Far East J. Math. Sci. (FJMS) 3(2) (2001), 209-225

CONDITIONS FOR THE INSOLVABILITY OF THE QUINTIC EQUATION $x^5 + ax + b = 0$

BLAIR K. SPEARMAN and KENNETH S. WILLIAMS

Dedicated to the memory of Sarvadaman Chowla (1907-1995)

(Received October 21, 2000)

Submitted by K. K. Azad

Abstract

Simple congruence conditions are proved which ensure that the quintic equation $x^5 + ax + b = 0$, where a and b are nonzero integers, is not solvable by radicals. For example, it is shown that if $a \equiv 1 \pmod 2$ and $b \equiv 2 \pmod 4$, then $x^5 + ax + b = 0$ is not solvable by radicals.

Let a and b be nonzero integers such that $x^5 + ax + b \in \mathbb{Z}[x]$ is irreducible. In this note we are concerned with the insolvability of the quintic equation

$$x^5 + ax + b = 0 \tag{1}$$

by radicals. In 1942, Bhalotra and Chowla [2] [3, pp. 529-531] gave the following three theorems.

Theorem A. *If* $a \equiv b \equiv 1 \pmod 2$, *then* (1) *is not solvable by radicals.*

Theorem B. *If* $a \equiv 1 \pmod 2$ *and* a *is not divisible by any prime* $\equiv 3 \pmod 4$, *then* (1) *is not solvable by radicals.*

2000 Mathematics Subject Classification: 12E05, 12E10.

Key words and phrases: quintic equations, insolvability by radicals.

© 2001 Pushpa Publishing House

Theorem C. *If a is a prime $\not\equiv 1 \pmod 5$ and $(a, b) = 1$, then (1) is not solvable by radicals.*

Theorem B is mentioned in the obituary of Chowla by Ayoub, Huard and Williams [1]. Unfortunately Theorem B is not correct [3, p. A3] as shown by the example

$$x^5 - 5x + 12 = 0,$$

which has the solution in radicals

$$x = \frac{1}{5}\left(R_{1,1}^{1/5} + R_{1,-1}^{1/5} + R_{-1,1}^{1/5} + R_{-1,-1}^{1/5} \right),$$

where $R_{\varepsilon,\delta}$ $(\varepsilon, \delta = \pm 1)$ is given by

$$R_{\varepsilon,\delta} = 625(-5 + 2\varepsilon\sqrt{5}) + \delta\frac{375}{2}\left(2\sqrt{100 - \varepsilon 20\sqrt{5}} - \varepsilon\sqrt{100 + \varepsilon 20\sqrt{5}} \right)$$

see [4, p. 399], [6, p. 990]. In this note we correct Theorem B (see Theorem 1) and prove three results similar to Theorems A, B, C (see Theorems 2, 3, 4). We make use of the following two results.

Proposition 1 ([2, p. 110], [3, p. 529], [4, p. 389], [6, p. 988]). *The equation (1) is solvable by radicals if and only if the equation*

$$x^6 + 8ax^5 + 40a^2x^4 + 160a^3x^3 + 400a^4x^2 + (512a^5 - 3125b^4)x + (256a^6 - 9375ab^4) = 0 \tag{2}$$

has an integral root.

Proposition 2 [6, p. 987]. *The equation (1) is solvable by radicals if and only if there exist rational numbers $\varepsilon(= \pm 1)$, $c(\geq 0)$ and $e(\neq 0)$ such that*

$$a = \frac{5e^4(3 - 4\varepsilon c)}{c^2 + 1}, \qquad b = \frac{-4e^5(11\varepsilon + 2c)}{c^2 + 1}. \tag{3}$$

We begin by correcting Theorem B.

Theorem 1. *If*

$$a > 0, \quad a \equiv 1 \pmod 2), \quad p(\text{prime}) \mid a \Rightarrow p \not\equiv 3 \pmod 4),$$

then (1) is not solvable by radicals.

