3b^2(a^2+12c)(2a^3-8ac+9b^2)\\&+4c(2a^3-8ac+9b^2)^2.\end{aligned} \tag{5.2}$$

It is easily seen that $D(a,b,c)$ is just the discriminant of the cubic polynomial $y^3+2ay^2+(a^2-4c)y-b^2$. So, if p is an odd prime, then the congruence $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\ (\mathrm{mod}\ p)$ has one multiple solution if and only if $p\mid D(a,b,c)$.

Lemma 5.1. *Let p be an odd prime, and $a,b,c\in\mathbb{Z}$ with $p\nmid b$. Then the congruence $x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)$ has one multiple solution if and only if $D(a,b,c)\equiv 0\ (\mathrm{mod}\ p)$.*

Proof. Let $x_0\in\mathbb{Z}$. It is clear that

$$\begin{aligned}&x\equiv x_0\ (\mathrm{mod}\ p)\quad\text{is a multiple solution of } x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)\\&\Leftrightarrow x_0^4+ax_0^2+bx_0+c\equiv 0\ (\mathrm{mod}\ p)\quad\text{and}\quad 4x_0^3+2ax_0+b\equiv 0\ (\mathrm{mod}\ p)\\&\Leftrightarrow b\equiv -2x_0(2x_0^2+a)\ (\mathrm{mod}\ p)\quad\text{and}\quad a^2-4c\equiv(2x_0^2+a)^2+4bx_0\ (\mathrm{mod}\ p)\\&\Leftrightarrow 2a\equiv -\frac{4x_0^3+b}{x_0}\ (\mathrm{mod}\ p)\quad\text{and}\quad a^2-4c\equiv\frac{b^2}{4x_0^2}+4bx_0\ (\mathrm{mod}\ p)\\&\Leftrightarrow y^3+2ay^2+(a^2-4c)y-b^2\equiv\left(y-\frac{b}{2x_0}\right)^2(y-4x_0^2)\ (\mathrm{mod}\ p)\\&\Leftrightarrow y\equiv\frac{b}{2x_0}\ (\mathrm{mod}\ p)\quad\text{is a multiple solution of}\\&\quad y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\ (\mathrm{mod}\ p).\end{aligned}$$

So

$$x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)\ \text{has one multiple solution}$$
$$\Leftrightarrow y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\ (\mathrm{mod}\ p)\ \text{has one multiple solution}$$
$$\Leftrightarrow D(a,b,c)\equiv 0\ (\mathrm{mod}\ p).$$

This proves the lemma. □

Remark 5.1. If $p>3$ is a prime, $a,b,c\in\mathbb{Z}$, $p\nmid b$ and $p\mid D(a,b,c)$, one can verify that the congruence $x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)$ has the following multiple solution:

$$x\equiv\begin{cases}-\frac{3b}{4a}\ (\mathrm{mod}\ p) & \text{if } 2a^3-8ac+9b^2\equiv 0\ (\mathrm{mod}\ p),\\ -\frac{(a^2+12c)b}{2a^3-8ac+9b^2}\ (\mathrm{mod}\ p) & \text{if } 2a^3-8ac+9b^2\not\equiv 0\ (\mathrm{mod}\ p).\end{cases}$$

Lemma 5.2. *Let p be an odd prime, $a,b,c\in\mathbb{Z}$ and $p\nmid bD(a,b,c)$. If there is an integer y such that $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\ (\mathrm{mod}\ p)$ and $(\frac{y}{p})=-1$, then the congruence $x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)$ is unsolvable.*

Proof. If $x=x_0$ is a solution of the congruence $x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)$, then clearly

$$x^4+ax^2+bx+c\equiv(x-x_0)(x^3+x_0x^2+(x_0^2+a)x+x_0^3+ax_0+b)\ (\mathrm{mod}\ p)\qquad(5.3)$$

and

$$\left(x_0^2+\frac{a}{2}\right)^2\equiv -bx_0+\frac{a^2-4c}{4}\ (\mathrm{mod}\ p).$$

