Journal of Number Theory 119(2006), 210-241.

# ON THE NUMBER OF INCONGRUENT RESIDUES OF $x^4+ax^2+bx$ MODULO $p$

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College,
Huaian, Jiangsu 223001, P.R. China

Received 1 December 2003;
revised 26 September 2005
Available online 15 December 2005

Communicated by David Goss

Abstract. Let $p>3$ be a prime and $a,b\in\mathbb{Z}$. In the paper we mainly determine the number $V_p(x^4+ax^2+bx)$ of incongruent residues of $x^4+ax^2+bx$ $(x\in\mathbb{Z})$ modulo $p$ and reveal the connections with elliptic curves over the field $\mathbb{F}_p$ of $p$ elements.

**MSC**: Primary 11A07; Secondary 11A15,11E25,11L10,14H52,11Y11
**Keywords**: The number of incongruent residues; Quartic polynomial; Congruence; Elliptic curve

## 1. Introduction.

Let $\mathbb{Z}$ be the set of integers. For a positive integer $m$ and given polynomial $f(x)$ with integral coefficients, denote the number of incongruent residues of $f(x)(x\in\mathbb{Z})$ modulo $m$ by $V_m(f(x))$. That is,

$$V_m(f(x))=\big|\big\{c\bigm| c\in\{0,1,\ldots,m-1\},\ f(x)\equiv c \pmod m \text{ is solvable}\big\}\big|.$$

Let $p>3$ be a prime, $a_1,a_2,a_3\in\mathbb{Z}$, and let $(\frac{d}{p})$ be the Legendre symbol. In 1908 R.D. von Sterneck[St] proved that if $a_1^2\not\equiv 3a_2 \pmod p$, then

$$V_p(x^3+a_1x^2+a_2x+a_3)=\frac{2p+(\frac{p}{3})}{3}. \tag{1.1}$$

This result was rediscovered by the author ([Su1, Theorem 4.3]). See also [K] and [MW1]. In the paper we give a general result for $V_m(x^3+a_1x^2+a_2x+a_3)$, where $m$ is a positive integer.

---

Email address: hyzhsun@public.hy.js.cn
URL: http://www.hytc.cn/xsjl/szh
Research of the author was supported by Natural Sciences Foundation of Jiangsu Educational Office (02KJB110007).

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

$$a=16a_2-6a_1^2,\ b=8(8a_3-4a_1a_2+a_1^3),\ c=256a_4-64a_1a_3+16a_1^2a_2-3a_1^4$$

and $X=4x+a_1$. Then we find

$$x^4+a_1x^3+a_2x^2+a_3x+a_4=\frac{1}{256}\big(X^4+aX^2+bX+c\big) \tag{1.2}$$

and so

$$V_p(x^4+a_1x^3+a_2x^2+a_3x+a_4)=V_p(x^4+ax^2+bx+c)=V_p(x^4+ax^2+bx). \tag{1.3}$$

Hence it suffices to discuss $V_p(x^4+ax^2+bx)$. In [MW2] K. McCann and K.S. Williams showed that

$$V_p(x^4+ax^2+bx)=\begin{cases}\frac{3}{8}p+O(1) & \text{if } p\nmid a \text{ and } p\mid b,\\ \frac{5}{8}p+O(\sqrt{p}) & \text{if } p\nmid b.\end{cases}$$

For a general estimate for $V_p(f(x))$ one may consult [BSD].

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

$$D(a,b,c)=-(4a^3+27b^2)b^2+16c(a^4+9ab^2-8a^2c+16c^2). \tag{1.4}$$

It is known that $D(a,b,c)$ is the discriminant of $x^4+ax^2+bx+c$ and $x^3+2ax^2+(a^2-4c)x-b^2$. From [Sk, Leo] and [Su3, Theorem 5.8] we have the following basic result for quartic congruences.

(1.5) Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$ and $p\nmid bD(a,b,c)$. Then the congruence $x^4+ax^2+bx+c\equiv 0 \pmod p$ is unsolvable 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 $(\frac{y}{p})=-1$.

On the basis of this result, in the paper we try to determine $V_p(x^4+ax^2+bx)(a,b\in\mathbb{Z})$ for any prime $p>3$ and obtain some explicit formulas.

Let $[\alpha]$ denote the greatest integer not exceeding $\alpha$. Let $\#E_p(x^3-Ax-B)$ be the number of points on the elliptic curve $E_p:\ y^2=x^3-Ax-B$ over the field $\mathbb{F}_p$ of $p$ elements. We list the following typical results in the paper.

(1.6) $V_p(x^4-6x^2+8x)=\big[\frac{5p+7}{8}\big]$.

(1.7) If $p\equiv 2 \pmod 3$ and $p\nmid b$, then $V_p(x^4+bx)=\big[\frac{5p+7}{8}\big]$.

(1.8) If $p\equiv 7 \pmod{12}$, $p\nmid b$ and $p=A^2+3B^2$ $(A,B\in\mathbb{Z})$ with $A\equiv 1 \pmod 3$, then

$$V_p(x^4+bx)=\begin{cases}\frac{1}{8}(5p+7+(-1)^{\frac{p-7}{12}}\cdot 6-4A) & \text{if } x^3\equiv 2b \pmod p \text{ is solvable},\\ \frac{1}{8}(5p+1+2A) & \text{if } x^3\equiv 2b \pmod p \text{ is unsolvable}.\end{cases}$$

(1.9) If $p\equiv 1 \pmod{12}$ and $p=A^2+3B^2(A,B\in\mathbb{Z})$, then

$$V_p(x^4+x)=\begin{cases}\frac{1}{8}\big(5p+9-(-1)^{\frac{p-1}{12}}\cdot 6\big) & \text{if } B\equiv 0 \pmod 3,\\ \frac{1}{8}(5p+3+6B) & \text{if } B\equiv 1 \pmod 3.\end{cases}$$

(1.10) If $p \equiv 1, 9 \pmod{40}$ and so $p = s^2 + 5t^2$ for some $s, t \in \mathbb{Z}$, then

$$V_p(x^4 - 4x^2 + 4x) = \frac{5p+3}{8} + \frac{1-(-1)^t}{2}.$$

(1.11) If $p \nmid ab$, $m \in \mathbb{Z}$ and $a^3 m \equiv b^2 \pmod{p}$, then

$$V_p(x^4 + ax^2 + bx) = V_p(x^4 + mx^2 + m^2 x).$$

(1.12) If $p \equiv 7 \pmod{120}$, then

$$V_p(x^4 - 4x^2 + 4x) = \frac{1}{8}\big(3p - 1 + 2\#E_p(x^3 - 12x - 11)\big).$$

(1.13) If $p \equiv 5 \pmod{12}$, then

$$V_p(x^4 - 3x^2 + 3x) = \frac{1}{8}\Big(6p + 6 + 2\Big(\frac{2^{\frac{p-2}{3}} + 1}{p}\Big) - \#E_p(x^3 - 12x + 20)\Big).$$

(1.14) If $p \equiv 5 \pmod{12}$ and $p = c^2 + d^2$ with $2 \mid d$, $c + d \equiv 1 \pmod{4}$ and $c \equiv d \pmod{3}$, then

$$V_p(x^4 - 3x^2 + 2x) = \frac{1}{8}\big(5p + 3 - 2d\big).$$

**2. On the value of $V_p(x^4 + ax^2 + bx)$ when $p$ is prime.**

Let $p$ be an odd prime and $ax \equiv c \pmod{p}$ with $a, c, x \in \mathbb{Z}$ and $p \nmid a$. Throughout this paper we use $\big(\frac{c/a}{p}\big)$ to denote the Legendre symbol $\big(\frac{x}{p}\big)$.

Let $a_1, a_2, a_3, a_4 \in \mathbb{Z}$. Since $x^2 \equiv x \pmod{2}$ and $x^3 \equiv x \pmod{3}$ we see that

$$\begin{aligned} &V_2(x^4 + a_1x^3 + a_2x^2 + a_3x + a_4) \\ &= V_2((1 + a_1 + a_2 + a_3)x + a_4) = \big(3 + (-1)^{a_1+a_2+a_3}\big)/2 \end{aligned}$$

and

$$\begin{aligned} &V_3(x^4 + a_1x^3 + a_2x^2 + a_3x + a_4) \\ &= V_3((1 + a_2)x^2 + (a_1 + a_3)x) = \begin{cases} 1 & \text{if } a_2 \equiv 2 \pmod{3} \text{ and } 3 \mid (a_1 + a_3), \\ 3 & \text{if } a_2 \equiv 2 \pmod{3} \text{ and } 3 \nmid (a_1 + a_3), \\ 2 & \text{otherwise.} \end{cases} \end{aligned}$$

Let $p > 3$ be a prime and $a, b \in \mathbb{Z}$. To determine the value of $V_p(x^4 + ax^2 + bx)$, we first deal with the simple case $b \equiv 0 \pmod{p}$.

**Theorem 2.1.** *Let $p$ be an odd prime, $a \in \mathbb{Z}$ and $p \nmid a$. Then*

$$V_p(x^4+ax^2) = \Big[\frac{3p+7-2(\frac{-a}{p})}{8}\Big]$$

Proof. Clearly

$$\begin{aligned} &V_p(x^4+ax^2) \\ &= \frac{p+1}{2} - \frac{1}{2}\Big|\Big\{(x,y) \mid x^4+ax^2 \equiv y^4+ay^2 \pmod p,\ x \neq y, \\ &\qquad x,y \in \{0,1,\dots,(p-1)/2\}\Big\}\Big| \\ &= \frac{p+1}{2} - \frac{1}{2}\Big|\Big\{(x,y) \mid x^2+y^2 \equiv -a \pmod p,\ x \neq y,\ x,y \in \{0,1,\dots,(p-1)/2\}\Big\}\Big| \\ &= \frac{p+1}{2} - \frac{1}{2}\Big|\Big\{(x,y) \mid x^2+y^2+a \equiv 0 \pmod p,\ x,y \in \{0,1,\dots,(p-1)/2\}\Big\}\Big| \\ &\qquad + \frac{1}{2}\Big|\Big\{(x,x) \mid 2x^2+a \equiv 0 \pmod p,\ x \in \{0,1,\dots,(p-1)/2\}\Big\}\Big| \\ &= \frac{p+1}{2} + \frac{1}{4}\Big(1+\Big(\frac{-2a}{p}\Big)\Big) - \frac{1}{2}\sum_{\substack{x=0 \\ (\frac{-x^2-a}{p})=0,1}}^{(p-1)/2} 1. \end{aligned}$$

Observe that

$$\sum_{\substack{x=0 \\ (\frac{-x^2-a}{p})=0,1}}^{(p-1)/2} 1 + \sum_{\substack{x=0 \\ (\frac{-x^2-a}{p})=-1}}^{(p-1)/2} 1 = \frac{p+1}{2}$$

and

$$\sum_{\substack{x=0 \\ (\frac{-x^2-a}{p})=0,1}}^{(p-1)/2} 1 - \sum_{\substack{x=0 \\ (\frac{-x^2-a}{p})=-1}}^{(p-1)/2} 1 = \sum_{x=0}^{(p-1)/2}\Big(\frac{-x^2-a}{p}\Big) + \frac{1+(\frac{-a}{p})}{2}.$$

We see that

$$\sum_{\substack{x=0 \\ (\frac{-x^2-a}{p})=0,1}}^{(p-1)/2} 1 = \frac{1}{2}\Big(\frac{p+1}{2} + \sum_{x=0}^{(p-1)/2}\Big(\frac{-x^2-a}{p}\Big) + \frac{1+(\frac{-a}{p})}{2}\Big).$$

From [BEW, p. 58] we know that $\sum_{x=0}^{p-1}\big(\frac{x^2+a}{p}\big) = -1$. Thus

$$\begin{aligned} \sum_{x=0}^{(p-1)/2}\Big(\frac{-x^2-a}{p}\Big) &= \Big(\frac{-a}{p}\Big) + \sum_{x=1}^{(p-1)/2}\Big(\frac{-x^2-a}{p}\Big) = \Big(\frac{-a}{p}\Big) + \frac{1}{2}\sum_{x=1}^{p-1}\Big(\frac{-x^2-a}{p}\Big) \\ &= \Big(\frac{-a}{p}\Big) + \frac{1}{2}\Big(\frac{-1}{p}\Big)\Big(\sum_{x=0}^{p-1}\Big(\frac{x^2+a}{p}\Big) - \Big(\frac{a}{p}\Big)\Big) \\ &= \Big(\frac{-a}{p}\Big) + \frac{1}{2}\Big(\frac{-1}{p}\Big)\Big(-1-\Big(\frac{a}{p}\Big)\Big) = \frac{1}{2}\Big(\Big(\frac{-a}{p}\Big) - \Big(\frac{-1}{p}\Big)\Big) \end{aligned}$$

and hence

$$\sum_{\substack{x=0\\ (\frac{-x^2-a}{p})=0,1}}^{(p-1)/2} 1 = \frac{1}{2}\Big(\frac{p+1}{2}+\frac{(\frac{-a}{p})-(\frac{-1}{p})}{2}+\frac{1+(\frac{-a}{p})}{2}\Big)$$
$$= \frac{1}{4}\Big(p+2-\Big(\frac{-1}{p}\Big)+2\Big(\frac{-a}{p}\Big)\Big).$$

Now combining the above we obtain

$$\begin{aligned} V_p(x^4+ax^2) &= \frac{p+1}{2}+\frac{1+(\frac{-2a}{p})}{4}-\frac{1}{8}\Big(p+2-\Big(\frac{-1}{p}\Big)+2\Big(\frac{-a}{p}\Big)\Big) \\ &= \frac{1}{8}\Big(3p+4+\Big(\frac{-1}{p}\Big)+2\Big(\frac{-a}{p}\Big)\Big(\Big(\frac{2}{p}\Big)-1\Big)\Big) \\ &= \Big[\frac{3p+7-2(\frac{-a}{p})}{8}\Big] \end{aligned}$$

as asserted.

