खण्ड-9, अंक-1, वर्ष-2021, मु0प्र0 55-61
D.O.I.: https://doi.org/10.22445/avsp.v9i1.11
SJIF (2021) : 7.247

मिश्रित द्विघातीय कौंग्रुएंस का सही क्रम में सरल हल

प्रीति बाजपेयी
गणित विभाग, बिट्स पिलानी, दुबई कैम्पस, दुबई, यू0ए0ई0
dr.priti.bajpai@gmail.com

प्राप्ति तिथि–10.08.2021, स्वीकृति तिथि–22.09.2021

सार– द्विघातीय कौंग्रुएंस सदियों से उत्सुकता का विषय रहा है। इन कौंग्रुएंस का पूर्णांक हल निकालने के भी अलग–अलग तरीके हैं। यदि हल करते समय सतर्कता बरती जाए और सही तरीका व क्रम अपनाया जाए तो इन्हें कम से कम संक्रियाओं में हल किया जा सकता है। प्रस्तुत अध्ययन उसी का एक प्रयास है।

बीज शब्द– द्विघातीय कौंनग्रुएंस, हल, पूर्णांक

Solving a Mixed System of Quadratic Congruence in an Organized Way

Priti Bajpai
Department of Mathematics, BITS Pilani, Dubai Campus, U.A.E.
dr.priti.bajpai@gmail.com

Abstract– Solving a Quadratic Congruence has been a topic of interest since ages. There are many different ways of solving them for integer solutions. When we are solving a system of Quadratic Congruence, the order in which they are solved matters a lot in reducing the number of steps. In case, care is not taken the number of steps increase unnecessarily. This paper is an attempt to give a systematic solution for such a system of mixed Quadratic Congruence, so that they can be solved in an organized way in the least number of steps.

Key words- Quadratic Congruence, Integer, Solution

1. **परिचय**–मान लीजिए हमें नीचे दिए गए मिश्रित द्विघातीय कौंग्रुएंस प्रणाली को हल करना है और x का सामान्य हल निकालना है। यह ध्यान रहे कि x के सभी मान पूर्णांक संख्या हों।

दिया गया है:

$$\left.\begin{aligned} ax^2 + bx + c &\equiv 0 \pmod{p} \\ x^2 &\equiv e \pmod{q} \\ mx &\equiv n \pmod{r} \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

यहाँ p, q और r अभाज्य विषम संख्या है।
पहला प्रश्न यह उठता है कि यह प्रणाली हल की जा सकती है कि नहीं ? दूसरा प्रश्न यह है कि अगर हल निकल सकता है तो x के कितने हल होंगे ? तीसरा यह कि किस क्रम में इस द्विघातीय प्रणाली को हल करें ?

इस प्रणाली में तीन कौंग्रुएंस हैं, और जब तक तीनों कौंग्रुएंस का व्यक्तिगत हल नहीं होगा, पूरी प्रणाली का हल नहीं निकल सकता।

माना, प्रत्येक कौंग्रुएंस का हल निकल सकता है तो ऐसे में सम्पूर्ण प्रणाली के 4 हल होंगे। वह इसलिए कि दूसरी और तीसरी कौंग्रुएंस द्विघातीय है और उनका modulus p और q है। ये दो अभाज्य विषम संख्या हैं। इसलिए 2^2 हल होंगे। अब पहली कौंग्रुएंस रेखीय है।

इसलिए वह अपने आप संतुष्ट होगी और हमें उसके हल को अलग से नहीं गिनना होगा।

अब बात आती है क्रम की। वैसे तो किसी भी क्रम से उत्तर वही आयेगा, पर अगर क्रम सही नही लिया गया तो संक्रियाएं बढ़ जायेंगी।

2. **परिणाम**– पहले हम मान के चलते हैं कि तीनों कौंग्रुएंस का हल निकलता है। ऐसे में हमें सबसे पहले किस कौंग्रुएंस से प्रारम्भ करना चाहिए ?