Proof. As a is odd and the primes dividing a are $\not\equiv 3 \pmod 4$, all the primes dividing a must be $\equiv 1 \pmod 4$. Hence

$$a = \pm(4t_1 + 1)\cdots(4t_n + 1),$$

where each $4t_i + 1$ is a prime. As $a > 0$ the $+$ sign must hold so that

$$a = (4t_1 + 1)\cdots(4t_n + 1) \tag{4}$$

and

$$a \equiv 1 \pmod 4. \tag{5}$$

Suppose that (1) is solvable by radicals. Then, by Proposition 1, there exists an integer r such that

$$(r + 2a)^4(r^2 + 16a^2) - 5^5b^4(r + 3a) = 0. \tag{6}$$

Set

$$z = r + 3a \in \mathbb{Z}. \tag{7}$$

From (6) and (7) we deduce that

$$(z - a)^4((z - 3a)^2 + 16a^2) = 5^5b^4z. \tag{8}$$

Clearly from (8) we deduce that

$$z > 0. \tag{9}$$

Also from (8) we see that

$$z \mid 25a^6. \tag{10}$$

From (4) and (10) we conclude that z is odd and divisible only by primes $\equiv 1 \pmod 4$. Thus, by (9), we have

$$z \equiv 1 \pmod 4. \tag{11}$$

Hence, by (5) and (11), we have

$$(z - 3a)^2 + 16a^2 \equiv 4 \pmod{16}$$

so that

$$v_2((z - 3a)^2 + 16a^2) = 2. \tag{12}$$

From (8) we see that

$$4v_2(z-a)+v_2((z-3a)^2+16a^2)=4v_2(b)$$

so that

$$v_2((z-3a)^2+16a^2)\equiv 0 \pmod 4,$$

which contradicts (12). Hence (1) is not solvable by radicals.

Our next result is an extension of Theorem A. Theorem A itself is actually very easy to prove using Galois theory. For $a \equiv b \equiv 1 \pmod 2$, we have

$$x^5+ax+b \equiv x^5+x+1 \equiv (x^2+x+1)(x^3+x^2+1) \pmod 2,$$

and since x^2+x+1 and x^3+x^2+1 are both irreducible $\pmod 2$ the Galois group of x^5+ax+b is the symmetric group S_5, and so (1) is not solvable by radicals. To prove our extension of Theorem A, we make use of Proposition 2.

Theorem 2. *If* $a \equiv 1 \pmod 2$ *and* $b \equiv 2 \pmod 4$, *then* (1) *is not solvable by radicals.*

Proof. Suppose that (1) is solvable by radicals. Then, by Proposition 2, there exist rational numbers $\varepsilon(=\pm 1)$, $c(\geq 0)$ and $e(\neq 0)$ such that

$$a=\frac{5e^4(3-4\varepsilon c)}{c^2+1}, \qquad b=\frac{-4e^5(11\varepsilon+2c)}{c^2+1}. \tag{13}$$

Set

$$e=r/s, \quad c=m/n, \tag{14}$$

where r, s, m, n are integers satisfying

$$r\neq 0, \quad s>0, \quad (r,s)=1, \tag{15}$$

and

$$m\geq 0, \quad n>0, \quad (m,n)=1. \tag{16}$$

Substituting (14) into (13), we obtain

$$a = \frac{5r^4(3n - 4\varepsilon m)n}{s^4(m^2 + n^2)} \tag{17}$$

and

$$b = \frac{-4r^5(11\varepsilon n + 2m)n}{s^5(m^2 + n^2)}. \tag{18}$$

We note that $3n - 4\varepsilon m \neq 0$ as $a \neq 0$ and $11\varepsilon n + 2m \neq 0$ as $b \neq 0$. As $a \equiv 1 \pmod 2$ and $b \equiv 2 \pmod 4$ we obtain from (17) and (18)

$$4v_2(r) + v_2(3n - 4\varepsilon m) + v_2(n) - 4v_2(s) - v_2(m^2 + n^2) = 0, \tag{19}$$

$$2 + 5v_2(r) + v_2(11\varepsilon n + 2m) + v_2(n) - 5v_2(s) - v_2(m^2 + n^2) = 1. \tag{20}$$

We consider nine cases as follows:

Case	$v_2(s)$	$v_2(n)$
(i)	0	
(ii)	1	0
(iii)	1	1
(iv)	1	2
(v)	1	≥ 3
(vi)	≥ 2	0
(vii)	≥ 2	1
(viii)	≥ 2	2
(ix)	≥ 2	≥ 3

Case (i): In this case we have $v_2(s) = 0$ so that (19) and (20) become

$$4v_2(r) + v_2(3n - 4\varepsilon m) + v_2(n) - v_2(m^2 + n^2) = 0, \tag{21}$$

$$5v_2(r) + v_2(11\varepsilon n + 2m) + v_2(n) - v_2(m^2 + n^2) = -1. \tag{22}$$

We consider three subcases.