Let $D(a,b,c)$ be given by (1.4). Then clearly

$$\begin{aligned} a^2D(a,b,c) =& 2ab^2(a^2+12c)^2+4c(2a^3-8ac+9b^2)^2 \\ & -3b^2(a^2+12c)(2a^3-8ac+9b^2). \end{aligned} \tag{2.1}$$

From [Su3, Lemma 4.1] we have

**Lemma 2.1.** *Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$, $p\nmid b$ and $p\mid D(a,b,c)$. Then the congruence $(*)$ $x^3+2ax^2+(a^2-4c)x-b^2\equiv 0 \pmod p$ has three solutions. If $p\mid(a^2+12c)$, then $x\equiv -2a/3 \pmod p$ is the triple solution of $(*)$. If $p\nmid(a^2+12c)$, then the three solutions of $(*)$ are given by*

$$x\equiv \frac{9b^2-32ac}{a^2+12c}, -\frac{2a^3-8ac+9b^2}{2(a^2+12c)}, -\frac{2a^3-8ac+9b^2}{2(a^2+12c)} \pmod p.$$

**Lemma 2.2.** *Let $p>3$ be a prime, $a,b\in\mathbb{Z}$, $p\nmid b$, and let $R_p$ be a complete set of residues modulo $p$. If $\delta(a,b,p)$ is the number of those $c\in R_p$ such that $p\mid D(a,b,c)$ and the congruence $x^3+2ax^2+(a^2-4c)x-b^2\equiv 0 \pmod p$ has a quadratic nonresidue solution, then*

$$\delta(a,b,p)=\Big|\Big\{y\mid 2y^3+2ay^2+b^2\equiv 0 \pmod p,\ \Big(\frac{y}{p}\Big)=-1,\ y\in R_p\Big\}\Big|.$$

Proof. We consider the following two cases.

**Case 1.** $8a^3+27b^2\equiv 0 \pmod p$. In this case, for $c\in\mathbb{Z}$ we have

$$2a^3-8ac+9b^2\equiv 2a^3-8ac-\frac{8}{3}a^3=-\frac{2a}{3}(a^2+12c) \pmod p.$$

This together with (2.1) yields

$$\begin{aligned} a^2 D(a,b,c) &\equiv (a^2+12c)^2\Big\{2ab^2 - 3b^2\Big(-\frac{2a}{3}\Big) + 4c\cdot\frac{4a^2}{9}\Big\} \\ &\equiv (a^2+12c)^2\Big\{4a\Big(-\frac{8}{27}a^3\Big) + \frac{16}{9}a^2c\Big\} \\ &= \frac{16}{9}a^2\Big(c-\frac{2}{3}a^2\Big)(a^2+12c)^2 \pmod p. \end{aligned}$$

As $p\nmid b$ we have $p\nmid a$. Thus

$$p \mid D(a,b,c) \iff c\equiv \frac{2a^2}{3} \pmod p \quad\text{or}\quad c\equiv -\frac{a^2}{12} \pmod p.$$

Clearly

$$\begin{aligned} &x^3+2ax^2+(a^2-4c)x-b^2 \\ &\equiv \begin{cases} \big(x+\frac{2a}{3}\big)^3 \pmod p & \text{if } c\equiv -\frac{a^2}{12} \pmod p, \\ \big(x-\frac{a}{3}\big)^2\big(x+\frac{8a}{3}\big) \pmod p & \text{if } c\equiv \frac{2a^2}{3} \pmod p. \end{cases} \end{aligned}$$

Since $b^2\equiv -\frac{8}{27}a^3 \pmod p$ we see that $-\frac{2a}{3}$ and $-\frac{8a}{3}$ are quadratic residues modulo $p$. Hence $\frac{a}{3}$ is a quadratic nonresidue modulo $p$ if and only if $\big(\frac{-2}{p}\big)=-1$. Thus, by the above and the definition of $\delta(a,b,p)$ we obtain

$$\delta(a,b,p) = \frac{1}{2}\Big(1-\Big(\frac{-2}{p}\Big)\Big).$$

On the other hand,

$$2y^3+2ay^2+b^2 \equiv 2y^3+2ay^2-\frac{8}{27}a^3 = 2\Big(y-\frac{a}{3}\Big)\Big(y+\frac{2a}{3}\Big)^2 \pmod p.$$

So we have

$$\begin{aligned} &\Big|\Big\{y \mid 2y^3+2ay^2+b^2\equiv 0 \pmod p,\ \Big(\frac{y}{p}\Big)=-1,\ y\in R_p\Big\}\Big| \\ &= \frac{1}{2}\Big(1-\Big(\frac{-2}{p}\Big)\Big) = \delta(a,b,p). \end{aligned}$$

**Case 2.** $8a^3+27b^2\not\equiv 0 \pmod p$. Let $c\in R_p$ be such that $p\mid D(a,b,c)$. We assert that $p\nmid (a^2+12c)$. If $p\mid (a^2+12c)$, by (2.1) we have $c(2a^3-8ac+9b^2)\equiv (8a^3+27b^2)c/3\equiv 0 \pmod p$. Thus $p\mid c$ and hence $p\mid a$. Applying (1.4) we see that $p\mid b$. This contradicts the assumption $p\nmid 8a^3+27b^2$. Thus the assertion is true.

Since $a^2+12c\not\equiv 0 \pmod p$, from Lemma 2.1 we know that the three solutions of the congruence $x^3+2ax^2+(a^2-4c)x-b^2\equiv 0 \pmod p$ are given by

$$x_1\equiv \frac{9b^2-32ac}{a^2+12c} \pmod p \quad\text{and}\quad x_2\equiv x_3\equiv -\frac{2a^3-8ac+9b^2}{2(a^2+12c)} \pmod p.$$

As $x_1x_2x_3 \equiv b^2 \pmod p$ we see that $\left(\frac{x_1}{p}\right) = 1$. Set

$$C = \Big\{c \,\Big|\, p \mid D(a,b,c),\ \Big(\frac{-2(a^2+12c)(2a^3-8ac+9b^2)}{p}\Big) = -1,\ c \in R_p\Big\}.$$

Then $\delta(a,b,p) = |C|$. It is easily seen that

$$\begin{aligned}
&2\Big(-\frac{2a^3-8ac+9b^2}{2(a^2+12c)}\Big)^3 + 2a\Big(-\frac{2a^3-8ac+9b^2}{2(a^2+12c)}\Big)^2 + b^2 \\
&= \frac{8a^3+27b^2}{4(a^2+12c)^3}\big(256c^3 - 128a^2c^2 + 16(a^4+9ab^2)c - (4a^3+27b^2)b^2\big) \\
&= \frac{8a^3+27b^2}{4(a^2+12c)^3} D(a,b,c).
\end{aligned}$$

Thus, if $c \in C$, then the congruence $2y^3 + 2ay^2 + b^2 \equiv 0 \pmod p$ has a quadratic nonresidue solution $y \equiv -(2a^3-8ac+9b^2)/(2(a^2+12c)) \pmod p$. Conversely, if $y$ is an integer such that $2y^3+2ay^2+b^2 \equiv 0 \pmod p$ and $\left(\frac{y}{p}\right) = -1$, then $y \not\equiv \frac{a}{3} \pmod p$ since $p \nmid 8a^3+27b^2$. Let $c \in R_p$ be given by $c \equiv -(2a^3+9b^2+2a^2y)/(24y-8a) \pmod p$. Then clearly $y \equiv -(2a^3-8ac+9b^2)/(2(a^2+12c)) \pmod p$ and so $p \mid D(a,b,c)$ by the above. Thus $c \in C$. Now it is clear that there is a one-to-one correspondence between $C$ and the set $S = \{y \mid 2y^3+2ay^2+b^2 \equiv 0 \pmod p,\ \left(\frac{y}{p}\right) = -1,\ y \in R_p\}$. This yields $\delta(a,b,p) = |C| = |S|$, which completes the proof.

Now we can prove

**Theorem 2.2.** *Let $p > 3$ be a prime and $a, b \in \mathbb{Z}$ with $p \nmid b$. Then*

$$V_p(x^4+ax^2+bx) = \frac{1}{8}\Big\{5p + 3 + 4\delta(a,b,p) + \sum_{x=1}^{p-1}\Big(\Big(\frac{x}{p}\Big) - 1\Big)\Big(\frac{x(x+2a)^2-4b^2}{p}\Big)\Big\},$$

*where*

$$\delta(a,b,p) = \Big|\Big\{y \mid 2y^3+2ay^2+b^2 \equiv 0 \pmod p,\ \Big(\frac{y}{p}\Big) = -1,\ y \in \{0,1,\dots,p-1\}\Big\}\Big|.$$

Proof. For a polynomial $f(x)$ with integral coefficients we let $N_p(f(x))$ denote the number of solutions of the congruence $f(x) \equiv 0 \pmod p$. Let $R_p = \{0,1,\dots,p-1\}$ and let $\alpha(a,b,p)$ denote the number of $c \in R_p$ such that $x^3+2ax^2+(a^2-4c)x-b^2 \equiv 0 \pmod p$ has a quadratic nonresidue solution. Since

$$V_p(x^4+ax^2+bx) = \Big|\Big\{c \mid x^4+ax^2+bx+c \equiv 0 \pmod p \text{ is solvable},\ c \in R_p\Big\}\Big|,$$

we see that

$$\begin{aligned}
&p - V_p(x^4+ax^2+bx)\\
&= \Big|\Big\{c \mid N_p(x^4+ax^2+bx+c)=0,\ c\in R_p\Big\}\Big|\\
&= \Big|\Big\{c \mid p\nmid D(a,b,c),\ N_p(x^4+ax^2+bx+c)=0,\ c\in R_p\Big\}\Big| \text{ (by [Su3, Lemma 5.1])}\\
&= \Big|\Big\{c \mid p\nmid D(a,b,c),\ x^3+2ax^2+(a^2-4c)x-b^2\equiv 0 \pmod p \text{ has a quadratic}\\
&\qquad \text{nonresidue solution},\ c\in R_p\Big\}\Big| \quad \text{(by(1.5))}\\
&= \alpha(a,b,p) - \Big|\Big\{c \mid p\mid D(a,b,c),\ x^3+2ax^2+(a^2-4c)x-b^2\equiv 0 \pmod p\\
&\qquad \text{has a quadratic nonresidue solution},\ c\in R_p\Big\}\Big|\\
&= \alpha(a,b,p)-\delta(a,b,p) \quad \text{(by Lemma 2.2)}.
\end{aligned}$$