माना हम शुरु करते हैं, $ax^2 + bx + c \equiv 0 \pmod p$ से और उपर दिए क्रम में ही हल करते हैं।

इस प्रकार की कौंग्रुएंस को सबसे पहले $y^2 = k \pmod p$ के रूप में बदलेंगे जो कि इस प्रकार है।

$$(2ax + b)^2 \equiv (b^2 - 4ac) \pmod p$$

अगर $2ax + b = y$ और $b^2 - 4ac = k$ लें तो हमें मिलेगा

$$y^2 \equiv k \pmod p$$

अगर k एक क्वाडरैटिक रैजिड्यू है, तभी इस कौंग्रुएंस का हल निकल सकता है। माना इसका एक हल y_0 है, तो दूसरा हल $(p - y_0)$ होगा। पर हमें तो x का मान चाहिए जिसके लिए हमें नीचे दी गयी दोनों कौंग्रुएंस हल करनी है।

$$2ax + b \equiv y_0 \pmod p$$

और

$$2ax + b \equiv (y_0 - p) \pmod p$$

अर्थात्

$$2ax \equiv (y_0 - b) \pmod p$$

और

$$2ax \equiv (y_0 - p - b) \pmod p \qquad \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

मान लीजिए (2) को हल करने पर हमें x के दो हल x_1 और x_2 मिलते हैं तो x का सामान्य हल होगाः

$$x = x_1 + pt'$$

और

$$x = x_2 + pt'' \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

यहाँ $t', t'' = 0, \pm 1, \pm 2, \ldots$

x के ये दोनों मान हम (1) की दूसरी कौंनग्रुएंस $x^2 \equiv e \pmod q$ में रखेंगे। जिससे हमें प्राप्त होगा

$$(x_1 + pt')^2 \equiv e \pmod q \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$(x_2 + pt'')^2 \equiv e \pmod q \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

(4) और (5) को अब हम t' और t'' के लिए हल करेंगे और प्रत्येक हमें 2 हल देगा। माना ये 4 हल इस प्रकार हैं:

(4) के हल $t' = t_1 + qt'''$

$t' = t_2 + qt^{iv}$

(5) के हल $t'' = t_3 + qt^{v}$

$t'' = t_4 + qt^{vi}$, यहाँ $t''', t^{iv}, t^{v}, t^{vi} = 0, \pm1, \pm2, ...$

t' और t'' के ये मान अब हम (3) में रखेंगे तो हमें x के 4 मान प्राप्त होंगे। ये चारों मान आखिर में (1) की पहली कौंग्रुएंस में रखने पर x के वो चार मान मिलेंगे जो सभी कौंग्रुएंस को संतुष्ट करेंगे। तो नीचे दिए गए क्रम को लेने से हमें प्रणाली का हल तो निकल आता है पर यह चयन सही है कि नहीं ?

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

$$x^2 \equiv e \pmod{q}$$

$$mx \equiv n \pmod{r}$$

उदाहरण के तौर पर चलिए हम हल करते हैं नीचे दी गई प्रणाली को :

(A) प्रश्नः—अगर यह सम्भव हो तो प्रस्तुत द्विघातीय प्रणाली का पूर्णांक हल निकालें

$$x^2 - 2x - 3 \equiv 0 \pmod{5}$$

$$x^2 \equiv 4 \pmod{3}$$

$$x \equiv 2 \pmod{7}$$

उत्तरः—सबसे पहले हम देखेंगे कि हर कौंनग्रुएंस का व्यक्तिगत हल निकल रहा है कि नहीं?

(i) $x \equiv 2 \pmod{7}$ का हल सम्भव है, क्योंकि g.c.d (1,7) = 1 और 1

(ii) $x^2 \equiv 4 \pmod{3}$ यहाँ 4 एक क्वाडरैटिक रैजि्डयू है या दूसरे शब्दों में क्योंकि Legendre Symbol $(\frac{4}{3})$ = 1, इसलिए इसका भी हल है।

(iii) $x^2 - 2x - 3 \equiv 0 \pmod{5}$

सबसे पहले कौंग्रुएंस $x^2 - 2x - 3 \equiv 0 \pmod{5}$ को एक पूर्ण वर्ग के रूप में बदलना पड़ेगा।

$$(2x - 2)^2 \equiv 16 \pmod{5}$$

यदि $2x - 2 = y$ तो

$$y^2 \equiv 16 \pmod{5}$$

यहाँ 16 क्वाडरैटिक रैजिड्यू है या $(\frac{16}{5}) = 1$ इसलिए इस कौंग्रुएंस का भी हल सम्भव है।

इस प्रणाली के 4 हल निकलेंगे। हम इसका हल नीचे दिए क्रम में अगर करेंगे तो देखें क्या प्राप्त होता है?