Since $p\nmid y$ we see that

$$\left(x_0^2+\frac{a}{2}+\frac{y}{2}\right)^2\equiv yx_0^2-bx_0+\frac{y^2+2ay+a^2-4c}{4}\equiv y\left(x_0-\frac{b}{2y}\right)^2\ (\mathrm{mod}\ p).\qquad(5.4)$$

If $x_0\not\equiv b/(2y)\ (\mathrm{mod}\ p)$, then $(\frac{y}{p})=1$ by (5.4). This contradicts the condition $(\frac{y}{p})=-1$. If $x_0\equiv b/(2y)\ (\mathrm{mod}\ p)$, we must have $x_0^2\equiv -(a+y)/2\ (\mathrm{mod}\ p)$ by (5.4). This yields $4x_0^3+2ax_0+b\equiv 0\ (\mathrm{mod}\ p)$. Hence $x\equiv x_0\ (\mathrm{mod}\ p)$ is a multiple solution of the congruence $x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)$ by (5.3). Using Lemma 5.1 we see that $D(a,b,c)\equiv 0\ (\mathrm{mod}\ p)$. This is also a contradiction. Thus the congruence $x^4+ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p)$ has no solutions. □

Theorem 5.1. *Let p be an odd prime, and $a,b,c\in\mathbb{Z}$ with $p\nmid bD(a,b,c)$. If $N_p(x^4+ax^2+bx+c)>0$, then $N_p(x^4+ax^2+bx+c)=N_p(y^3+2ay^2+(a^2-4c)y-b^2)+1$.*

Proof. Suppose that $x_0 \pmod p$ is a solution of the congruence $x^4+ax^2+bx+c\equiv 0 \pmod p$. For $u=-x-x_0$ one can easily verify that

$$u^3+2x_0u^2+(2x_0^2+a)u-b=-(x^3+x_0x^2+(x_0^2+a)x+x_0^3+ax_0+b).$$

Thus, by (5.3) we have

$$x^4+ax^2+bx+c\equiv -(x-x_0)(u^3+2x_0u^2+(2x_0^2+a)u-b) \pmod p.$$

So

$$N_p(x^4+ax^2+bx+c)=1+N_p(u^3+2x_0u^2+(2x_0^2+a)u-b).$$

Set $f(u)=u^3+2x_0u^2+(2x_0^2+a)u-b$. We claim that $f(-u)\not\equiv 0 \pmod p$ when $f(u)\equiv 0 \pmod p$. If $f(u)\equiv f(-u)\equiv 0 \pmod p$, then $f(u)\pm f(-u)\equiv 0 \pmod p$ and $p\nmid u$ since $p\nmid b$. This implies that $2x_0u^2-b\equiv 0 \pmod p$ and $u^2+2x_0^2+a\equiv 0 \pmod p$. So $4x_0^3+2ax_0+b\equiv 0 \pmod p$. This together with (5.3) shows that $x\equiv x_0 \pmod p$ is a multiple solution of the congruence $x^4+ax^2+bx+c\equiv 0 \pmod p$. Hence $D(a,b,c)\equiv 0 \pmod p$ by Lemma 5.1. This contradicts the condition $p\nmid D(a,b,c)$. So the claim holds.

Clearly,

$$\begin{aligned} f(u)f(-u)&=(2x_0u^2-b)^2-(u^3+(2x_0^2+a)u)^2\\ &=-u^6-2au^4-(4x_0^4+4ax_0^2+4bx_0+a^2)u^2+b^2\\ &\equiv -(u^6+2au^4+(a^2-4c)u^2-b^2) \pmod p. \end{aligned} \tag{5.5}$$

Hence, if $f(u)\equiv 0 \pmod p$ for some $u\in\mathbb{Z}$, then $y\equiv u^2 \pmod p$ is a solution of the congruence $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0 \pmod p$. Conversely, if $y\in\mathbb{Z}$ satisfies $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0 \pmod p$, then $y\equiv u^2 \pmod p$ for some $u\in\mathbb{Z}$ by Lemma 5.2. So $f(u)\equiv 0 \pmod p$ or $f(-u)\equiv 0 \pmod p$ by (5.5). By the above claim, $f(u)\equiv 0 \pmod p$ implies that $f(-u)\not\equiv 0 \pmod p$. So we have $N_p(x^4+ax^2+bx+c)-1=N_p(u^3+2x_0u^2+(2x_0^2+a)u-b)=N_p(y^3+2ay^2+(a^2-4c)y-b^2)$. This completes the proof. □