Thus,

$$V_p(x^4+ax^2+bx) = p+\delta(a,b,p)-\alpha(a,b,p). \tag{2.2}$$

If $x_1, x_2, x_3$ are distinct integers such that

$$x_1^2+2ax_1+a^2-\frac{b^2}{x_1}\equiv x_2^2+2ax_2+a^2-\frac{b^2}{x_2}\equiv x_3^2+2ax_3+a^2-\frac{b^2}{x_3} \pmod p,$$

then clearly $x_1x_2x_3\equiv b^2 \pmod p$ by Vieta's theorem. This implies that $\left(\frac{x_1}{p}\right) = \left(\frac{x_2}{p}\right) = \left(\frac{x_3}{p}\right) = -1$ does not hold. From this we see that

$$\begin{aligned}
&\alpha(a,b,p)\\
&= \Big|\Big\{c \,\Big|\, c\equiv \frac{x^3+2ax^2+a^2x-b^2}{4x} \pmod p,\ \Big(\frac{x}{p}\Big)=-1,\ c\in R_p\Big\}\Big|\\
&= \Big|\Big\{c \,\Big|\, c\equiv x^2+2ax+a^2-\frac{b^2}{x} \pmod p,\ \Big(\frac{x}{p}\Big)=-1,\ c\in R_p\Big\}\Big|\\
&= \Big|\Big\{x \mid \Big(\frac{x}{p}\Big)=-1,\ x\in R_p\Big\}\Big| - \frac12\Big|\Big\{(x_1,x_2) \mid x_1^2+2ax_1+a^2-\frac{b^2}{x_1}\equiv x_2^2\\
&\quad +2ax_2+a^2-\frac{b^2}{x_2} \pmod p,\ \Big(\frac{x_1}{p}\Big)=\Big(\frac{x_2}{p}\Big)=-1,\ x_1\ne x_2,\ x_1,x_2\in R_p\Big\}\Big|\\
&= \frac{p-1}{2}-\frac12\Big|\Big\{(x_1,x_2) \mid x_1+x_2+2a+\frac{b^2}{x_1x_2}\equiv 0 \pmod p,\\
&\qquad \Big(\frac{x_1}{p}\Big)=\Big(\frac{x_2}{p}\Big)=-1,\ x_1\ne x_2,\ x_1,x_2\in R_p\Big\}\Big|\\
&= \frac{p-1}{2}-\frac12\Big|\Big\{(x_1,x_2) \mid x_1x_2^2+(2a+x_1)x_1x_2+b^2\equiv 0 \pmod p,\\
&\qquad \Big(\frac{x_1}{p}\Big)=\Big(\frac{x_2}{p}\Big)=-1,\ x_1\ne x_2,\ x_1,x_2\in R_p\Big\}\Big|\\
&= \frac{p-1}{2}-\frac{N-\delta(a,b,p)}{2},
\end{aligned}$$

where

$$N = \Big|\Big\{(x_1,x) \;\Big|\; x_1x^2+(2a+x_1)x_1x+b^2 \equiv 0 \pmod p,\ \big(\frac{x}{p}\big) = \big(\frac{x_1}{p}\big) = -1,\ x_1,x \in R_p\Big\}\Big|.$$

Thus, by (2.2) we have

$$\begin{aligned} V_p(x^4+ax^2+bx) &= p+\delta(a,b,p) - \Big(\frac{p-1}{2} - \frac{N-\delta(a,b,p)}{2}\Big) \\ &= \frac{1}{2}\big(p+1+\delta(a,b,p)+N\big). \end{aligned} \tag{2.3}$$

Suppose $x_1 \in R_p$ and $(\frac{x_1}{p}) = -1$. Set $\Delta = (2a+x_1)^2x_1^2 - 4b^2x_1$. Then clearly $\Delta \not\equiv 0 \pmod p$ and

$$N_p\big(x_1x^2+(2a+x_1)x_1x+b^2\big) = 1 + \Big(\frac{\Delta}{p}\Big).$$

If $\big(\frac{\Delta}{p}\big) = 1$, then the two solutions $x_2, x_3$ of the congruence $x_1x^2+(2a+x_1)x_1x+b^2 \equiv 0 \pmod p$ satisfy the relation $x_2x_3 \equiv \frac{b^2}{x_1} \pmod p$. Hence $\big(\frac{x_2}{p}\big)\big(\frac{x_3}{p}\big) = \big(\frac{x_1}{p}\big) = -1$. So we have

$$\begin{aligned} N &= \Big|\Big\{x_1 \;\Big|\; \Big(\frac{x_1}{p}\Big) = -1,\ \Big(\frac{\Delta}{p}\Big) = 1,\ x_1 \in R_p\Big\}\Big| \\ &= \Big|\Big\{x \;\Big|\; \Big(\frac{x}{p}\Big) = \Big(\frac{x(x+2a)^2-4b^2}{p}\Big) = -1,\ x \in R_p\Big\}\Big|. \end{aligned}$$

From this it's easy to see that

$$\sum_{x\in R_p}\Big(1-\Big(\frac{x}{p}\Big)\Big)\Big(1-\Big(\frac{x(x+2a)^2-4b^2}{p}\Big)\Big) = 4N+1-\Big(\frac{-1}{p}\Big).$$

Thus, noting that $\sum_{x\in R_p}\big(\frac{x}{p}\big) = 0$ we obtain

$$\begin{aligned} N &= \frac{1}{4}\Big\{\sum_{x\in R_p}\Big(1-\Big(\frac{x}{p}\Big)\Big)\Big(1-\Big(\frac{x(x+2a)^2-4b^2}{p}\Big)\Big) - 1 + \Big(\frac{-1}{p}\Big)\Big\} \\ &= \frac{1}{4}\Big\{p-1+\Big(\frac{-1}{p}\Big) - \sum_{x\in R_p}\Big(\frac{x(x+2a)^2-4b^2}{p}\Big) + \sum_{x\in R_p}\Big(\frac{x}{p}\Big)\Big(\frac{x(x+2a)^2-4b^2}{p}\Big)\Big\} \\ &= \frac{1}{4}\Big\{p-1+\sum_{x=1}^{p-1}\Big(\Big(\frac{x}{p}\Big)-1\Big)\Big(\frac{x(x+2a)^2-4b^2}{p}\Big)\Big\}. \end{aligned}$$

This together with (2.3) gives the result.

From Theorem 2.2 we have

**Theorem 2.3.** *Let $p > 3$ be a prime, $a, b \in \mathbb{Z}$ and $p \nmid ab$. Then $V_p(x^4 + ax^2 + bx)$ depends only on $p$ and $b^2/a^3 \pmod p$. Moreover, if $k \in \mathbb{Z}$ and $k \equiv b^2/(2a^3) \pmod p$, then*

$$\begin{aligned} &V_p(x^4 + ax^2 + bx) \\ &= \frac{1}{8}\Big\{5p + 2 + (-1)^{\frac{p-1}{2}} + 4\delta(k,p) + \Big(\frac{p}{3}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3 - (18k+3)x - (27k^2+18k+2)}{p}\Big) \\ &\quad - \Big(\frac{p}{3}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\Big)\Big\}, \end{aligned}$$

*where*

$$\delta(k,p) = \Big|\Big\{x \mid x^3+4kx+8k^2 \equiv 0 \pmod p,\ \Big(\frac{x}{p}\Big) = -1,\ x \in \{1,2,\dots,p-1\}\Big\}\Big|. \quad (2.4)$$

Proof. Let $R_p = \{0, 1, \dots, p-1\}$ and let $\delta(a, b, p)$ be given as in Theorem 2.2. Since $(\frac{2ak}{p}) = 1$ we see that

$$\begin{aligned} \delta(a,b,p) &= \Big|\Big\{x \mid 2(2akx)^3 + 2a(2akx)^2 + 2a^3k \equiv 0 \pmod p,\ \Big(\frac{x}{p}\Big) = -1,\ x \in R_p\Big\}\Big| \\ &= \Big|\Big\{x \mid 8k^2x^3 + 4kx^2 + 1 \equiv 0 \pmod p,\ \Big(\frac{x}{p}\Big) = -1,\ x \in R_p\Big\}\Big| \\ &= \delta(k,p). \end{aligned}$$

On the other hand, observing that $x(x+1)^2 - k = \frac{1}{27}((3x+2)^3 - 3(3x+2) - 27k - 2)$ we obtain

$$\begin{aligned} &\sum_{x=1}^{p-1}\Big(\frac{x(x+2a)^2 - 4b^2}{p}\Big) \\ &= \sum_{x=1}^{p-1}\Big(\frac{2ax(2ax+2a)^2 - 4b^2}{p}\Big) = \sum_{x=1}^{p-1}\Big(\frac{k}{p}\Big)\Big(\frac{x(x+1)^2 - k}{p}\Big) \\ &= \sum_{x=0}^{p-1}\Big(\frac{k}{p}\Big)\Big(\frac{x(x+1)^2 - k}{p}\Big) - \Big(\frac{-1}{p}\Big) \\ &= \Big(\frac{k}{p}\Big)\sum_{x=0}^{p-1}\Big(\frac{27((3x+2)^3 - 3(3x+2) - 27k - 2)}{p}\Big) - \Big(\frac{-1}{p}\Big) \\ &= \Big(\frac{3k}{p}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3 - 3x - 27k - 2}{p}\Big) - \Big(\frac{-1}{p}\Big) \\ &= \Big(\frac{-3}{p}\Big)\sum_{x=0}^{p-1}\Big(\frac{-k^3x^3 + 3k^3x + k^3(27k+2)}{p}\Big) - \Big(\frac{-1}{p}\Big) \\ &= \Big(\frac{p}{3}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\Big) - \Big(\frac{-1}{p}\Big). \end{aligned}$$

Also, since $y^3+y^2-2ky+k^2 = -\frac{1}{27}((-3y-1)^3-3(6k+1)(-3y-1)-(27k^2+18k+2))$ we have

$$\begin{aligned}
&\sum_{x=1}^{p-1}\Big(\frac{x}{p}\Big)\Big(\frac{x(x+2a)^2-4b^2}{p}\Big)\\
&=\sum_{x=1}^{p-1}\Big(\frac{2ax}{p}\Big)\Big(\frac{2ax(2ax+2a)^2-4b^2}{p}\Big)=\sum_{x=1}^{p-1}\Big(\frac{x}{p}\Big)\Big(\frac{x(x+1)^2-k}{p}\Big)\\
&=\sum_{x=1}^{p-1}\Big(\frac{1+\frac{2}{x}+\frac{1}{x^2}-\frac{k}{x^3}}{p}\Big)=\sum_{t=1}^{p-1}\Big(\frac{1+2t+t^2-kt^3}{p}\Big)\\
&=\sum_{t=1}^{p-1}\Big(\frac{-k^3t^3+k^2t^2+2k^2t+k^2}{p}\Big)=\sum_{y=0}^{p-1}\Big(\frac{y^3+y^2-2ky+k^2}{p}\Big)-1\\
&=\sum_{y=0}^{p-1}\Big(\frac{-3}{p}\Big)\Big(\frac{(-3y-1)^3-3(6k+1)(-3y-1)-(27k^2+18k+2)}{p}\Big)-1\\
&=\Big(\frac{p}{3}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-(18k+3)x-(27k^2+18k+2)}{p}\Big)-1.
\end{aligned}$$

Now putting all the above together with Theorem 2.2 yields the result.

**Corollary 2.1.** *Let $p>3$ be a prime, $a,b\in\mathbb{Z}$ and $p\nmid ab$. If $m$ is an integer such that $a^3m\equiv b^2 \pmod p$, then*

$$V_p(x^4+ax^2+bx)=V_p(x^4+mx^2+m^2x).$$

Proof. This is immediate from Theorem 2.3.

For any prime $p>3$ let $\mathbb{F}_p$ be the field consisting of residue classes modulo $p$, and let $\#E_p(x^3-Ax-B)$ be the number of points on the elliptic curve $E_p:\ y^2=x^3-Ax-B$ over $\mathbb{F}_p$.

**Corollary 2.2.** *Let $p>3$ be a prime, and $k\in\mathbb{Z}$ with $p\nmid k$. Then*

$$\begin{aligned}
&V_p(x^4+2kx^2+4k^2x)\\
&=\frac{1}{8}\Big\{5p+2+(-1)^{\frac{p-1}{2}}+4\delta(k,p)+\Big(\frac{p}{3}\Big)\{\#E_p(x^3-(18k+3)x-27k^2-18k-2)\\
&\quad-\#E_p(x^3-3k^2x+k^3(27k+2))\}\Big\},
\end{aligned}$$

*where $\delta(k,p)$ is given by (2.4).*

Proof. Let $f(x)$ be a polynomial with integral coefficients, and $N_p(y^2=f(x))$ denote the number of solutions $(x,y)$ of the congruence $y^2\equiv f(x) \pmod p$. It is easily seen that

$$N_p(y^2=f(x)) = \sum_{\substack{x=0\\ (\frac{f(x)}{p})=0}}^{p-1} 1 + 2\sum_{\substack{x=0\\ (\frac{f(x)}{p})=1}}^{p-1} 1 = p + \sum_{\substack{x=0\\ (\frac{f(x)}{p})=1}}^{p-1} 1 - \sum_{\substack{x=0\\ (\frac{f(x)}{p})=-1}}^{p-1} 1$$
$$= p + \sum_{x=0}^{p-1}\Big(\frac{f(x)}{p}\Big).$$

Thus for $A, B \in \mathbb{Z}$ we have

$$\#E_p(x^3-Ax-B) = 1 + N_p(y^2 = x^3-Ax-B) = p+1+\sum_{x=0}^{p-1}\Big(\frac{x^3-Ax-B}{p}\Big). \quad (2.5)$$

Now putting $a=2k$ and $b=4k^2$ in Theorem 2.3 and then applying the above we obtain the result.