I $x^2 - 2x - 3 \equiv 0 \pmod 5$

II $x^2 \equiv 4 \pmod 3$

III $x \equiv 2 \pmod 4$

हलः–

(I) सबसे पहले हम हल करेंगे $x^2 - 2x - 3 \equiv 0 \pmod 5$ को

यहाँ $a = 1, b = -2, c = -3$ है और पूर्व में हम देख चुके हैं कि

$(2ax - b)^2 \equiv (b^2 - 4ac) \pmod p$ से हमें प्राप्त होता है :

$$y^2 \equiv 16 \pmod 5$$

इसके दो हल होंगे एक $y_0 = 4$ और दसूरा $y_0 = 1$ चूंकि हमें x का मान चाहिए हम

$2ax = y_0 - b \pmod p$ का प्रयोग कर दो कौंनग्रुएंस प्राप्त करते हैं :

$$2x \equiv (4 + 2) \pmod 5 \Longrightarrow x \equiv 3 \pmod 5 \text{ या } x = 3 + 5t' \quad \ldots\ldots\ldots\ldots\ldots\ldots(6)$$

और $2x \equiv (1 + 2) \pmod 5 \Longrightarrow x \equiv 4 \pmod 5$ या $x = 4 + 5t'' \quad \ldots\ldots\ldots\ldots\ldots\ldots(7)$

यहाँ $t', t'' = 0, \pm 1, \pm 2, \ldots$

अब हम (6) और (7) को दूसरी कौंग्रुएंस $x^2 \equiv 4 \pmod 3$, में एक–एक करके रखेंगे।

(i) समी0 (6) से प्राप्त होगा

$$(5t' + 3)^2 \equiv 4 \pmod 3$$

अगर $5t' + 3 = z$ लें तो

$\Longrightarrow$ $z^2 \equiv 4 \pmod 3$ इसके दो हल निकलेंगे

$z_0 = 2$ और 1

$\Longrightarrow$ $5t' + 3 \equiv 2 \pmod 3 \Longrightarrow t' \equiv 1 \pmod 3$ या $t' = 1 + 3t''' \quad \ldots\ldots\ldots\ldots\ldots\ldots(8)$

और $5t' + 3 \equiv 1 \pmod 3 \Longrightarrow t' \equiv 2 \pmod 3$ या $t' = 2 + 3t^{iv} \quad \ldots\ldots\ldots\ldots\ldots\ldots(9)$

(ii) समी0 (7) से प्राप्त होगा

$$(5\,t'' + 4)^2 \equiv 4 \pmod 3$$

अगर $5\,t'' + 4 = g$ तो

$\Longrightarrow$ $g^2 \equiv 4 \pmod 3$

g के हमें दो मान मिलेंगे $g_o = 2$ और 1

$\Longrightarrow$ $5\,t'' + 4 \equiv 2 \pmod 3 \Longrightarrow t'' \equiv 2 \pmod 3$ या $t'' = 2 + 3\,t^v$ .....(10)

और $5\,t'' + 4 \equiv 1 \pmod 3 \Longrightarrow t'' \equiv 2 \pmod 3$ या $t'' = 3 + 3\,t^{vi}$ .....(11)

यहाँ $t''', t^{iv}, t^v, t^{vi} = 0, \pm1, \pm2, ...$

आखिर में (8), (9), (10) और (11) को जब हम (6) और (7) में रखेंगे तो x के चार मान निकलेंगे।

$$\left.\begin{aligned} x &\equiv 8 \pmod{15} \\ x &\equiv 13 \pmod{15} \\ x &\equiv 14 \pmod{15} \\ x &\equiv 19 \pmod{15} \end{aligned}\right\} \quad \text{या} \quad \left.\begin{aligned} x &= 8 + 15\,t_1 \\ x &= 13 + 15\,t_2 \\ x &= 14 + 15\,t_3 \\ x &= 19 + 15\,t_4 \end{aligned}\right\} \quad .....(12)$$

यहाँ $t_1, t_2, t_3, t_4 = 0, \pm1, \pm2, ...$

(i) अब (12) से x के मान को सीधे आखिरी कौंग्रुएंस $x \equiv 2 \pmod 4$ में रखते हैं तो प्राप्त होगा।

$$\left.\begin{aligned} 15\,t_1 &\equiv -6 \pmod 7 \Longrightarrow t_1 \equiv 1 \pmod 7 \Longrightarrow t_1 = 1 + 7\,k_1 \\ 15\,t_2 &\equiv -11 \pmod 7 \Longrightarrow t_2 \equiv 3 \pmod 7 \Longrightarrow t_2 = 3 + 7\,k_2 \\ 15\,t_3 &\equiv -12 \pmod 7 \Longrightarrow t_3 \equiv 2 \pmod 7 \Longrightarrow t_3 = 2 + 7\,k_3 \\ 15\,t_4 &\equiv -17 \pmod 7 \Longrightarrow t_4 \equiv 4 \pmod 7 \Longrightarrow t_4 = 4 + 7\,k_4 \end{aligned}\right\} \quad .....(13)$$