Now we give

Theorem 5.2. *Let $p>3$ be a prime, and $a,b,c\in\mathbb{Z}$. Then the congruence $(*)x^4+ax^2+bx+c\equiv 0\pmod p$ has one and only one solution if and only if the congruence $(**)$ $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\pmod p$ is unsolvable. Moreover, if $(**)$ is unsolvable, then the unique solution of $(*)$ is given by*

$$x\equiv\frac{1}{4b}(a^2-4c-S^2_{\frac{p+1}{2}})\pmod p,$$

where $\{S_n\}$ is defined by

$$S_0=3,\quad S_1=-2a,\quad S_2=2a^2+8c,$$

$$S_{n+3}=-2aS_{n+2}+(4c-a^2)S_{n+1}+b^2S_n\quad(n=0,1,2,\ldots).\tag{5.6}$$

Proof. If $N_p(x^4+ax^2+bx+c)=1$, then clearly $p\nmid b$ and so $p\nmid D(a,b,c)$ by Lemma 5.1. From this and Theorem 5.1 we see that $N_p(y^3+2ay^2+(a^2-4c)y-b^2)=0$.

Now suppose that the congruence $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\pmod p$ is unsolvable. Then clearly $p\nmid b$ and $p\nmid D(a,b,c)$. It then follows from Theorem 5.1 that $N_p(x^4+ax^2+bx+c)=0$ or 1. To see the result, we only need to show that $x_0=\frac{1}{4b}(a^2-4c-S^2_{\frac{p+1}{2}})$ satisfies the congruence $x_0^4+ax_0^2+bx_0+c\equiv 0\pmod p$.

Let $a_1=2a$, $a_2=a^2-4c$ and $a_3=-b^2$. Then the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0\pmod p$ is unsolvable and $S_n=s_n(a_1,a_2,a_3)$. Applying Lemma 4.4 we find

$$\begin{aligned}x_0^2&=\frac{1}{16b^2}(a^2-4c-S^2_{\frac{p+1}{2}})^2=-\frac{1}{16a_3}(a_2-S^2_{\frac{p+1}{2}})^2\\&\equiv\frac{1}{16a_3}\left(8a_3\left(\frac{-a_3}{p}\right)S_{\frac{p+1}{2}}-4a_1a_3\right)=\frac{1}{2}(S_{\frac{p+1}{2}}-a)\pmod p.\end{aligned}$$

Thus

$$\begin{aligned}x_0^4+ax_0^2+bx_0+c&\equiv\frac{1}{4}(S_{\frac{p+1}{2}}-a)^2+\frac{a}{2}(S_{\frac{p+1}{2}}-a)+\frac{1}{4}(a^2-4c-S^2_{\frac{p+1}{2}})+c\\&=\frac{1}{4}((S_{\frac{p+1}{2}}-a)^2+2a(S_{\frac{p+1}{2}}-a)+a^2-S^2_{\frac{p+1}{2}})=0\pmod p.\end{aligned}$$

This completes the proof. □

From Theorems 5.2 and 4.1 we have

Theorem 5.3. *Let $p>3$ be a prime, and $a,b,c\in\mathbb{Z}$.*

(i) *If* $a^2+12c\not\equiv 0 \pmod p$, *then the congruence* $x^4+ax^2+bx+c\equiv 0 \pmod p$ *has one and only one solution if and only if* $S_{p+1}\equiv a^2-4c \pmod p$, *where* $\{S_n\}$ *is given by* (5.6).

(ii) *If* $a^2+12c\equiv 0 \pmod p$, *then the congruence* $x^4+ax^2+bx+c\equiv 0 \pmod p$ *has one and only one solution if and only if* $p\equiv 1 \pmod 3$ *and* $8a^3+27b^2$ *is a cubic nonresidue* $\pmod p$.