**Remark 2.1** Let $p>3$ be a prime, $k\in\mathbb{Z}$ and $p\nmid k$. By (2.5) we have

$$\begin{aligned}\#E_p(x^3-3k^2x+k^3(27k+2)) &= p+1+\sum_{x=0}^{p-1}\Big(\frac{x^3-3k^2x+k^3(27k+2)}{p}\Big)\\ &= p+1+\sum_{x=0}^{p-1}\Big(\frac{(kx)^3-3k^2\cdot kx+k^3(27k+2)}{p}\Big)\\ &= p+1+\Big(\frac{k}{p}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-3x+27k+2}{p}\Big)\\ &= p+1+\Big(\frac{k}{p}\Big)\big(\#E_p(x^3-3x+27k+2)-p-1\big).\end{aligned}$$

Hence

$$\#E_p(x^3-3k^2x+k^3(27k+2)) = \begin{cases} \#E_p(x^3-3x+27k+2) & \text{if } (\frac{k}{p})=1,\\ 2p+2-\#E_p(x^3-3x+27k+2) & \text{if } (\frac{k}{p})=-1.\end{cases}$$

From Corollary 2.2 we have

**Corollary 2.3.** *Let $p>3$ be a prime, and $k\in\mathbb{Z}$ with $p\nmid k$. Then*

$$\begin{aligned}&\#E_p(x^3-3k^2x+k^3(27k+2)) - \#E_p(x^3-(18k+3)x-(27k^2+18k+2))\\ &\equiv 4\delta(k,p)+2-2\Big(\frac{-2}{p}\Big) \pmod 8.\end{aligned}$$

Proof. From Corollary 2.2 we see that

$$\begin{aligned}
&\#E_p(x^3-3k^2x+k^3(27k+2))-\#E_p(x^3-(18k+3)x-(27k^2+18k+2))\\
&\equiv\Big(\frac p3\Big)\Big(5p+2+\Big(\frac{-1}{p}\Big)+4\delta(k,p)\Big)\equiv\Big(\frac p3\Big)\Big(p-\Big(\frac{-1}{p}\Big)+2\Big(1-\Big(\frac{-1}{p}\Big)\Big)+4\delta(k,p)\Big)\\
&\equiv 4\Big(\frac14\Big(p-\Big(\frac{-1}{p}\Big)\Big)+\frac12\Big(1-\Big(\frac{-1}{p}\Big)\Big)+\delta(k,p)\Big)\\
&\equiv 4\Big(\frac12\Big(1-\Big(\frac{2}{p}\Big)\Big)+\frac12\Big(1-\Big(\frac{-1}{p}\Big)\Big)+\delta(k,p)\Big)\\
&\equiv 4\Big(\frac12\Big(1-\Big(\frac{-2}{p}\Big)\Big)+\delta(k,p)\Big)\ (\mathrm{mod}\ 8).
\end{aligned}$$

So the corollary is proved.

**Conjecture 2.1.** Let $p>3$ be a prime, and $k\in\mathbb{Z}$ with $p\nmid k(27k+4)$. Then

$$\#E_p(x^3-(18k+3)x-(27k^2+18k+2))\equiv 0\ (\mathrm{mod}\ 3).$$

**Theorem 2.4.** *Let $p>3$ be a prime. If $a,b\in\mathbb{Z}$, $p\nmid ab$ and $8a^3\equiv-27b^2\ (\mathrm{mod}\ p)$, then*

$$V_p(x^4+ax^2+bx)=\Big[\frac{5p+7}{8}\Big].$$

Proof. Let $k\in\mathbb{Z}$ be such that $k\equiv\frac{b^2}{2a^3}\equiv-\frac{4}{27}\ (\mathrm{mod}\ p)$. Then clearly

$$x^3+4kx+8k^2\equiv x^3-\frac{16}{27}x+\frac{8\cdot16}{27^2}=\Big(x-\frac49\Big)^2\Big(x+\frac89\Big)\ (\mathrm{mod}\ p).$$

From this and (2.4) we see that

$$\delta(k,p)=\frac12\Big(1-\Big(\frac{-2}{p}\Big)\Big).$$

On the other hand, setting $x=\frac49y$ we find

$$\begin{aligned}
x^3-3k^2x+k^3(27k+2)&\equiv x^3-\frac{48}{27^2}x+\frac{128}{27^3}=\frac{64}{729}\Big(y^3-\frac13y+\frac{2}{27}\Big)\\
&\equiv\frac{64}{729}(y^3-(18k+3)y-(27k^2+18k+2))\ (\mathrm{mod}\ p).
\end{aligned}$$

Thus,

$$\sum_{x=0}^{p-1}\Big(\frac{x^3-3k^2x+k^3(27k+2)}{p}\Big)=\sum_{x=0}^{p-1}\Big(\frac{x^3-(18k+3)x-(27k^2+18k+2)}{p}\Big).$$

Now applying the above and Theorem 2.3 we get

$$\begin{aligned}
V_p(x^4+ax^2+bx)&=\frac18\Big\{5p+2+\Big(\frac{-1}{p}\Big)+2\Big(1-\Big(\frac{-2}{p}\Big)\Big)\Big\}\\
&=\frac18\Big\{5p+4-2\Big(\frac{-2}{p}\Big)+\Big(\frac{-1}{p}\Big)\Big\}=\Big[\frac{5p+7}{8}\Big].
\end{aligned}$$

This proves the theorem.

**Corollary 2.4.** *Let $p > 3$ be a prime. Then*

$$V_p(x^4 - 6x^2 + 8x) = \Big[\frac{5p+7}{8}\Big].$$

Proof. Putting $a = -6$ and $b = 8$ in Theorem 2.4 we get the result.

**Theorem 2.5.** *Let $p > 3$ be a prime, and $a, b \in \mathbb{Z}$ with $p \nmid b$. Then*

$$\Big|V_p(x^4 + ax^2 + bx) - \frac{5p}{8}\Big| \le \frac{1}{2}\sqrt{p} + \frac{15}{8}.$$

Proof. If $p \nmid a$, letting $k \equiv b^2/(2a^3) \pmod p$ and then using Theorem 2.3 we see that

$$\begin{aligned}&|8V_p(x^4 + ax^2 + bx) - 5p| \\ &\le \Big|2 + \Big(\frac{-1}{p}\Big) + 4\delta(k,p)\Big| + \Big|\sum_{x=0}^{p-1}\Big(\frac{x^3 - (18k+3)x - (27k^2+18k+2)}{p}\Big)\Big| \\ &\quad + \Big|\sum_{x=0}^{p-1}\Big(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\Big)\Big|.\end{aligned}$$

By Weil's estimate ([BEW, p.183]) we have

$$\Big|\sum_{x=0}^{p-1}\Big(\frac{x^3 - (18k+3)x - (27k^2+18k+2)}{p}\Big)\Big| \le 2\sqrt{p}$$

and

$$\Big|\sum_{x=0}^{p-1}\Big(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\Big)\Big| \le 2\sqrt{p}.$$

As $0 \le \delta(k,p) \le 3$, applying the above we obtain

$$\Big|V_p(x^4 + ax^2 + bx) - \frac{5p}{8}\Big| \le \frac{2+1+4\cdot 3}{8} + \frac{4\sqrt{p}}{8} = \frac{1}{2}\sqrt{p} + \frac{15}{8}.$$

If $p \mid a$, then $V_p(x^4 + ax^2 + bx) = V_p(x^4 + bx)$. It follows from Theorem 2.2 that

$$\begin{aligned}&8V_p(x^4 + bx) - 5p \\ &= 3 + 4\delta(0,b,p) + \sum_{x=1}^{p-1}\Big(\frac{x}{p}\Big)\Big(\frac{x^3 - 4b^2}{p}\Big) - \sum_{x=1}^{p-1}\Big(\frac{x^3 - 4b^2}{p}\Big).\end{aligned}$$

Since

$$\sum_{x=1}^{p-1}\Big(\frac{x^4-4b^2x}{p}\Big)=\sum_{x=1}^{p-1}\Big(\frac{1-4b^2/x^3}{p}\Big)=\sum_{t=1}^{p-1}\Big(\frac{1-4b^2t^3}{p}\Big)$$
$$=\Big(\frac{-2b}{p}\Big)\sum_{t=1}^{p-1}\Big(\frac{-2b+8b^3t^3}{p}\Big)=\Big(\frac{-2b}{p}\Big)\sum_{x=1}^{p-1}\Big(\frac{x^3-2b}{p}\Big)$$
$$=\Big(\frac{-2b}{p}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-2b}{p}\Big)-1,$$

we see that

$$8V_p(x^4+bx)-5p$$
$$=2+\Big(\frac{-1}{p}\Big)+4\delta(0,b,p)+\Big(\frac{-2b}{p}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-2b}{p}\Big)-\sum_{x=0}^{p-1}\Big(\frac{x^3-4b^2}{p}\Big). \tag{2.6}$$

Thus, using Weil's estimate we also get

$$|8V_p(x^4+ax^2+bx)-5p|\le 2+1+4\cdot 3+2\sqrt{p}+2\sqrt{p}.$$

This yields the result and hence the proof is complete.

**Theorem 2.6.** *Let $p\equiv 2 \pmod 3$ be an odd prime, $b\in\mathbb{Z}$ and $p\nmid b$. Then*

$$V_p(x^4+bx)=\Big[\frac{5p+7}{8}\Big].$$

Proof. Let

$$\delta(0,b,p)=\Big|\Big\{y \mid 2y^3+b^2\equiv 0 \pmod p,\ \Big(\frac{y}{p}\Big)=-1,\ y\in\{0,1,\dots,p-1\}\Big\}\Big|.$$

Since $p\equiv 2 \pmod 3$ we know that the congruence $x^3\equiv t \pmod p$ has one and only one solution for any given integer $t$. So we have

$$\delta(0,b,p)=\frac{1}{2}\Big(1-\Big(\frac{-2}{p}\Big)\Big)$$

and

$$\sum_{x=0}^{p-1}\Big(\frac{x^3+m}{p}\Big)=\sum_{y=0}^{p-1}\Big(\frac{y+m}{p}\Big)=\sum_{x=0}^{p-1}\Big(\frac{x}{p}\Big)=0\quad\text{for}\quad m\in\mathbb{Z}. \tag{2.7}$$

Hence, by (2.6) we have

$$V_p(x^4+bx)=\frac{1}{8}\Big\{5p+2+(-1)^{\frac{p-1}{2}}+2\Big(1-\Big(\frac{-2}{p}\Big)\Big)\Big\}$$
$$=\frac{1}{8}\Big(5p+4+\Big(\frac{-1}{p}\Big)-2\Big(\frac{-2}{p}\Big)\Big)=\Big[\frac{5p+7}{8}\Big].$$

This completes the proof.

**Theorem 2.7.** *Let* $p \equiv 1 \pmod 3$ *be a prime,* $p = A^2 + 3B^2 (A, B \in \mathbb{Z})$, $A \equiv 1 \pmod 3$, $b \in \mathbb{Z}$ *and* $p \nmid b$.