Subcase (a): $v_2(m)=v_2(n)=0$. Here $v_2(3n-4\varepsilon m)=0$ and $v_2(m^2+n^2)=1$, and (21) gives

$$(\text{multiple of } 4) + 0 + 0 - 1 = 0,$$

a contradiction.

Subcase (b): $v_2(m)\geq 1$, $v_2(n)=0$. Here $v_2(11\varepsilon n+2m)=0$, $v_2(m^2+n^2)=0$ and (22) gives

$$(\geq 0) + 0 + 0 - 0 = -1,$$

a contradiction.

Subcase (c): $v_2(m)=0$, $v_2(n)\geq 1$. Here $v_2(3n-4\varepsilon m)\geq 1$, $v_2(m^2+n^2)=0$ and (21) gives

$$(\geq 0) + (\geq 1) + (\geq 1) - 0 = 0,$$

a contradiction.

Thus Case (i) cannot occur.

Case (ii): In this case we have

$$v_2(s) = 1, \quad v_2(n) = 0, \quad v_2(r) = 0,$$

$$v_2(3n - 4\varepsilon m) = 0, \quad v_2(m^2 + n^2) = 0 \text{ or } 1,$$

and (19) becomes

$$0 + 0 + 0 - 4 - (0 \text{ or } 1) = 0,$$

which is impossible. Thus Case (ii) cannot occur.

Case (iii): In this case we have

$$v_2(s) = 1, \quad v_2(n) = 1, \quad v_2(r) = 0, \quad v_2(m) = 0,$$

$$v_2(3n - 4\varepsilon m) = 1, \quad v_2(m^2 + n^2) = 0,$$

and (19) becomes

$$0 + 1 + 1 - 4 - 0 = 0,$$

which is impossible. Thus Case (iii) cannot occur.

Case (iv): In this case we have

$$v_2(s) = 1, \quad v_2(n) = 2, \quad v_2(r) = 0, \quad v_2(m) = 0,$$

$$v_2(m^2 + n^2) = 0, \quad v_2(3n - 4\varepsilon m) \geq 3,$$

and (19) gives

$$0 + (\geq 3) + 2 - 4 - 0 = 0,$$

which is impossible. Thus Case (iv) cannot occur.

Case (v): In this case we have

$$v_2(s) = 1, \quad v_2(n) \geq 3, \quad v_2(r) = 0, \quad v_2(m) = 0,$$

$$v_2(m^2 + n^2) = 0, \quad v_2(3n - 4\varepsilon m) = 2,$$

and (19) gives

$$0 + 2 + (\geq 3) - 4 - 0 = 0,$$

which is impossible. Thus Case (v) cannot occur.

Case (vi): In this case we have

$$v_2(s) \geq 2, \quad v_2(n) = 0, \quad v_2(r) = 0,$$

$$v_2(3n - 4\varepsilon m) = 0, \quad v_2(m^2 + n^2) = 0 \text{ or } 1,$$

and (19) becomes

$$0 + 0 + 0 - (\geq 8) - (0 \text{ or } 1) = 0,$$

which is impossible. Thus Case (vi) cannot occur.

Case (vii): In this case we have

$$v_2(s) \geq 2, \quad v_2(n) = 1, \quad v_2(r) = 0, \quad v_2(m) = 0,$$

$$v_2(3n - 4\varepsilon m) = 1, \quad v_2(m^2 + n^2) = 0,$$

and (19) becomes

$$0 + 1 + 1 - (\geq 8) - 0 = 0,$$

which is impossible. Thus Case (vii) cannot occur.

Case (viii): In this case we have

$$v_2(s) \geq 2, \quad v_2(n) = 2, \quad v_2(r) = 0, \quad v_2(m) = 0,$$

$$v_2(11\varepsilon n + 2m) = 1, \quad v_2(m^2 + n^2) = 0,$$

and (20) becomes

$$2 + 0 + 1 + 2 - (\geq 10) - 0 = 1,$$

which is impossible. Thus Case (viii) cannot occur.