Proof. Obviously $(2a)^2-3(a^2-4c)=a^2+12c$. If $a^2+12c\not\equiv 0 \pmod p$, using Theorems 5.2 and 4.1 we see that

$$N_p(x^4+ax^2+bx+c)=1 \Leftrightarrow N_p(y^3+2ay^2+(a^2-4c)y-b^2)=0$$
$$\Leftrightarrow S_{p+1}\equiv a^2-4c \pmod p.$$

This proves (i).

Now suppose $a^2+12c\equiv 0 \pmod p$. Setting $x=3y+2a$ we find

$$y^3+2ay^2+(a^2-4c)y-b^2\equiv \frac{1}{27}(x^3-(8a^3+27b^2)) \pmod p.$$

This together with Theorem 5.2 implies that

$$\begin{aligned} &N_p(x^4+ax^2+bx+c)=1\\ &\Leftrightarrow N_p(y^3+2ay^2+(a^2-4c)y-b^2)=0\\ &\Leftrightarrow x^3\equiv 8a^3+27b^2 \pmod p \text{ is unsolvable}\\ &\Leftrightarrow p\equiv 1 \pmod 3 \text{ and } 8a^3+27b^2 \text{ is a cubic nonresidue} \pmod p. \end{aligned}$$

So the theorem is proved. □

Theorem 5.4. *Let* $p>3$ *be a prime,* $a,b,c\in\mathbb{Z}$ *and* $p\nmid bD(a,b,c)$. *Then congruence* $(*)$ $x^4+ax^2+bx+c\equiv 0 \pmod p$ *has exactly two solutions if and only if congruence* $(**)$ $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0 \pmod p$ *has one and only one solution and the unique solution of* $(**)$ *is a quadratic residue modulo p. Furthermore, if* $y\equiv u^2 \pmod p$ *is the unique solution of* $(**)$ *and* $v^2\equiv -u^4-2au^2-2bu \pmod p$, *then the two solutions of* $(*)$ *are given by* $x\equiv \frac{1}{2}(u\pm\frac{v}{u}) \pmod p$.

Proof. If $N_p(x^4+ax^2+bx+c)=2$, using Theorem 5.1 and Lemma 5.2 we see that $N_p(y^3+2ay^2+(a^2-4c)y-b^2)=1$ and the unique solution of $(**)$ is a quadratic residue $\pmod p$.

Conversely, if $y\equiv u^2 \pmod p$ $(u\in\mathbb{Z})$ is the unique solution of $(**)$, then $N_p(x^4+ax^2+bx+c)=0$ or 2 by Theorem 5.1. It is easily seen that

$$\begin{aligned}&y^3+2ay^2+(a^2-4c)y-b^2\\&\quad\equiv(y-u^2)\left(\left(y+\frac{u^2+2a}{2}\right)^2-\frac{u^2(u^2+2a)^2-4b^2}{4u^2}\right)\pmod p.\end{aligned}$$

Thus,

$$\left(\frac{-u^4-2au^2-2bu}{p}\right)\left(\frac{-u^4-2au^2+2bu}{p}\right)=\left(\frac{u^4(u^2+2a)^2-4b^2u^2}{p}\right)=-1.$$

So we may choose the sign of u so that $(\frac{-u^4-2au^2-2bu}{p})=1$.

Now suppose $(\frac{-u^4-2au^2-2bu}{p})=1$ and $v^2\equiv -u^4-2au^2-2bu \pmod p$ with $v\in\mathbb{Z}$. Then clearly

$$\left(\frac12\left(u\pm\frac{v}{u}\right)\right)^2\equiv\frac14\left(u^2+\frac{-u^4-2au^2-2bu}{u^2}\pm2v\right)=\frac12\left(-a-\frac{b}{u}\pm v\right)\pmod p$$

and therefore

$$\begin{aligned}\left(\frac12\left(u\pm\frac{v}{u}\right)\right)^4&\equiv\frac14\left(a^2+\frac{b^2}{u^2}+\frac{2ab}{u}+v^2\mp2\left(a+\frac{b}{u}\right)v\right)\\&\equiv\frac14\left(a^2+\left(-u^4-2au^2+\frac{b^2}{u^2}\right)+\frac{2ab}{u}-2bu\mp2\left(a+\frac{b}{u}\right)v\right)\\&\equiv\frac14\left(a^2+(a^2-4c)+\frac{2ab}{u}-2bu\mp2\left(a+\frac{b}{u}\right)v\right)\\&=\frac12\left(a^2-2c+\frac{ab}{u}-bu\mp\left(a+\frac{b}{u}\right)v\right)\pmod p.\end{aligned}$$