(i) *If* $p \equiv 1 \pmod{12}$, *then*

$$V_p(x^4 + bx) = \begin{cases} \frac{1}{8}\big(5p + 9 - 6(-1)^{\frac{p-1}{12}}\big) & \text{if } 2b \text{ is a cubic residue} \pmod p, \\ \frac{1}{8}(5p + 3 \pm 6B) & \text{if } (2b)^{\frac{p-1}{3}} \equiv \frac{1}{2}\big(-1 \mp \frac{A}{B}\big) \pmod p. \end{cases}$$

(ii) *If* $p \equiv 7 \pmod{12}$, *then*

$$V_p(x^4 + bx) = \begin{cases} \frac{1}{8}(5p + 7 + 6(-1)^{\frac{p-7}{12}} - 4A) & \text{if } 2b \text{ is a cubic residue} \pmod p, \\ \frac{1}{8}(5p + 1 + 2A) & \text{if } 2b \text{ is a cubic nonresidue} \pmod p. \end{cases}$$

Proof. Let $a \in \mathbb{Z}$ be such that $p \nmid a$. The cubic Jacobsthal sums $\phi_3(a)$ and $\psi_3(a)$ are defined by

$$\phi_3(a) = \sum_{x=1}^{p-1} \Big(\frac{x}{p}\Big)\Big(\frac{x^3 + a}{p}\Big) \quad \text{and} \quad \psi_3(a) = \sum_{x=1}^{p-1} \Big(\frac{x^3 + a}{p}\Big).$$

It is clear that

$$\Big(\frac{a}{p}\Big)\phi_3(a^{-1}) = \sum_{x=1}^{p-1} \Big(\frac{x}{p}\Big)\Big(\frac{ax^3 + 1}{p}\Big) = \sum_{x=1}^{p-1} \Big(\frac{a + \frac{1}{x^3}}{p}\Big) = \sum_{y=1}^{p-1} \Big(\frac{y^3 + a}{p}\Big) = \psi_3(a).$$

From [BEW, Theorem 6.2.10, pp. 195-196] we have

$$\phi_3(a) = \begin{cases} -1 - 2A & \text{if } a \text{ is a cubic residue} \pmod p, \\ -1 + A \pm 3B & \text{if } a^{\frac{p-1}{3}} \equiv \frac{1}{2}\big(-1 \pm \frac{A}{B}\big) \pmod p. \end{cases} \tag{2.8}$$

Hence

$$\Big(\frac{a}{p}\Big)\psi_3(a) = \phi_3(a^{-1}) = \begin{cases} -1 - 2A & \text{if } a \text{ is a cubic residue} \pmod p, \\ -1 + A \pm 3B & \text{if } a^{\frac{p-1}{3}} \equiv \frac{1}{2}\big(-1 \mp \frac{A}{B}\big) \pmod p. \end{cases} \tag{2.9}$$

Observe that $(4b^2)^{\frac{p-1}{3}} \equiv (2b)^{-\frac{p-1}{3}} \pmod p$. From (2.6) and the above we deduce that

$$\begin{aligned} &8V_p(x^4 + bx) - 5p - 3 - 4\delta(0, b, p) \\ &= \Big(\frac{-2b}{p}\Big)\psi_3(-2b) - \psi_3(-4b^2) = \phi_3\Big(-\frac{1}{2b}\Big) - \Big(\frac{-4b^2}{p}\Big)\phi_3\Big(-\frac{1}{4b^2}\Big) \\ &= \begin{cases} -1 - 2A - \big(\frac{-1}{p}\big)(-1 - 2A) & \text{if } 2b \text{ is a cubic residue} \pmod p, \\ -1 + A \pm 3B - \big(\frac{-1}{p}\big)(-1 + A \mp 3B) & \text{if } (2b)^{\frac{p-1}{3}} \equiv \frac{1}{2}\big(-1 \mp \frac{A}{B}\big) \pmod p. \end{cases} \end{aligned}$$

This together with the fact

$$\begin{aligned}\delta(0,b,p)&=\Big|\Big\{y\mid y^3\equiv -\frac{b^2}{2}\pmod p,\ \Big(\frac{y}{p}\Big)=-1,\ y\in\{0,1,\dots,p-1\}\Big\}\Big|\\&=\begin{cases}3 & \text{if } (\frac{-2}{p})=-1 \text{ and } 2b \text{ is a cubic residue} \pmod p,\\ 0 & \text{otherwise}\end{cases}\\&=\begin{cases}3 & \text{if } p\equiv 7,13 \pmod{24} \text{ and } 2b \text{ is a cubic residue} \pmod p,\\ 0 & \text{otherwise}\end{cases}\end{aligned}$$

yields the desired result.

Let $p$ be a prime of the form $3k+1$. Assume $p=A^2+3B^2$ and $4p=L^2+27M^2$ with $A,B,L,M\in\mathbb{Z}$. If 2 is a cubic residue of $p$, it is well known that $3\mid B$, $2\mid L$ and $2\mid M$ (see [IR, p. 119]). Thus

$$A=\pm\frac{L}{2},\ B=\pm\frac{3M}{2},\ L=\pm 2A,\ M=\pm\frac{2B}{3}. \tag{2.10}$$

If 2 is a cubic nonresidue of $p$, then $3\nmid AB$ and $2\nmid LM$. Thus we may choose the signs of $A,B,L$ and $M$ such that

$$L\equiv 1 \pmod 3,\ M\equiv L \pmod 4 \quad\text{and}\quad A\equiv B\equiv 1 \pmod 3.$$

Now it is easy to check that

$$A=\frac{L-9M}{4},\ B=\frac{L+3M}{4},\ L=A+3B \quad\text{and}\quad M=\frac{B-A}{3}. \tag{2.11}$$

In [L1], E. Lehmer showed that $2^{\frac{p-1}{3}}\equiv (L+9M)/(L-9M)\pmod p$. (See also [IR, p. 137] and [Su1, Theorem 2.1].) Thus applying (2.11) we obtain

$$2^{\frac{p-1}{3}}\equiv\frac{(A+3B)+9(B-A)/3}{(A+3B)-9(B-A)/3}=\frac{-1+3B/A}{2}\equiv\frac{-1-A/B}{2}\pmod p. \tag{2.12}$$

Now from Theorem 2.7 and (2.12) we have

**Corollary 2.5.** *Let $p\equiv 1\pmod 6$ be a prime and $p=A^2+3B^2$ with $A\equiv 1\pmod 3$ and $B\equiv 0,1\pmod 3$.*

(i) *If $p\equiv 1\pmod{12}$, then*

$$V_p(x^4\pm x)=\begin{cases}\frac18\big(5p+9-(-1)^{\frac{p-1}{12}}\cdot 6\big) & \text{if } B\equiv 0\pmod 3,\\ \frac18(5p+3+6B) & \text{if } B\equiv 1\pmod 3.\end{cases}$$

(ii) *If $p\equiv 7\pmod{12}$, then*

$$V_p(x^4\pm x)=\begin{cases}\frac18(5p+7+(-1)^{\frac{p-7}{12}}\cdot 6-4A) & \text{if } B\equiv 0\pmod 3,\\ \frac18(5p+1+2A) & \text{if } B\equiv 1\pmod 3.\end{cases}$$

**Remark 2.2** Suppose that $p\equiv 1\pmod 3$ is a prime and $p=A^2+3B^2$ with $A\equiv 1\pmod 3$. If $2b$ is a cubic nonresidue of $p$, using (2.11) and [Su1, Theorem 2.1] we can determine the sign of $B$ so that $(2b)^{\frac{p-1}{3}}\equiv\frac12\big(-1-\frac{A}{B}\big)\pmod p$ and hence $V_p(x^4+bx)=\frac18(5p+3+6B)$ for $p\equiv 1\pmod{12}$.

**Theorem 2.8.** *Let $p$ be a prime greater than 3. Let $a, b \in \mathbb{Z}$ be such that $p \nmid ab$ and $a^3 \equiv -4b^2 \pmod{p}$ (for example $a = -4$ and $b = 4$). Let*

$$\delta(p) = \begin{cases} 0 & \text{if } p \equiv 7, 17, 23, 33 \pmod{40}, \\ 1 & \text{if } p \equiv 3, 13, 27, 31, 37, 39 \pmod{40} \\ 2 & \text{if } p \equiv 11, 19 \pmod{40}, \\ 1 - (-1)^t & \text{if } p \equiv 1, 9 \pmod{40} \text{ and } p = s^2 + 5t^2 (s, t \in \mathbb{Z}), \\ 2 + (-1)^t & \text{if } p \equiv 21, 29 \pmod{40} \text{ and } p = s^2 + 5t^2 (s, t \in \mathbb{Z}). \end{cases}$$

(i) *If $p \equiv 1 \pmod{4}$, then*

$$V_p(x^4 + ax^2 + bx) = \frac{1}{8}\big(5p + 3 + 4\delta(p)\big).$$

(ii) *If $p \equiv 7 \pmod{12}$, then*

$$V_p(x^4 + ax^2 + bx) = \frac{1}{8}\big(3p - 1 + 4\delta(p) + 2\#E_p(x^3 - 12x - 11)\big).$$

(iii) *If $p \equiv 11 \pmod{12}$, then*

$$V_p(x^4 + ax^2 + bx) = \frac{1}{8}\big(7p + 3 + 4\delta(p) - 2\#E_p(x^3 - 12x - 11)\big).$$

Proof. Let $k \in \mathbb{Z}$ be such that $k \equiv \frac{b^2}{2a^3} \equiv -\frac{1}{8} \pmod{p}$. Let $\delta(k, p)$ be given by (2.4) and $R_p = \{0, 1, \dots, p-1\}$. Then

$$\begin{aligned} \delta(k,p) &= \Big|\Big\{x \mid x^3 - \frac{1}{2}x + \frac{1}{8} \equiv 0 \pmod{p},\ \Big(\frac{x}{p}\Big) = -1,\ x \in R_p\Big\}\Big| \\ &= \Big|\Big\{x \;\Big|\; \Big(x - \frac{1}{2}\Big)\Big(x^2 + \frac{1}{2}x - \frac{1}{4}\Big) \equiv 0 \pmod{p},\ \Big(\frac{x}{p}\Big) = -1,\ x \in R_p\Big\}\Big| \\ &= \frac{1 - (\frac{2}{p})}{2} + \Big|\Big\{x \mid x^2 + \frac{x}{2} - \frac{1}{4} \equiv 0 \pmod{p},\ \Big(\frac{x}{p}\Big) = -1,\ x \in R_p\Big\}\Big| \\ &= \frac{1 - (\frac{2}{p})}{2} + \Big|\Big\{y \;\Big|\; \Big(\frac{y}{4}\Big)^2 + \frac{1}{2} \cdot \frac{y}{4} - \frac{1}{4} \equiv 0 \pmod{p},\ \Big(\frac{y}{p}\Big) = -1,\ y \in R_p\Big\}\Big| \\ &= \frac{1 - (\frac{2}{p})}{2} + \Big|\Big\{y \mid y^2 + 2y - 4 \equiv 0 \pmod{p},\ \Big(\frac{y}{p}\Big) = -1,\ y \in R_p\Big\}\Big| \\ &= \frac{1 - (\frac{2}{p})}{2} + \Big|\Big\{y \mid (y+1)^2 \equiv 5 \pmod{p},\ \Big(\frac{y}{p}\Big) = -1,\ y \in R_p\Big\}\Big|. \end{aligned}$$

Thus, if $p \equiv 2, 3 \pmod{5}$, then $(\frac{5}{p}) = -1$ and so $\delta(k, p) = \frac{1}{2}(1 - (\frac{2}{p})) = \delta(p)$. If $p \equiv 11, 19 \pmod{20}$, then

$$\Big(\frac{-1 + \sqrt{5}}{p}\Big)\Big(\frac{-1 - \sqrt{5}}{p}\Big) = \Big(\frac{(-1 + \sqrt{5})(-1 - \sqrt{5})}{p}\Big) = \Big(\frac{-4}{p}\Big) = -1$$

and so $\delta(k,p)=\frac{1}{2}(1-(\frac{2}{p}))+1=\delta(p)$. If $p\equiv 1,9 \pmod{20}$, we see that $\big(\frac{-1+\sqrt5}{p}\big)\big(\frac{-1-\sqrt5}{p}\big)$ $=\big(\frac{-4}{p}\big)=1$ and thus

$$\delta(k,p)=\frac{1-(\frac{2}{p})}{2}+1-\Big(\frac{1+\sqrt5}{p}\Big)=\frac{3-(\frac{2}{p})}{2}-\Big(\frac{2}{p}\Big)\Big(\frac{(1+\sqrt5)/2}{p}\Big).$$

It is well known that $p=s^2+5t^2$ for some $s,t\in\mathbb{Z}$. From [Br] or [Su4, Remark 6.1] we know that $\big(\frac{(1+\sqrt5)/2}{p}\big)=(-1)^t$. Thus

$$\delta(k,p)=\frac{3-(\frac{2}{p})}{2}-\Big(\frac{2}{p}\Big)(-1)^t=\delta(p).$$

Since $k\equiv -\frac{1}{8} \pmod p$, we see that

$$\begin{aligned}&\sum_{x=0}^{p-1}\Big(\frac{x^3-(18k+3)x-(27k^2+18k+2)}{p}\Big)\\&=\sum_{x=0}^{p-1}\Big(\frac{x^3-\frac{3}{4}x-\frac{11}{64}}{p}\Big)=\sum_{y=0}^{p-1}\Big(\frac{\frac{y^3}{4^3}-\frac{3}{4}\cdot\frac{y}{4}-\frac{11}{64}}{p}\Big)=\sum_{y=0}^{p-1}\Big(\frac{y^3-12y-11}{p}\Big)\end{aligned}$$

and

$$\begin{aligned}&\sum_{x=0}^{p-1}\Big(\frac{x^3-3k^2x+k^3(27k+2)}{p}\Big)\\&=\sum_{x=0}^{p-1}\Big(\frac{x^3-\frac{3}{64}x+\frac{11}{64^2}}{p}\Big)=\sum_{y=0}^{p-1}\Big(\frac{(-\frac{y}{16})^3-\frac{3}{64}(-\frac{y}{16})+\frac{11}{64^2}}{p}\Big)\\&=\sum_{y=0}^{p-1}\Big(\frac{-1}{p}\Big)\Big(\frac{y^3-12y-11}{p}\Big).\end{aligned}$$

Now combining the above with Theorem 2.3 and (2.5) we obtain

$$\begin{aligned}&V_p(x^4+ax^2+bx)\\&=\frac{1}{8}\Big\{5p+2+(-1)^{\frac{p-1}{2}}+4\delta(p)+\Big(\frac{p}{3}\Big)\big(1-(-1)^{\frac{p-1}{2}}\big)\sum_{y=0}^{p-1}\Big(\frac{y^3-12y-11}{p}\Big)\Big\}\\&=\frac{1}{8}\Big\{5p+2+(-1)^{\frac{p-1}{2}}+4\delta(p)+\Big(\frac{p}{3}\Big)\big(1-(-1)^{\frac{p-1}{2}}\big)\big(\#E_p(x^3-12x-11)-p-1\big)\Big\}.\end{aligned}$$

This yields the result.