Case (ix): In this case we have

$$v_2(s) \geq 2, \quad v_2(n) \geq 3, \quad v_2(r) = 0, \quad v_2(m) = 0,$$

$$v_2(3n - 4\varepsilon m) = 2, \quad v_2(11\varepsilon n + 2m) = 1, \quad v_2(m^2 + n^2) = 0,$$

and (19) and (20) give

$$\begin{cases} 0 + 2 + v_2(n) - 4v_2(s) - 0 = 0, \\ 2 + 0 + 1 + v_2(n) - 5v_2(s) - 0 = 1, \end{cases}$$

so that

$$\begin{cases} v_2(n) - 4v_2(s) = -2, \\ v_2(n) - 5v_2(s) = -2. \end{cases}$$

Hence

$$v_2(n) = -2, \quad v_2(s) = 0,$$

contradicting

$$v_2(n) \geq 3, \quad v_2(s) \geq 2.$$

Hence all nine cases cannot occur and the theorem is proved.

Theorem 3. *If p is a prime $\equiv 3 \pmod 4$ such that*

$$p \parallel a,\ p^2 \mid b \quad or \quad p^2 \parallel a,\ p^3 \mid b \quad or \quad p^3 \parallel a,\ p^4 \mid b, \tag{23}$$

then (1) *is not solvable by radicals.*

Proof. Suppose that (1) is solvable by radicals. Then, by Proposition 2, there exist rational numbers $\varepsilon(= \pm 1)$, $c(\geq 0)$, $e(\neq 0)$, such that

$$a = \frac{5e^4(3 - 4\varepsilon c)}{c^2 + 1}, \qquad b = \frac{-4e^5(11\varepsilon + 2c)}{c^2 + 1}. \tag{24}$$

If $c = 0$, then

$$a = 15e^4, \quad b = -44\varepsilon e^5. \tag{25}$$

As a is an integer, from (25) we see that e must be an integer. Further, as $a \neq 0$, we must have $e \neq 0$. If $p \mid e$, then $v_p(a) \geq 4$, contradicting $v_p(a) = 1, 2$ or 3. Hence $p \nmid e$. Since $p \mid a = 15e^4$ and $p \nmid e$, we must have $p \mid 15$. But $p \equiv 3 \pmod 4$ so $p = 3$. Thus $v_p(a) = v_3(a) = 1$ and so $v_p(b) = v_3(b) \geq 2$. Clearly $3 \nmid b = -44\varepsilon e^5$, a contradiction. Hence $c \geq 1$.

Set $c = m/n$ and $e = r/s$, where m, n, r, s are integers with $m > 0$, $n > 0$, $r \neq 0$, $s > 0$ and $(m, n) = (r, s) = 1$. Thus

$$v_p(m) = 0 \text{ or } v_p(n) = 0$$

and

$$v_p(r) = 0 \text{ or } v_p(s) = 0.$$

From (24), we obtain

$$(m^2 + n^2)as^4 = -5r^4(4\varepsilon m - 3n)n, \tag{26}$$

$$(m^2 + n^2)bs^5 = -4\varepsilon r^5(2\varepsilon m + 11n)n. \tag{27}$$

Clearly from (26) and (27) we see that $4\varepsilon m - 3n \neq 0$ and $2\varepsilon m + 11n \neq 0$. Now $p \equiv 3 (\mathrm{mod}\ 4)$ and $\gcd(m, n) = 1$, so that

$$v_p(m^2 + n^2) = 0. \tag{28}$$

From (26)-(28), we obtain

$$v_p(a) + 4v_p(s) = 4v_p(r) + v_p(4\varepsilon m - 3n) + v_p(n), \tag{29}$$

$$v_p(b) + 5v_p(s) = 5v_p(r) + v_p(2\varepsilon m + 11n) + v_p(n). \tag{30}$$

We consider two cases:

(i) $v_p(n) = 0$,

(ii) $v_p(m) = 0$, $v_p(n) \geq 1$.

Case (i): In this case (29) and (30) become

$$v_p(a) + 4v_p(s) = 4v_p(r) + v_p(4\varepsilon m - 3n), \tag{31}$$

$$v_p(b) + 5v_p(s) = 5v_p(r) + v_p(2\varepsilon m + 11n). \tag{32}$$

If $v_p(4\varepsilon m - 3n) = 0$, then (31) gives $4 \mid v_p(a)$ contradicting $v_p(a) = 1$, 2 or 3. Thus $v_p(4\varepsilon m - 3n) \geq 1$. From

$$2(2\varepsilon m + 11n) = (4\varepsilon m - 3n) + 25n,$$

we deduce that $v_p(2\varepsilon m + 11n) = 0$. Hence (32) gives

$$v_p(b) + 5v_p(s) = 5v_p(r).$$

If $v_p(r) = 0$, then $v_p(b) = 0$, contradicting $v_p(b) \geq 2$. If $v_p(r) \geq 1$, then $v_p(s) = 0$ and (31) gives

$$v_p(a) = 4v_p(r) + v_p(4\varepsilon m - 3n) \geq (4 \times 1) + 1 = 5,$$

contradicting $v_p(a) = 1$, 2 or 3.