So

$$\begin{aligned}&\left(\frac12\left(u\pm\frac{v}{u}\right)\right)^4+a\left(\frac12\left(u\pm\frac{v}{u}\right)\right)^2+b\cdot\frac12\left(u\pm\frac{v}{u}\right)+c\\&\quad\equiv\frac12\left(a^2-2c+\frac{ab}{u}-bu\mp\left(a+\frac{b}{u}\right)v-a^2-\frac{ab}{u}\pm av+bu\pm\frac{bv}{u}+2c\right)\\&\quad=0\pmod p.\end{aligned}$$

This shows that congruence $(*)$ has two solutions $x\equiv\frac12(u\pm\frac{v}{u})\pmod p$ since $p\nmid v$. Hence $N_p(x^4+ax^2+bx+c)=2$ and the proof is complete. □

From Theorems 5.4 and 4.2 we have

Theorem 5.5. *Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$, $p\nmid bD(a,b,c)$, and let $\{S_n\}$ be given by* (5.6). *Then $N_p(x^4+ax^2+bx+c)=2$ if and only if $S_{p+1}\not\equiv a^2-4c, 2a^2+8c \pmod p$ and $(4a^3-16ac+9b^2-2aS_{p+1})/(-5a^2-12c+3S_{p+1})$ is a quadratic residue $\pmod p$. Moreover, if the above condition holds, then the two solutions of the congruence $x^4+ax^2+bx+c\equiv 0 \pmod p$ are given by $x\equiv\frac{1}{2}(u\pm\frac{v}{u}) \pmod p$, where u is determined by*

$$u^2\equiv\frac{4a^3-16ac+9b^2-2aS_{p+1}}{-5a^2-12c+3S_{p+1}}\pmod p \quad \text{and} \quad \left(\frac{-u^4-2au^2-2bu}{p}\right)=1,$$

and v is given by $v^2\equiv -u^4-2au^2-2bu \pmod p$.

Proof. Let $a_1=2a$, $a_2=a^2-4c$ and $a_3=-b^2$. Then clearly $a_1^2-2a_2=2a^2+8c$ and

$$\frac{2a_1a_2-9a_3-a_1S_{p+1}}{-2a_1^2+3a_2+3S_{p+1}}=\frac{4a^3-16ac+9b^2-2aS_{p+1}}{-5a^2-12c+3S_{p+1}}.$$

Now, applying Theorems 5.4 and 4.2 we obtain the result. □

Now we point out the following criterion for $N_p(x^4+ax^2+bx+c)=4$, which can also be deduced from Galois theory.

Theorem 5.6. *Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$ and $p\nmid bD(a,b,c)$. Then congruence* $(*)$ $x^4+ax^2+bx+c\equiv 0 \pmod p$ *has four solutions if and only if congruence* $(**)$ $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0 \pmod p$ *has three solutions and all the three solutions are quadratic residues modulo p. Furthermore, if $y\equiv u_1^2, u_2^2, u_3^2 \pmod p$ $(u_1,u_2,u_3\in\mathbb{Z})$ are the solutions of $(**)$ such that $u_1u_2u_3\equiv -b \pmod p$, then the four solutions of $(*)$ are given by*

$$x\equiv\frac{u_1+u_2+u_3}{2},\ \frac{u_1-u_2-u_3}{2},\ \frac{-u_1+u_2-u_3}{2},\ \frac{-u_1-u_2+u_3}{2}\pmod p.$$

Proof. If $N_p(x^4+ax^2+bx+c)=4$, it follows from Lemma 5.2 and Theorem 5.1 that $N_p(y^3+2ay^2+(a^2-4c)y-b^2)=3$ and all the three solutions of congruence $(**)$ are quadratic residues $\pmod p$.