**Remark 2.3** If $p>3$ is a prime of the form $4n+3$, from Theorem 2.8 we deduce the following congruence

$$\#E_p(x^3-12x-11)\equiv\begin{cases}2 \pmod 4 & \text{if } p\equiv 3,7 \pmod{20},\\ 0 \pmod 4 & \text{if } p\equiv 11,19 \pmod{20}.\end{cases}$$

If $p$ is a prime greater than 5, we conjecture that

$$\#E_p(x^3-12x-11)\equiv\begin{cases}6 \pmod{12} & \text{if } p\equiv 3,7 \pmod{20},\\ 0 \pmod{12} & \text{if } p\equiv 1,9,11,13,17,19 \pmod{20}.\end{cases}$$

**Theorem 2.9.** *Let $p$ be a prime greater than 3. Let $a, b \in \mathbb{Z}$ be such that $p \nmid ab$ and $a^3 \equiv -3b^2 \pmod p$ (for example $a = -3$ and $b = 3$). Let*

$$\delta(p) = \Big|\Big\{t \mid t^3 \equiv 2 \pmod p,\ \Big(\frac{t+1}{p}\Big) = -\Big(\frac{2}{p}\Big),\ t \in \{0, 1, \dots, p-1\}\Big\}\Big|.$$

(i) *If $p \equiv 1 \pmod{12}$ and $p = A^2 + 3B^2 (A, B \in \mathbb{Z})$ with $A \equiv 1 \pmod 3$, then*

$$V_p(x^4 + ax^2 + bx) = \begin{cases} \frac{1}{8}\big(6p + 4 + 4\delta(p) - 2A - \#E_p(x^3 - 12x + 20)\big) & \text{if } B \equiv 0 \pmod 3, \\ \frac{1}{8}\big(6p + 4 + A + 3B - \#E_p(x^3 - 12x + 20)\big) & \text{if } B \equiv 1 \pmod 3. \end{cases}$$

(ii) *If $p \equiv 5 \pmod{12}$, then*

$$V_p(x^4 + ax^2 + bx) = \frac{1}{8}\Big(6p + 6 + 2\Big(\frac{2^{\frac{p-2}{3}} + 1}{p}\Big) - \#E_p(x^3 - 12x + 20)\Big).$$

(iii) *If $p \equiv 7 \pmod{12}$ and $p = A^2 + 3B^2 (A, B \in \mathbb{Z})$ with $A \equiv 1 \pmod 3$, then*

$$V_p(x^4 + ax^2 + bx) = \begin{cases} \frac{1}{8}\big(4p + 4\delta(p) - 2A + \#E_p(x^3 - 12x + 20)\big) & \text{if } B \equiv 0 \pmod 3, \\ \frac{1}{8}\big(4p + A + 3B + \#E_p(x^3 - 12x + 20)\big) & \text{if } B \equiv 1 \pmod 3. \end{cases}$$

(iv) *If $p \equiv 11 \pmod{12}$, then*

$$V_p(x^4 + ax^2 + bx) = \frac{1}{8}\Big(4p + 2 + 2\Big(\frac{2^{\frac{p-2}{3}} + 1}{p}\Big) + \#E_p(x^3 - 12x + 20)\Big).$$

Proof. Let $k$ be an integer such that $k \equiv \frac{b^2}{2a^3} \equiv -\frac{1}{6} \pmod p$. Set

$$S = \sum_{x=0}^{p-1}\Big(\frac{x^3 - (18k+3)x - 27k^2 - 18k - 2}{p}\Big)$$

and

$$T = \sum_{x=0}^{p-1}\Big(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\Big).$$

If $p \equiv 2 \pmod 3$, then $S = \sum_{x=0}^{p-1}\big(\frac{x^3 + \frac{1}{4}}{p}\big) = 0$ by (2.7). If $p \equiv 1 \pmod 3$ and $p = A^2 + 3B^2$ with $A \equiv 1 \pmod 3$ and $B \equiv 0, 1 \pmod 3$, applying (2.8), (2.9) and (2.12) we see that

$$\begin{aligned} S - 1 &= \sum_{x=1}^{p-1}\Big(\frac{x^3 + \frac{1}{4}}{p}\Big) = \psi_3\Big(\frac{1}{4}\Big) = \phi_3(4) \\ &= \begin{cases} -1 - 2A & \text{if 2 is a cubic residue} \pmod p, \\ -1 + A \pm 3B & \text{if } 2^{\frac{p-1}{3}} \equiv \frac{1}{2}\big(-1 \mp \frac{A}{B}\big) \pmod p \end{cases} \\ &= \begin{cases} -1 - 2A & \text{if } B \equiv 0 \pmod 3, \\ -1 + A + 3B & \text{if } B \equiv 1 \pmod 3. \end{cases} \end{aligned}$$

We also have

$$\begin{aligned}
T &= \sum_{x=0}^{p-1}\Big(\frac{x^3-\frac{1}{12}x+\frac{5}{432}}{p}\Big) = \sum_{y=0}^{p-1}\Big(\frac{\frac{1}{12^3}y^3-\frac{1}{12^2}y+\frac{5}{432}}{p}\Big) \\
&= \sum_{y=0}^{p-1}\Big(\frac{12^3}{p}\Big)\Big(\frac{y^3-12y+20}{p}\Big) = \Big(\frac{3}{p}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-12x+20}{p}\Big) \\
&= (-1)^{\frac{p-1}{2}}\Big(\frac{p}{3}\Big)\big(\#E_p(x^3-12x+20)-p-1\big).
\end{aligned}$$

Let $R_p=\{0,1,\dots,p-1\}$. By (2.4) we have

$$\begin{aligned}
\delta(k,p) &= \Big|\Big\{x \mid x^3-\frac{2}{3}x+\frac{2}{9}\equiv 0 \pmod p,\ \Big(\frac{x}{p}\Big)=-1,\ x\in R_p\Big\}\Big| \\
&= \Big|\Big\{y \mid -\frac{y^3}{3^3}-\frac{2}{3}\Big(-\frac{y}{3}\Big)+\frac{2}{9}\equiv 0 \pmod p,\ \Big(\frac{y}{p}\Big)=-\Big(\frac{-3}{p}\Big),\ y\in R_p\Big\}\Big| \\
&= \Big|\Big\{y \mid y^3-6y-6\equiv 0 \pmod p,\ \Big(\frac{y}{p}\Big)=-\Big(\frac{p}{3}\Big),\ y\in R_p\Big\}\Big|.
\end{aligned}$$

If $p\equiv 1 \pmod 3$, putting $a_1=0$ and $a_2=a_3=-6$ in [Su3, Theorem 4.5] we see that $x^3-6x-6\equiv 0 \pmod p$ has three solutions if and only if $x^3\equiv 2 \pmod p$ is solvable (that is $3\mid B$). Moreover, if $t^3\equiv 2 \pmod p$ for $t\in\mathbb{Z}$, then $x\equiv(t^2+2)/t\equiv t(t+1) \pmod p$ is a solution of $x^3-6x-6\equiv 0 \pmod p$ with $(\frac{x}{p})=(\frac{2}{p})(\frac{t+1}{p})$. Thus, in view of [Su3, Lemma 2.2] we have $\delta(k,p)=\delta(p)$ or 0 according as $3\mid B$ or $3\nmid B$. If $p\equiv 2 \pmod 3$, from [Su3, Lemma 2.2] we know that the congruence $x^3-6x-6\equiv 0 \pmod p$ has the unique solution $x\equiv 2^{\frac{p+1}{3}}(2^{\frac{p-2}{3}}+1) \pmod p$. We thus have $\delta(k,p)=\frac{1}{2}(1+(\frac{2^{\frac{p-2}{3}}+1}{p}))$.

From Theorem 2.3 we know that

$$V_p(x^4+ax^2+bx)=\frac{1}{8}\Big\{5p+2+(-1)^{\frac{p-1}{2}}+4\delta(k,p)+\Big(\frac{p}{3}\Big)(S-T)\Big\}.$$

Now putting all the above together we obtain the result.

**Lemma 2.3.** *Let $p$ be a prime greater than 3. Then*

$$\begin{aligned}
&\#E_p(x^3-15x+22)-p-1 \\
&= \sum_{x=0}^{p-1}\Big(\frac{x^3-15x+22}{p}\Big) \\
&= \begin{cases} -2A & \text{if } p\equiv 1 \pmod 3 \text{ and } p=A^2+3B^2 \text{ with } A\equiv 1 \pmod 3, \\ 0 & \text{if } p\equiv 2 \pmod 3. \end{cases}
\end{aligned}$$

Proof. From [W, p. 295] or [BEW, Ex. 21, p. 208] we know that

$$1+\sum_{n=0}^{p-1}\Big(\frac{(n^2+4n+1)(n^2+2n)}{p}\Big)=\begin{cases} -2A & \text{if } p\equiv 1 \pmod 3, \\ 0 & \text{if } p\equiv 2 \pmod 3. \end{cases}$$

As

$$\begin{aligned}
&1+\sum_{n=0}^{p-1}\Big(\frac{(n^2+4n+1)(n^2+2n)}{p}\Big)\\
&=1+\sum_{n=1}^{p-1}\Big(\frac{n^4+6n^3+9n^2+2n}{p}\Big)=1+\sum_{n=1}^{p-1}\Big(\frac{1+\frac{6}{n}+\frac{9}{n^2}+\frac{2}{n^3}}{p}\Big)\\
&=\sum_{x=0}^{p-1}\Big(\frac{1+6x+9x^2+2x^3}{p}\Big)=\sum_{x=0}^{p-1}\Big(\frac{4+24x+36x^2+8x^3}{p}\Big)\\
&=\sum_{x=0}^{p-1}\Big(\frac{x^3+9x^2+12x+4}{p}\Big)=\sum_{x=0}^{p-1}\Big(\frac{(x-3)^3+9(x-3)^2+12(x-3)+4}{p}\Big)\\
&=\sum_{x=0}^{p-1}\Big(\frac{x^3-15x+22}{p}\Big),
\end{aligned}$$

by the above and (2.5) we obtain the result.

**Theorem 2.10.** *Let $p$ be a prime greater than 3. Let $a,b\in\mathbb{Z}$, $p\nmid ab$ and $4a^3\equiv -27b^2 \pmod p$ (for example $a=-3$ and $b=2$).*

(i) *If $p\equiv 1 \pmod{12}$ and $p=A^2+3B^2=c^2+d^2$ with $2\mid d$, $c+d\equiv 1 \pmod 4$ and $A\equiv 1 \pmod 3$, then*

$$V_p(x^4+ax^2+bx)=\begin{cases}\frac18\big(5p+3+4\delta(p)-2A-2c\big) & \text{if } 3\mid c,\\ \frac18\big(5p+3+4\delta(p)-2A+2c\big) & \text{if } 3\mid d,\end{cases}$$

*where*

$$\delta(p)=\begin{cases}1 & \text{if } p\equiv 13 \pmod{24},\\ 0 & \text{if } p\equiv 1 \pmod{24} \text{ and } B\equiv d \pmod 8,\\ 2 & \text{if } p\equiv 1 \pmod{24} \text{ and } B\not\equiv d \pmod 8.\end{cases}$$

(ii) *If $p\equiv 5 \pmod{12}$ and $p=c^2+d^2$ with $2\mid d$, $c+d\equiv 1 \pmod 4$ and $c\equiv d \pmod 3$, then*

$$V_p(x^4+ax^2+bx)=\frac18\big(5p+3-2d\big).$$

(iii) *If $p\equiv 7 \pmod{12}$ and $p=A^2+3B^2$ with $A\equiv 1 \pmod 3$, then*

$$V_p(x^4+ax^2+bx)=\frac18\big(5p+1-2A\big).$$

(iv) *If $p\equiv 11 \pmod{12}$, then*

$$V_p(x^4+ax^2+bx)=\begin{cases}\frac{5p+1}{8}+\frac12\Big(1-\Big(\frac{3^{\frac{p+1}{4}}+1}{p}\Big)\Big) & \text{if } p\equiv 11 \pmod{24},\\ \frac58(p+1) & \text{if } p\equiv 23 \pmod{24}.\end{cases}$$