यहाँ $k_1, k_2, k_3, k_4 = 0, \pm1, \pm2, ...$

t_1, t_2, t_3, t_4 के मान (12) में रखने पर हमें प्राप्त होगा–

$x = 18 + 15\,(1 + 7\,k_1) \Longrightarrow x = 23 + 105\,k_1$

$x = 13 + 15\,(3 + 7\,k_2) \Longrightarrow x = 58 + 105\,k_2$

$x = 14 + 15\,(2 + 7\,k_3) \quad \Longrightarrow \quad x = 44 + 105\,k_3$

$x = 19 + 15\,(4 + 7\,k_4) \quad \Longrightarrow \quad x = 79 + 105\,k_4$

x के चार उत्तर हैं $x \equiv 23 \pmod{105}$, $x \equiv 58 \pmod{105}$, $x \equiv 44 \pmod{105}$ और $x \equiv 79 \pmod{105}$।

यह देखा जा सकता है, यह चारों (1) को संतुष्ट करती हैं। इस पूरी प्रक्रिया में 24 संक्रियाएं लगी।

(B) माना हम प्रश्न को नीचे दिये गये क्रम

I $\quad x \equiv 2 \pmod 4$

II $\quad x^2 \equiv 4 \pmod 3$

III $\quad x^2 - 2x - 3 \equiv 0 \pmod 5$

में हल करते हैं तो

(I) हम प्रारम्भ करेंगे $x \equiv 2 \pmod 7$, इसका हल है

$x = 2 + 7\,t$, यहाँ $t = 0, \pm 1, \pm 2, \ldots$

(II) इसे दूसरी कौंग्रुएंस $x^2 \equiv 4 \pmod 3$ में रखेंगे

$\Longrightarrow \quad (2 + 7\,t)^2 \equiv 4 \pmod 3$ या $(7\,t + 2)^2 \equiv 4 \pmod 3$

यदि $\quad 7\,t + 2 = y \Longrightarrow y^2 \equiv 4 \pmod 3$

$\Longrightarrow$ t के दो मान होंगे 2 और 1 और यह हमें x के दो मान देंगे–

$$x = 16 + 21\,t' \qquad \ldots\ldots(14)$$

और

$$x = 2 + 21\,t'' \qquad \ldots\ldots(15)$$

यहाँ $t', t'' = 0, \pm 1, \pm 2, \ldots$

(III) (14) और (15) को अब हम $x^2 - 2\,x - 3 \equiv 0 \pmod 5$ में रखेंगे। यह प्रदान करेगा–

$$(16 + 21\,t')^2 - 2\,(16 + 21\,t') - 3 \equiv 0 \pmod 5 \qquad \ldots\ldots(16)$$

और

$$(2 + 21\,t'')^2 - 2\,(2 + 21\,t'') - 3 \equiv 0 \pmod 5 \qquad \ldots\ldots(17)$$

(16) और (17) को t' और t'' के लिये हल करना है। हल करने पर

$t' = 1 + 5t'''$ और$t' = 2 + 5t^{iv}$..... (18)

$t'' = 2 + 5t^{v}$ और $t''=3 + 5t^{vi}$ ..... (19)

यहाँ $t''', t^{iv}, t^{v}, t^{vi} = 0, \pm 1, \pm 2, ...$

t', t''के मान (18) और (19) से (16) और (17) में रखने पर x के चार मान मिलेंगे

$x \equiv 23 \pmod{105}$, $x \equiv 58 \pmod{105}$, $x \equiv 44 \pmod{105}$ और $x \equiv 79 \pmod{105}$

जो हमें पहले मिले।

निष्कर्ष– यहाँ यह देखा जा सकता है इनको हल करने में केवल 18 संक्रियाएं लगी। इसी कारण सही चयन बहुत आवश्यक है।

आभार– लेखिका, श्री अखिलेश वर्मा की सहायता की आभारी है।

संदर्भ

1. कोशी, थौमस (2008) एलिमेंटरी नम्बर थ्योरी विद् एप्लीकेशन, एलजीवियर, दूसरा संस्करण।
2. डेविड, एम0 बर्टन (2012) एलिमेंटरी नम्बर थ्योरी, मैक–ग्रॉहिल पब्लिकेशन, सातवां संस्करण।