Now suppose that $y\equiv u_1^2,u_2^2,u_3^2 \pmod p$ are the three solutions of $(**)$ such that $u_1u_2u_3\equiv -b \pmod p$. From Vieta's theorem we have

$$u_1^2+u_2^2+u_3^2\equiv -2a \pmod p,\quad u_1^2u_2^2+u_2^2u_3^2+u_1^2u_3^2\equiv a^2-4c \pmod p$$

and

$$u_1^2u_2^2u_3^2 \equiv b^2 \pmod p.$$

Using this one can easily verify that

$$x \equiv \tfrac{1}{2}(u_1+u_2+u_3),\ \tfrac{1}{2}(u_1-u_2-u_3),\ \tfrac{1}{2}(-u_1+u_2-u_3),\ \tfrac{1}{2}(-u_1-u_2+u_3) \pmod p$$

are the solutions of congruence $(*)$. Since $p\nmid D(a,b,c)$, we see that $(**)$ has no multiple solutions. So

$$u_1^2 \not\equiv u_2^2 \pmod p, \quad u_1^2 \not\equiv u_3^2 \pmod p \quad \text{and} \quad u_2^2 \not\equiv u_3^2 \pmod p.$$

Hence the above four solutions of $(*)$ are distinct. This completes the proof. □

Theorem 5.7. *Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$ and $p\nmid(a^2+12c)bD(a,b,c)$. Then the congruence $(*)$ $x^4+ax^2+bx+c\equiv 0 \pmod p$ has four solutions if and only if $S_{(p-1)/2}\equiv 3 \pmod p$ and $S_{p+1}\equiv 2a^2+8c \pmod p$, where $\{S_n\}$ is given by $S_0=3$, $S_1=-2a$, $S_2=2a^2+8c$ and $S_{n+3}=-2aS_{n+2}+(4c-a^2)S_{n+1}+b^2S_n$ $(n\geqslant 0)$.*

Proof. Clearly $S_n=s_n(2a,a^2-4c,-b^2)$. From the fact that $p\nmid a^2+12c$ and Theorem 4.1 we see that $N_p(y^3+2ay^2+(a^2-4c)y-b^2)=3$ if and only if $S_{p+1}\equiv 2a^2+8c \pmod p$. If $y\equiv y_1,y_2,y_3 \pmod p$ are the three solutions of the congruence $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0 \pmod p$, then clearly $y_1y_2y_3\equiv b^2 \pmod p$ and so

$$\begin{aligned} S_{\frac{p-1}{2}} &\equiv y_1^{\frac{p-1}{2}}+y_2^{\frac{p-1}{2}}+y_3^{\frac{p-1}{2}} \equiv \left(\frac{y_1}{p}\right)+\left(\frac{y_2}{p}\right)+\left(\frac{y_3}{p}\right) \\ &= \begin{cases} 3 \pmod p & \text{if } (\frac{y_1}{p})=(\frac{y_2}{p})=(\frac{y_3}{p})=1, \\ -1 \pmod p & \text{otherwise.} \end{cases} \end{aligned}$$

Thus, y_1,y_2,y_3 are all quadratic residues of p if and only if $S_{(p-1)/2}\equiv 3 \pmod p$. Now applying Theorem 5.6 we obtain the result. □

From Theorems 5.2, 5.4, 5.6 and Lemma 5.2 we have the following conclusion.

Theorem 5.8. *Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$ and $p\nmid bD(a,b,c)$. Then $N_p(x^4+ax^2+bx+c)=0$ if and only if there exists an integer y such that $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0 \pmod p$ and $(\frac{y}{p})=-1$. When $N_p(x^4+ax^2+bx+c)>0$ we have $N_p(x^4+ax^2+bx+c)=N_p(y^3+2ay^2+(a^2-4c)y-b^2)+1$.*

Theorem 5.8 is equivalent to the following result.

Theorem 5.9. *Let $p>3$ be a prime, and $a,b,c\in\mathbb{Z}$ with $p\nmid bD(a,b,c)$. Then*

$$N_p(x^4+ax^2+bx+c)=1+\sum_y\left(\frac{y}{p}\right),$$

where y runs over the solutions of the congruence $(**)$ $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\pmod p$.