Proof. Let $k \in \mathbb{Z}$ be such that $k \equiv \frac{b^2}{2a^3} \equiv -\frac{2}{27} \pmod p$. Let $\delta(k,p)$ be given by (2.4) and $R_p = \{0, 1, \dots, p-1\}$. Then

$$\begin{aligned}
\delta(k,p) &= \left|\left\{x \mid x^3 - \frac{8}{27}x + \frac{32}{27^2} \equiv 0 \pmod p,\ \left(\frac{x}{p}\right) = -1,\ x \in R_p\right\}\right| \\
&= \left|\left\{x \mid \left(x - \frac{4}{9}\right)\left(\left(x + \frac{2}{9}\right)^2 - \frac{4}{27}\right) \equiv 0 \pmod p,\ \left(\frac{x}{p}\right) = -1,\ x \in R_p\right\}\right| \\
&= \left|\left\{x \mid \left(x + \frac{2}{9}\right)^2 \equiv \frac{4}{27} \pmod p,\ \left(\frac{x}{p}\right) = -1,\ x \in R_p\right\}\right| \\
&= \left|\left\{x \mid \left(-\frac{2y}{9} + \frac{2}{9}\right)^2 \equiv \frac{4}{27} \pmod p,\ \left(\frac{-2y}{p}\right) = -1,\ y \in R_p\right\}\right| \\
&= \left|\left\{y \mid (y-1)^2 \equiv 3 \pmod p,\ \left(\frac{y}{p}\right) = -\left(\frac{-2}{p}\right),\ y \in R_p\right\}\right|.
\end{aligned}$$

Thus, if $p \equiv 5, 7 \pmod{12}$, then $\left(\frac{3}{p}\right) = -1$ and so $\delta(k,p) = 0$. If $p \equiv 13, 23 \pmod{24}$, then

$$\left(\frac{1+\sqrt{3}}{p}\right)\left(\frac{1-\sqrt{3}}{p}\right) = \left(\frac{(1+\sqrt{3})(1-\sqrt{3})}{p}\right) = \left(\frac{-2}{p}\right) = -1$$

and so $\delta(k,p) = 1$. If $p \equiv 1, 11 \pmod{24}$, we see that $\left(\frac{1+\sqrt{3}}{p}\right)\left(\frac{1-\sqrt{3}}{p}\right) = \left(\frac{-2}{p}\right) = 1$ and thus $\delta(k,p) = 1 - \left(\frac{1+\sqrt{3}}{p}\right)$. When $p \equiv 11 \pmod{24}$, we have $\left(3^{\frac{p+1}{4}}\right)^2 \equiv 3 \pmod p$ and so $\delta(k,p) = 1 - \left(\frac{1+3^{\frac{p+1}{4}}}{p}\right)$.

When $p \equiv 1 \pmod{24}$, then $p = A^2 + 3B^2 = c^2 + d^2$ with $B \equiv d \equiv 0 \pmod 4$. It is well known that $2^{\frac{p-1}{4}} \equiv (-1)^{\frac{d}{4}} \pmod p$. Also,

$$\left(\frac{1+\sqrt{3}}{p}\right) = (1+\sqrt{3})^{\frac{p-1}{2}} = 2^{\frac{p-1}{4}}(2+\sqrt{3})^{\frac{p-1}{4}} \equiv (-1)^{\frac{d}{4}}(2+\sqrt{3})^{\frac{p-1}{4}} \pmod p.$$

From [L2] or [Su4, Theorem 8.1 (with $m = 4$, $n = 2$, $d = 3$ and $k = 8$)] we have

$$(2+\sqrt{3})^{\frac{p-1}{4}} \equiv (-1)^{\frac{B}{4}} \pmod p. \tag{2.13}$$

Thus

$$\left(\frac{1+\sqrt{3}}{p}\right) = (-1)^{\frac{B-d}{4}}. \tag{2.14}$$

Hence $\delta(k,p) = 1 - \left(\frac{1+\sqrt{3}}{p}\right) = \delta(p)$.

Using Lemma 2.3 we see that

$$\begin{aligned}
&\sum_{x=0}^{p-1}\Big(\frac{x^3-(18k+3)x-27k^2-18k-2}{p}\Big)\\
&=\sum_{x=0}^{p-1}\Big(\frac{x^3-\frac{5}{3}x-\frac{22}{27}}{p}\Big)=\sum_{y=0}^{p-1}\Big(\frac{(-\frac{y}{3})^3-\frac{5}{3}\cdot(-\frac{y}{3})-\frac{22}{27}}{p}\Big)\\
&=\Big(\frac{-3}{p}\Big)\sum_{y=0}^{p-1}\Big(\frac{y^3-15y+22}{p}\Big)\\
&=\begin{cases}-2A & \text{if } p\equiv 1 \pmod 3 \text{ and } p=A^2+3B^2 \text{ with } A\equiv 1 \pmod 3,\\ 0 & \text{if } p\equiv 2 \pmod 3.\end{cases}
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\sum_{x=0}^{p-1}\Big(\frac{x^3-3k^2x+k^3(27k+2)}{p}\Big)\\
&=\sum_{x=0}^{p-1}\Big(\frac{x^3-\frac{12}{27^2}x}{p}\Big)=\sum_{y=0}^{p-1}\Big(\frac{\frac{1}{27^3}y^3-\frac{12}{27^2}\cdot\frac{y}{27}}{p}\Big)=\sum_{y=0}^{p-1}\Big(\frac{27^3}{p}\Big)\Big(\frac{y^3-12y}{p}\Big)\\
&=\Big(\frac{3}{p}\Big)\sum_{x=1}^{p-1}\Big(\frac{x^3-12x}{p}\Big)=\Big(\frac{3}{p}\Big)\phi_2(-12),
\end{aligned}$$

where

$$\phi_2(D)=\sum_{x=1}^{p-1}\Big(\frac{x^3+Dx}{p}\Big)\quad\text{for}\quad D\in\mathbb{Z}.$$

Suppose $p\nmid D$. If $p\equiv 3 \pmod 4$, we see that

$$\phi_2(D)=\sum_{y=1}^{p-1}\Big(\frac{(-y)^3+D(-y)}{p}\Big)=\Big(\frac{-1}{p}\Big)\phi_2(D)\quad\text{and so}\quad \phi_2(D)=0. \tag{2.15}$$

If $p\equiv 1 \pmod 4$, we may write $p=c^2+d^2 (c,d\in\mathbb{Z})$ with $2\mid d$ and $c+d\equiv 1 \pmod 4$. Since $p\equiv 1 \pmod 8 \Leftrightarrow 4\mid d\Leftrightarrow c\equiv 1 \pmod 4$ we see that $-(-1)^{\frac{p-1}{4}}c\equiv -1 \pmod 4$. Hence by [BEW, Theorem 6.2.9, p. 195] we have

$$\phi_2(-D)=\begin{cases}\pm 2\big(-(-1)^{\frac{p-1}{4}}c\big) & \text{if } (-D)^{\frac{p-1}{4}}\equiv\pm 1 \pmod p,\\ \pm 2d & \text{if } (-D)^{\frac{p-1}{4}}\equiv\pm\frac{d}{-(-1)^{\frac{p-1}{4}}c} \pmod p.\end{cases}$$

Thus

$$\phi_2(-D)=\begin{cases}\mp 2c & \text{if } D^{\frac{p-1}{4}}\equiv\pm 1 \pmod p,\\ \mp 2d & \text{if } D^{\frac{p-1}{4}}\equiv\pm\frac{d}{c} \pmod p.\end{cases} \tag{2.16}$$

Since

$$12^{\frac{p-1}{4}} = (-3)^{\frac{p-1}{4}} \cdot (-1)^{\frac{p-1}{4}} \cdot 2^{\frac{p-1}{2}} \equiv (-3)^{\frac{p-1}{4}} \cdot (-1)^{\frac{p-1}{4}} \Big(\frac{2}{p}\Big) = (-3)^{\frac{p-1}{4}} \pmod p,$$

by (2.16) we have

$$\phi_2(-12) = \begin{cases} \mp 2c & \text{if } (-3)^{\frac{p-1}{4}} \equiv \pm 1 \pmod p, \\ \mp 2d & \text{if } (-3)^{\frac{p-1}{4}} \equiv \pm \frac{d}{c} \pmod p. \end{cases}$$

From [Su2, Theorem 2.2 and Example 2.1] we know that

$$(-3)^{\frac{p-1}{4}} \equiv \begin{cases} 1 \pmod p & \text{if } 3 \mid d, \\ -1 \pmod p & \text{if } 3 \mid c, \\ \pm \frac{d}{c} \pmod p & \text{if } c \equiv \mp d \pmod 3. \end{cases}$$

Thus

$$\phi_2(-12) = \begin{cases} -2c & \text{if } 3 \mid d, \\ 2c & \text{if } 3 \mid c, \\ \pm 2d & \text{if } c \equiv \pm d \pmod 3. \end{cases} \tag{2.17}$$

From the above we see that

$$\begin{aligned} &\Big(\frac{p}{3}\Big) \sum_{x=0}^{p-1} \Big(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\Big) \\ &= \Big(\frac{p}{3}\Big)\Big(\frac{3}{p}\Big)\phi_2(-12) = (-1)^{\frac{p-1}{2}}\phi_2(-12) \\ &= \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4, \\ 2c & \text{if } p \equiv 1 \pmod 4 \text{ and } 3 \mid c, \\ -2c & \text{if } p \equiv 1 \pmod 4 \text{ and } 3 \mid d, \\ \pm 2d & \text{if } p \equiv 1 \pmod 4 \text{ and } c \equiv \pm d \pmod 3. \end{cases} \end{aligned}$$

By Theorem 2.3,

$$\begin{aligned} &V_p(x^4 + ax^2 + bx) \\ &= \frac{1}{8}\Big\{5p + 2 + (-1)^{\frac{p-1}{2}} + 4\delta(k,p) + \Big(\frac{p}{3}\Big) \sum_{x=0}^{p-1} \Big(\frac{x^3 - (18k+3)x - (27k^2+18k+2)}{p}\Big) \\ &\quad - \Big(\frac{p}{3}\Big) \sum_{x=0}^{p-1} \Big(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\Big)\Big\}. \end{aligned}$$

Now putting all the above together we deduce the result.

**3. The values of $V_m(x^2)$ and $V_m(x^3+a_1x^2+a_2x+a_3)$.**

For any positive integer $m$ and polynomial $f(x)$ with integral coefficients let

$$S_m(f(x)) = \big\{c \bigm| f(x)\equiv c \pmod m \quad \text{is solvable, } c\in\{0,1,\dots,m-1\}\big\}.$$

Then clearly $V_m(f(x)) = |S_m(f(x))|$.

**Theorem 3.1.** *Suppose that $f(x)$ is a polynomial with integral coefficients and $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is the prime decomposition of $m$. Then*

$$V_m(f(x)) = V_{p_1^{\alpha_1}}(f(x))\cdots V_{p_r^{\alpha_r}}(f(x)).$$

Proof. For $a,c\in\{0,1,\dots,m-1\}$ and $i\in\{1,2,\dots,r\}$ let $a_i,c_i\in\{0,1,\dots,p_i^{\alpha_i}-1\}$ be given by $a\equiv a_i \pmod{p_i^{\alpha_i}}$ and $c\equiv c_i \pmod{p_i^{\alpha_i}}$. It is clear that

$$\begin{aligned} f(a)\equiv c \pmod m &\iff f(a)\equiv c \pmod{p_i^{\alpha_i}}\ (i=1,2,\dots,r)\\ &\iff f(a)\equiv c_i \pmod{p_i^{\alpha_i}}\ (i=1,2,\dots,r)\\ &\iff f(a_i)\equiv c_i \pmod{p_i^{\alpha_i}}\ (i=1,2,\dots,r).\end{aligned}$$

Thus

$$c\in S_m(f(x)) \iff c_i\in S_{p_i^{\alpha_i}}(f(x))\ (i=1,2,\dots,r).$$

Now applying the Chinese Remainder Theorem we see that

$$V_m(f(x)) = |S_m(f(x))| = \prod_{i=1}^r \big|\, S_{p_i^{\alpha_i}}(f(x))\,\big| = \prod_{i=1}^r V_{p_i^{\alpha_i}}(f(x)).$$

This proves the theorem.

