J. London Math. Soc. (2) 64 (2001) 273–274
DOI: 10.1112/S0024610701002381

THE CUBIC CONGRUENCE $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$ AND BINARY QUADRATIC FORMS II

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

Abstract

It is shown that the splitting modulo a prime p of a given monic, integral, irreducible cubic with non-square discriminant is equivalent to p being represented by forms in a certain subgroup of index 3 in the form class group of discriminant equal to the discriminant of the field defined by the cubic.

1. *Introduction*

Let A, B, C be integers such that x^3+Ax^2+Bx+C is irreducible in $\mathbb{Z}[x]$ with non-square discriminant D. Throughout this paper p denotes a prime > 3 with $(D/p) = 1$. Let $H(\Delta)$ denote the group of classes of primitive, integral, binary quadratic forms of discriminant Δ. In our paper [**3**], we proved the following.

Theorem A. *There exists a unique subgroup $J = J(A, B, C)$ of index 3 in $H(D)$ such that $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$ has three solutions if and only if p is represented by one of the forms in $J(A, B, C)$.*

Since the publication of this paper in 1992, a number of mathematicians have asked us 'can the polynomial discriminant D be replaced in the theorem by the field discriminant $d = d(C_1)$ of the cubic field $C_1 = \mathbb{Q}(\theta)$, where $\theta^3 + A\theta^2 + B\theta + C = 0$?'. It is the purpose of this sequel to answer their question in the affirmative.

2. *Proof of revised theorem*

Let K be the quadratic field $\mathbb{Q}(\sqrt{D})$. Let L be the splitting field of x^3+Ax^2+Bx+C. Let $f_0 = f_0(L/K) \in \mathbb{Z}$ be the finite part of the conductor of the extension L/K.

We first prove the following.

Theorem 1. *Let f be a positive integer with $f_0|f$. Then there exists a unique subgroup $J = J(L, K, f)$ of index 3 in $H(d(K)f^2)$ with the property*

$x^3+Ax^2+Bx+C \equiv 0 \pmod p$ *has three solutions* $\Leftrightarrow$ *p is represented by a form in J.*

Proof. Let $F_f^+(K)$ denote the strict ring class field of the order of conductor f in K. As $f_0|f$, by [**1**, Lemma 3.1.6], we have $L \subseteq F_f^+(K)$. Then, by [**1**, Theorem 3.1.3], there exists a unique subgroup $J = J(L, K, f)$ of index 3 in $H(d(K)f^2)$ such that

Received 9 January 2000.

2000 *Mathematics Subject Classification* 11A07.

Both authors were supported by Natural Sciences and Engineering Research Council of Canada grants.

$x^3 + Ax^2 + Bx + C \equiv 0 \pmod{p}$ has three solutions if and only if p is represented by one of the forms in J. □

We can now answer the question.

THEOREM 2. *There exists a unique subgroup $J = J(L, K, f_0)$ of index 3 in $H(d)$ such that*

$x^3+Ax^2+Bx+C \equiv 0 \pmod{p}$ *has three solutions* $\Leftrightarrow$ p *is represented by a form in* J.

Proof. The theorem follows from Theorem 1 by taking $f = f_0 = f_0(L/K)$ and recalling that $d(K)f_0^2 = d(C_1) = d$; see for example [**2**, pp. 835–836; **1**, Theorem 4.2.7]. □

3. *Concluding remarks*

We note that [**3**, Corollaries 1 and 2] are still true with D replaced by d; [**3**, Corollaries 3 and 4] remain the same. We also note that in [**3**, Examples 1–4] the corresponding values of d are −3159, −31, 321, −3299 and Theorem 2 explains why subgroups of $H(-3159)$, $H(-31)$, $H(321)$, $H(-3299)$ can be used to characterize the splitting of the cubics given in the examples.

References

1. D. LIU, 'Dihedral polynomial congruences and binary quadratic forms: a class field theory approach', PhD Thesis, Carleton University, 1992.
2. D. C. MAYER, 'Multiplicities of dihedral discriminants', *Math. Comp.* 58 (1992) 831–847.
3. B. K. SPEARMAN and K. S. WILLIAMS, 'The cubic congruence $x^3 + Ax^2 + Bx + C \equiv 0 \pmod{p}$ and binary quadratic forms', *J. London Math. Soc.* 46 (1992) 397–410.

Department of Mathematics and Statistics
Okanagan University College
Kelowna
British Columbia V1V 1V7
Canada

bkspearm@okuc02.okanagan.bc.ca

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa
Ontario K1S 5B6
Canada

williams@math.carleton.ca