Proof. If the congruence $(**)$ is unsolvable, then $N_p(x^4+ax^2+bx+c)=1$ by Theorem 5.2. If $y\equiv y_0\pmod p$ is the unique solution of $(**)$, using Theorems 5.1 and 5.4 we know that $N_p(x^4+ax^2+bx+c)=0$ or 2 according as $(\frac{y_0}{p})=-1$ or $(\frac{y_0}{p})=1$. If $y\equiv y_1,y_2,y_3\pmod p$ are the three solutions of $(**)$, then $(\frac{y_1}{p})(\frac{y_2}{p})(\frac{y_3}{p})=(\frac{y_1y_2y_3}{p})=(\frac{b^2}{p})=1$. When $(\frac{y_1}{p})=(\frac{y_2}{p})=(\frac{y_3}{p})=1$, it follows from Theorem 5.6 that $N_p(x^4+ax^2+bx+c)=4$. Otherwise $N_p(x^4+ax^2+bx+c)=0$ by Lemma 5.2. So the theorem is proved. □

Remark 5.2. In [10] Skolem obtained the result which is close to Theorem 5.9. However, his condition includes the value of the Legendre symbol $(\frac{D}{p})$, where D is the discriminant of the given quartic polynomial $f(x)$, and p is a prime greater than 3 such that $p\nmid D$. Compared with Skolem's condition, the condition of Theorem 5.9 is more simple.

References

[1] H.R. Brahana, Note on irreducible quartic congruence, Trans. Amer. Math. Soc. 38 (1935) 395–400.
[2] L. Carlitz, A special quartic congruence, Math. Scand. 4 (1956) 243–246.
[3] L. Carlitz, Note on a quartic congruence, Amer. Math. Monthly 63 (1956) 569–571.
[4] A. Cauchy, Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers, Exercises Math. 4 (1829) 253–292.
[5] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Text in Mathematics, Vol. 138, Springer, Berlin, 1993, pp. 198–199.
[6] L.E. Dickson, Criteria for the irreducibility of functions in a finite field, Bull. Amer. Math. Soc. 13 (1906) 1–8.
[7] P.A. Leonard, On factoring quartics (mod p), J. Number Theory 1 (1969) 113–115.
[8] P. Ribenboim, The Book of Prime Number Records, 2nd Edition, Springer, Berlin, 1989, pp. 44–50.
[9] T. Skolem, Zwei Sätze über kubische Kongruenzen, Norske Vid. Selsk. Forhdl. 10 (1937) 89–92.
[10] T. Skolem, The general congruence of 4th degree modulo p, p prime, Norsk Mat. Tidsskr. 34 (1952) 73–80.
[11] T. Skolem, On a certain connection between the discriminant of a polynomial and the number of its irreducible factors mod p, Norsk Mat. Tidsskr. 34 (1952) 81–85.
[12] B.K. Spearman, K.S. Williams, The cubic congruence $x^3+Ax^2+Bx+C\equiv 0\pmod p$ and binary quadratic forms, J. London Math. Soc. 46 (1992) 397–410 MR93j:11004.
[13] B.K. Spearman, K.S. Williams, The cubic congruence $x^3+Ax^2+Bx+C\equiv 0\pmod p$ and binary quadratic forms II, J. London Math. Soc. 64 (2001) 273–274.

[14] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Verhand. I, Internat. Math. Kongress Zürich, 1897, pp. 182–193.
[15] Z.H. Sun, On the theory of cubic residues and nonresidues, Acta Arith. 84 (1998) 291–335 MR99c:11005.
[16] Z.H. Sun, Linear recursive sequences and powers of matrices, Fibonacci Quart. 39 (2001) 339–351 MR2002f:11013.
[17] J.P. Tignol, Galois' Theory of Algebraic Equations, World Scientific Publishing Co., Singapore, New Jersey, 2001, pp. 38, 107.
[18] K.S. Williams, R.H. Hudson, Representation of primes by the principal form of discriminant $-D$ when the classnumber $h(-D)$ is 3, Acta Arith. 57 (1991) 131–153.
[19] H.C. Williams, C.R. Zarnke, Some algorithms for solving a cubic congruence modulo p, Utilitas Math. 6 (1974) 285–306.