**Theorem 3.2.** *Let $p>1$ be odd. Then $p$ is a prime if and only if $0^2,1^2,2^2,\dots,(\frac{p-1}{2})^2$ are pairwise distinct modulo $p$. Namely, $p$ is a prime if and only if $V_p(x^2)=\frac{p+1}{2}$.*

Proof. If $p$ is a prime, it is well known that $0^2,1^2,2^2,\dots,(\frac{p-1}{2})^2$ are pairwise distinct modulo $p$. If $p$ is composite, then there are two odd numbers $d$ and $d'$ such that $1<d'\le d<p$ and $dd'=p$. Set $x_1=(d+d')/2$ and $x_2=(d-d')/2$. Then clearly $x_1,x_2\in\{0,1,\cdots,p-1\}$ and $x_1^2-x_2^2=(x_1+x_2)(x_1-x_2)=dd'=p$. Let $y_1=\min\{x_1,p-x_1\}$ and $y_2=\min\{x_2,p-x_2\}$. Then $y_1,y_2\in\{0,1,\dots,(p-1)/2\}$ and $y_1^2\equiv x_1^2\equiv x_2^2\equiv y_2^2 \pmod p$. Since $x_1+x_2=d$ and $x_1-x_2=d'$ we see that $x_1\ne x_2, p-x_2$ and so $y_1\ne y_2$. Thus $0^2,1^2,2^2,\dots,(\frac{p-1}{2})^2$ are not pairwise distinct modulo $p$ and hence $V_p(x^2)<\frac{p+1}{2}$. This proves the theorem.

For a given polynomial $f(x)$ we let $f'(x)$ denote the derivative of $f(x)$. If $p$ is a prime and $f(x_0)\equiv 0 \pmod{p^{\alpha-1}}$ for $x_0\in\mathbb{Z}$ and $\alpha>1$, using the binomial theorem one can easily derive that

$$f(x_0+sp^{\alpha-1})\equiv f(x_0)+sp^{\alpha-1}f'(x_0) \pmod{p^\alpha} \quad \text{for} \quad s\in\mathbb{Z}.$$

From this we deduce

**Lemma 3.1.** *Suppose that $p$ is a prime and $f(x)$ is a polynomial with integral coefficients. If there is an integer $x_0$ such that $f(x_0) \equiv 0 \pmod p$ and $p \nmid f'(x_0)$, then for any positive integer $\alpha$ the congruence $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable.*

Lemma 3.1 can be deduced from Hensel's lemma. See [HW, Theorem 123, pp. 96-97] and [R, Theorem 4.14].

**Theorem 3.3.** *If $m > 1$ is odd and $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime decomposition of $m$, then*

$$V_m(x^2) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} + p_i + 2 + (p_i - 1)(1 - (-1)^{\alpha_i})/2}{2(p_i + 1)}.$$

Proof. Let $p$ be an odd prime and let $\alpha \geq 2$ be a positive integer. We assert that

$$V_{p^\alpha}(x^2) = V_{p^{\alpha-2}}(x^2) + \frac{p^{\alpha-1}(p-1)}{2}. \tag{3.1}$$

If $c \in \mathbb{Z}$ and $p \nmid c$, it follows from Lemma 3.1 that $x^2 \equiv c \pmod{p^\alpha}$ is solvable if and only if $x^2 \equiv c \pmod p$ is solvable. Suppose $S_p(x^2) = \{0, a_1, a_2, \ldots, a_{\frac{p-1}{2}}\}$. We then have

$$\big\{c \bigm| c \in S_{p^\alpha}(x^2),\ p \nmid c\big\} = \big\{a_i + sp \mid i = 1, 2, \ldots, (p-1)/2,\ s = 0, 1, \ldots, p^{\alpha-1} - 1\big\}$$

and thus

$$\big|\big\{c \bigm| c \in S_{p^\alpha}(x^2),\ p \nmid c\big\}\big| = p^{\alpha-1}(p-1)/2.$$

If $c \in S_{p^\alpha}(x^2)$ and $p \mid c$, then $x^2 \equiv c \pmod{p^\alpha}$ for some $x \in \mathbb{Z}$. As $p \mid c$ we have $p \mid x$ and so $p^2 \mid c$. For $t \in \mathbb{Z}$, clearly $x^2 \equiv p^2 t \pmod{p^\alpha}$ is solvable if and only if $y^2 \equiv t \pmod{p^{\alpha-2}}$ is solvable. Thus

$$\big|\big\{c \bigm| c \in S_{p^\alpha}(x^2),\ p \mid c\big\}\big| = \big|\big\{t \mid t \in S_{p^{\alpha-2}}(x^2)\big\}\big| = V_{p^{\alpha-2}}(x^2).$$

Hence

$$\begin{aligned} V_{p^\alpha}(x^2) &= \big|\big\{c \bigm| c \in S_{p^\alpha}(x^2),\ p \mid c\big\}\big| + \big|\big\{c \bigm| c \in S_{p^\alpha}(x^2),\ p \nmid c\big\}\big| \\ &= V_{p^{\alpha-2}}(x^2) + p^{\alpha-1}(p-1)/2. \end{aligned}$$

This proves the assertion (3.1).

Observe that $V_p(x^2) = \frac{p+1}{2}$ and $V_1(x^2) = 1$. Using (3.1) we see that

$$V_{p^{2\beta+1}}(x^2) = \frac{p-1}{2} \sum_{s=1}^{\beta} p^{2s} + V_p(x^2) = \frac{p^{2\beta+2} + 2p + 1}{2(p+1)}$$

and

$$V_{p^{2\beta}}(x^2) = \frac{p-1}{2} \sum_{s=1}^{\beta} p^{2s-1} + V_1(x^2) = \frac{p^{2\beta+1} + p + 2}{2(p+1)}.$$

Now combining this with Theorem 3.1 gives the result.

**Theorem 3.4.** *Let $a_1, a_2, a_3$ and $m > 1$ be integers with* $\gcd(m, 6(a_1^2 - 3a_2)) = 1$. *If $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime decomposition of $m$, then*

$$V_m(x^3 + a_1x^2 + a_2x + a_3) = m \prod_{i=1}^{r} \frac{2p_i + \left(\frac{p_i}{3}\right)}{3p_i}.$$

Proof. Let $p$ be a prime divisor of $m$. Let $c \in \mathbb{Z}$ and $f(x) = x^3 + a_1x^2 + a_2x + a_3 - c$. According to [Su3], the discriminant of $f(x)$ is given by $D(f(x)) = -\frac{1}{27}(b^2 - 4a)$, where $a = (a_1^2 - 3a_2)^3$ and $b = -2a_1^3 + 9a_1a_2 - 27(a_3 - c)$. Now we claim that $f(x) \equiv 0 \pmod p$ is solvable if and only if $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable. Clearly $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable implies $f(x) \equiv 0 \pmod p$ is solvable.

If $p \nmid D(f(x))$, it is well known that $f(x) \equiv 0 \pmod p$ has no multiple solutions. Hence, if $f(x_0) \equiv 0 \pmod p$ for some integer $x_0$, then $f'(x_0) \not\equiv 0 \pmod p$. Now, using Lemma 3.1 we see that $f(x) \equiv 0 \pmod p$ is solvable implies $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable.

If $p \mid D(f(x))$, we set

$$x_0 = -a_1 + \frac{a_1a_2 - 9(a_3 - c)}{a_1^2 - 3a_2} = \frac{1}{3}\Big(\frac{b}{a_1^2 - 3a_2} - a_1\Big).$$

From [Su3, Lemma 4.1] we know that $x \equiv x_0 \pmod p$ is a solution of the congruence $f(x) \equiv 0 \pmod p$. As $b^2 \equiv 4a \pmod p$ we see that

$$\begin{aligned} f'(x_0) &= 3x_0^2 + 2a_1x_0 + a_2 \\ &= \frac{1}{3}\Big(\frac{b}{a_1^2 - 3a_2} - a_1\Big)^2 + \frac{2a_1}{3}\Big(\frac{b}{a_1^2 - 3a_2} - a_1\Big) + a_2 \\ &= \frac{1}{3(a_1^2 - 3a_2)^2}\big(b^2 - (a_1^2 - 3a_2)^3\big) \equiv a_1^2 - 3a_2 \not\equiv 0 \pmod p. \end{aligned}$$

Thus $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable by Lemma 3.1.

By the above, the assertion is true. Suppose

$$S_p(x^3 + a_1x^2 + a_2x + a_3) = \{c_1, c_2, \ldots, c_n\}.$$

Then we must have

$$S_{p^\alpha}(x^3 + a_1x^2 + a_2x + a_3) = \big\{c_i + tp \;\big|\; i = 1, 2, \ldots, n,\ t = 0, 1, \ldots, p^{\alpha-1} - 1\big\}.$$

Hence applying (1.1) we get

$$V_{p^\alpha}(x^3 + a_1x^2 + a_2x + a_3) = p^{\alpha-1}n = p^{\alpha-1}V_p(x^3 + a_1x^2 + a_2x + a_3) = p^{\alpha-1}\frac{2p + (\frac{p}{3})}{3}.$$

This together with Theorem 3.1 yields the result.

**Theorem 3.5.** *Let $m, a_1, a_2, a_3 \in \mathbb{Z}$ with $m > 3$ and $\gcd(m, 6(a_1^2 - 3a_2)) = 1$. Then $m$ is a prime if and only if $V_m(x^3 + a_1x^2 + a_2x + a_3) = (2m + (\frac{m}{3}))/3$.*

Proof. If $m$ is a prime, the result is true by (1.1). Now suppose $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is composite, where $p_1, \ldots, p_r$ are distinct primes. If $r = 1$, then $\alpha_1 > 1$. It follows from Theorem 3.4 that

$$V_m(x^3 + a_1x^2 + a_2x + a_3) = m\Big(\frac{2}{3} + \frac{1}{3p_1}\Big(\frac{p_1}{3}\Big)\Big) \neq \frac{1}{3}\Big(2m + \Big(\frac{m}{3}\Big)\Big).$$

So the result holds in the case $r = 1$.

Now suppose $r > 1$. Since $p_i \geq 5$ we see that

$$\prod_{i=1}^{r}\Big(\frac{2}{3} + \frac{1}{3p_i}\Big(\frac{p_i}{3}\Big)\Big) \leq \prod_{i=1}^{r}\Big(\frac{2}{3} + \frac{1}{15}\Big) = \Big(\frac{11}{15}\Big)^r < 0.54 \cdot \Big(\frac{11}{15}\Big)^{r-2} < \frac{2}{3} + \frac{1}{3m}\Big(\frac{m}{3}\Big).$$

Thus, by Theorem 3.4,

$$V_m(x^3 + a_1x^2 + a_2x + a_3) = m\prod_{i=1}^{r}\Big(\frac{2}{3} + \frac{1}{3p_i}\Big(\frac{p_i}{3}\Big)\Big) < \frac{2m + (\frac{m}{3})}{3}.$$

This completes the proof.

**Corollary 3.1.** *Let $p \geq 5$ be an integer such that $p \equiv \pm 1 \pmod 6$. Then $p$ is a prime if and only if $V_p(x^3 - x) = (2p + (\frac{p}{3}))/3$.*

## References


[BEW] B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, Inc., New York, Chichester, 1998.

[BSD] B.J. Birch and H.P.F. Swinnerton-Dyer, *Note on a problem of Chowla*, Acta Arith. **5** (1959), 417-423.

[Br] J. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory **5** (1973), 271-287.

[HW] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers (fifth edition)*, Oxford Univ. Press, 1981, p. 97.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982.

[K] R. Kantor, *Über die Anzahl inkongruenter Werte ganzer, rationaler Funktionen*, Monatsh. Math. Phys. **26** (1915), 24-39.

[L1] E. Lehmer, *On Euler's criterion*, J. Austral. Math. Soc. **1** (1959/1961, part 1), 64-70.

[L2] E. Lehmer, *On the quartic character of quadratic units*, J. Reine Angew. Math. **268/269** (1974), 294-301.

[Leo] P.A. Leonard, *On factoring quartics* (mod $p$), J. Number Theory **1** (1969), 113-115.

[MW1] K. McCann and K.S. Williams, *On the residues of a cubic polynomial* (mod $p$), Canad. Math. Bull. **10** (1967), 29-38.

[MW2] K. McCann and K.S. Williams, *The distribution of the residues of a quartic polynomial*, Glasgow Math. J. **8** (1967), 67-88.

[R] K.H. Rosen, *Elementary Number Theory and Its Applications, fourth ed.*, Addison Wesley, Reading, MA, 2000.

[Sk] T. Skolem, *The general congruence of* 4*th degree modulo p, p prime*, Norsk Mat. Tidsskr. **34** (1952), 73-80.

[St] R.D. von Sterneck, *Über die Anzahl inkongruenter Werte, die eine ganze Funktion dritten Grades annimmt*, Sitzungsber. Akad. Wiss. Wien (2A) **114** (1908), 711-717.

[Su1] Z.H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291-335.

[Su2] Z.H. Sun, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), 361-377.

[Su3] Z.H. Sun, *Cubic and quartic congruences modulo a prime*, J. Number Theory **102** (2003), 41-89.

[Su4] Z.H. Sun, *Quartic residues and binary quadratic forms*, J. Number Theory **113** (2005), 10-52.

[W] K.S. Williams, *Evaluation of character sums connected with elliptic curves*, Proc. Amer. Math. Soc. **73** (1979), 291-299.