Case (ii): In this case we have

$$v_p(4\varepsilon m - 3n) = v_p(2\varepsilon m + 11n) = 0$$

so that (29) and (30) become

$$v_p(a) + 4v_p(s) = 4v_p(r) + v_p(n), \tag{33}$$

$$v_p(b) + 5v_p(s) = 5v_p(r) + v_p(n). \tag{34}$$

If $v_p(r) = v_p(s) = 0$, then (33) and (34) give $v_p(a) = v_p(b)$, a contradiction. If $v_p(r) \geq 1$, $v_p(s) = 0$, then (33) gives $v_p(a) = 4v_p(r) + v_p(n) \geq (4 \times 1) + 1 = 5$, a contradiction. If $v_p(r) = 0$, $v_p(s) \geq 1$, then (33) and (34) give

$$v_p(a) + 4v_p(s) = v_p(n) = v_p(b) + 5v_p(s)$$

so

$$v_p(a) - v_p(b) = v_p(s) \geq 1$$

giving

$$v_p(a) > v_p(b),$$

a contradiction.

Hence neither Case (i) nor Case (ii) can occur and this completes the proof that (1) is not solvable by radicals.

Theorem 4. *If* $b \mid a$, *then* (1) *is not solvable by radicals.*

Proof. Suppose that (1) is solvable by radicals. Then, by Proposition 2, there exist rational numbers $\varepsilon(= \pm 1)$, $c(\geq 0)$, and $e(\neq 0)$ such that

$$a = \frac{5e^4(3 - 4\varepsilon c)}{c^2 + 1}, \qquad b = \frac{-4e^5(11\varepsilon + 2c)}{c^2 + 1}. \tag{35}$$

Set

$$c = m/n, \quad m \geq 0, \quad n > 0, \quad (m, n) = 1, \tag{36}$$

and

$$e = r/s, \quad r \neq 0, \quad s > 0, \quad (r, s) = 1. \tag{37}$$

Further, as $b \mid a$, we have

$$a = bk, \tag{38}$$

for some integer $k \neq 0$. From (35)-(38), we obtain

$$a = 5\frac{r^4}{s^4}\frac{(3n - 4\varepsilon m)n}{m^2 + n^2} = -4k\frac{r^5}{s^5}\frac{(11\varepsilon n + 2m)n}{m^2 + n^2}. \tag{39}$$

As $a \neq 0$, we have $3n - 4\varepsilon m \neq 0$ and $11\varepsilon n + 2m \neq 0$. Solving (39) for s, we obtain

$$s = -\frac{4}{5}kr\frac{11\varepsilon n + 2m}{3n - 4\varepsilon m}. \tag{40}$$

Putting this value of s back into (39), we deduce

$$a = \frac{5^5(3n - 4\varepsilon m)^5 n}{2^8 k^4 (11\varepsilon n + 2m)^4 (m^2 + n^2)}. \tag{41}$$

As

$$\frac{5^5(3n - 4\varepsilon m)^5 n}{2} = 2^7 a k^4 (11\varepsilon n + 2m)^4 (m^2 + n^2)$$

is an integer, we have $2 \mid 5^5(3n - 4\varepsilon m)^5 n$, so that

$$2 \mid n. \tag{42}$$

Next we show that

$$(11\varepsilon n + 2m,\ 3n - 4\varepsilon m) = 2^\alpha 5^\beta, \tag{43}$$

for nonnegative integers α and β. This follows from the identities

$$2\varepsilon(11\varepsilon n + 2m) + (3n - 4\varepsilon m) = 25n, \tag{44}$$

$$3(11\varepsilon n + 2m) - 11\varepsilon(3n - 4\varepsilon m) = 50m, \tag{45}$$

as $(m, n) = 1$.

Further, we show that

$$(m^2 + n^2,\ 3n - 4\varepsilon m) = 5^\gamma, \tag{46}$$

for a nonnegative integer γ. This follows from the identities

$$9(m^2 + n^2) - (3n - 4\varepsilon m)(3n + 4\varepsilon m) = 25m^2, \tag{47}$$

$$16(m^2 + n^2) + (3n - 4\varepsilon m)(3n + 4\varepsilon m) = 25n^2, \tag{48}$$

as $(m, n) = 1$.

Moreover,

$$(m^2 + n^2,\ n) = 1 \tag{49}$$

and

$$(11\varepsilon n + 2m,\ n) = 1 \text{ or } 2 \tag{50}$$

as $(m, n) = 1$.

From (41) we see that

$$\frac{5^5(3n - 4\varepsilon m)^5 n}{(11\varepsilon n + 2m)^4(m^2 + n^2)} = 2^8 k^4 a$$

is an integer. Hence, in view of (43), (46), (49), (50), we must have

$$|11\varepsilon n + 2m| = 2^u 5^v, \quad m^2 + n^2 = 5^w, \tag{51}$$

for nonnegative integers u, v, w. We now consider two cases:

(i) $4v + w > 5$,

(ii) $4v + w \leq 5$.

Case (i): $4v + w > 5$. In this case at least one of v and w is positive so that either $5 \mid 11\varepsilon n + 2m$ or $5 \mid m^2 + n^2$. By (49) and (50) both possibilities imply that

$$5 \nmid n. \tag{52}$$

Hence, as $5^6 \mid (11\varepsilon n + 2m)^4(m^2 + n^2)$ (since $4v + w \geq 6$) and a is an integer, by (41) we must have

$$5 \mid 3n - 4\varepsilon m. \tag{53}$$

Then, by (45), we deduce that

$$5 \mid 11\varepsilon n + 2m. \tag{54}$$

Hence, by (51) and (54), we have

$$v > 0. \tag{55}$$

We show next that $w \leq 3$. Suppose on the contrary that $w > 3$, so that, by (51), we have $5^4 \mid m^2 + n^2$. From the identity

$$4(m^2 + n^2) + (11\varepsilon n + 2m)(11\varepsilon n - 2m) = 125n^2, \tag{56}$$

we deduce that

$$5^3 \parallel (11\varepsilon n + 2m)(11\varepsilon n - 2m). \tag{57}$$

As $(m, n) = 1$ and $5 \mid 11\varepsilon n + 2m$, we have $5 \nmid 11\varepsilon n - 2m$, so that by (57), we have

$$5^3 \parallel 11\varepsilon n + 2m, \tag{58}$$

that is, by (51),

$$v = 3. \tag{59}$$

From (52), (58) and the identity

$$(3n - 4\varepsilon m) + 2\varepsilon(11\varepsilon n + 2m) = 25n,$$

we deduce that

$$5^2 \parallel 3n - 4\varepsilon m. \tag{60}$$

Then, by (41), (51), (52), (59), (60) we see that

$$v_5(a) = 3 - w - 4v_5(k) \leq 3 - w < 0,$$

as $w \geq 4$, a contradiction. Hence $w \leq 3$.

Case (ii): $4v + w \leq 5$. In this case we have

$$w \leq 4v + w \leq 5.$$

Thus in both cases we have $w \leq 5$. We examine the possibilities $w = 0, 1, 2, 3, 4, 5$ individually.

$\boldsymbol{w = 0}$. Here $m^2 + n^2 = 1$. As $m \geq 0$ and $2 \mid n$ we have $(m, n) = (1, 0)$, contradicting $n > 0$.

$\boldsymbol{w = 1}$. Here $m^2 + n^2 = 5$. As $m \geq 0$, $n > 0$ and $2 \mid n$ we have $(m, n) = (1, 2)$. Then, by (51), we have

$$2^u 5^v = |11\varepsilon n + 2m| = |22\varepsilon + 2| = \begin{cases} 24, & \text{if } \varepsilon = 1, \\ 20, & \text{if } \varepsilon = -1, \end{cases}$$

so that $\varepsilon = -1$, $u = 2$, $v = 1$. Hence, from (41), we have $a = \dfrac{5^5}{2^{10}k^4}$, which is not an integer for any integer k, a contradiction.

$w = 2$. Here $m^2 + n^2 = 5^2$. In view of (36) and (42) we have $(m, n) = (3, 4)$. Then, by (51), we have

$$2^u 5^v = |11\varepsilon n + 2m| = |44\varepsilon + 6| = \begin{cases} 50, \text{ if } \varepsilon = 1, \\ 38, \text{ if } \varepsilon = -1, \end{cases}$$

so that $\varepsilon = 1$, $u = 1$, $v = 2$. Thus $3n - 4\varepsilon m = 0$, so that $a = 0$, a contradiction.

$w = 3$. Here $m^2 + n^2 = 5^3$. In view of (36) and (42) we have $(m, n) = (11, 2)$. Then, by (51), we have

$$2^u 5^v = |11\varepsilon n + 2m| = |22\varepsilon + 22| = \begin{cases} 44, \text{ if } \varepsilon = 1, \\ 0, \ \text{ if } \varepsilon = -1, \end{cases}$$

a contradiction.

$w = 4$. Here $m^2 + n^2 = 5^4$. In view of (36) and (42) we have $(m, n) = (7, 24)$. Then, by (51), we have

$$2^u 5^v = |11\varepsilon n + 2m| = |264\varepsilon + 14| = \begin{cases} 278, \text{ if } \varepsilon = 1, \\ 250, \text{ if } \varepsilon = -1, \end{cases}$$

so that $\varepsilon = -1$, $u = 1$, $v = 3$. Then, by (41), we have $a = \dfrac{2 \cdot 3}{5k^4}$, which is not an integer for any integer k, a contradiction.

$w = 5$. Here $m^2 + n^2 = 5^5$. In view of (36) and (42) we have $(m, n) = (41, 38)$. Then, by (51), we have

$$2^u 5^v = |11\varepsilon n + 2m| = |418\varepsilon + 82| = \begin{cases} 500, \text{ if } \varepsilon = 1, \\ 336, \text{ if } \varepsilon = -1, \end{cases}$$

so that $\varepsilon = 1$, $u = 2$, $v = 3$. Then, by (41), we have $a = \dfrac{-19}{2^{10}5^2k^4}$, which is not an integer for any k, a contradiction.

This completes the proof of Theorem 4.

We close with some examples. The second column of the Table indicates the theorem (Theorems 1, 2, 3 or 4), which applies to the polynomial $x^5 + ax + b$ in the first column to ensure that the equation $x^5 + ax + b = 0$ is insolvable by radicals. The third column gives the Galois group of the polynomial $x^5 + ax + b$.

Table. Quintic trinomials $x^5 + ax + b$ for which the quintic equation $x^5 + ax + b = 0$ is insolvable by radicals.

$x^5 + ax + b$	Theorem	$Gal(x^5 + ax + b)$
$x^5 + 145x + 232$	Theorem 1	A_5
$x^5 + 239x + 956$	Theorem 1	A_5
$x^5 + 545x + 872$	Theorem 1	A_5
$x^5 + 5x + 1$	Theorem 1	S_5
$x^5 + 130x + 4$	Theorem 1	S_5
$x^5 + x + 10$	Theorem 2	S_5
$x^5 + 3x + 6$	Theorem 2	S_5
$x^5 + 3x + 9$	Theorem 3	S_5
$x^5 - 49x + 686$	Theorem 3	S_5
$x^5 - 54x + 162$	Theorem 3	S_5
$x^5 + 3x + 3$	Theorem 4	S_5
$x^5 + 72x - 36$	Theorem 4	S_5

References

[1] R. G. Ayoub, J. G. Huard and K. S. Williams, Sarvadaman Chowla (1907-1995), Notices Amer. Math. Soc. 45 (1998), 594-598.

[2] Y. Bhalotra and S. Chowla, Some theorems concerning quintics insoluble by radicals, Math. Student 10 (1942), 110-112.

[3] S. Chowla, The Collected Papers of Sarvadaman Chowla, Vol. II, 1936-1961, Centre de Recherches Mathématiques, Montréal, Canada, 1999.

[4] D. S. Dummit, Solving solvable quintics, Math. Comp. 57 (1991), 387-401.

[5] S. Kobayashi and H. Nakagawa, Resolution of solvable quintic equation, Math. Japon. 37 (1992), 883-886.

[6] B. K. Spearman and K. S. Williams, Characterization of solvable quintics $x^5 + ax + b$, Amer. Math. Monthly 101 (1994), 986-992.

Department of Mathematics and Statistics
Okanagan University College
Kelowna, B.C.
Canada V1V 1V7
e-mail: bkspearm@okuc02.okanagan.bc.ca

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6
e-mail: williams@math.carleton.ca