THE NUMBER OF SOLUTIONS OF A TRINOMIAL CONGRUENCE INVOLVING A kTH POWER AND A SQUARE

BY J. T. CROSS

Communicated by G. B. Huff, September 28, 1962

Let K denote a finite extension of the rational number field and D the domain of algebraic integers of K. Let P be a prime ideal of D having norm $N(P)=p^h=q$, where h is a positive integer and p is an odd rational prime number. This announcement is concerned with the number of solutions of the trinomial congruence,

$$(1) \qquad X^k + \alpha Y^2 \equiv \rho \pmod{P^r},$$

where α and ρ are in D with ρ arbitrary and $(\alpha, P)=1$, r is a positive integer, k is a positive integer such that $(k, p)=1$, and $d=(k, q-1)>1$. Let C denote an ideal of D such that $(P, C)=1$ and $PC=(\theta)$ is principal, and let b be the greatest integer n such that $0\leqq n\leqq r$ and $P^n|\rho$. Then we may put

$$(2) \qquad \rho \equiv \eta\theta^b \pmod{P^r}, \qquad (\eta, P) = 1,$$

where η is uniquely determined (mod P^{r-b}) if $b<r$.

In Theorems 1–8 we give formulas for the number $Q_r(\rho)$ of solutions of (1). Solvability criteria are obtained as corollaries of these theorems. (We remark that if $\rho\equiv 0$ (mod P^r), then (1) has the trivial solution (0, 0).) The formulas given in this note follow directly from more general theorems proved for congruences (mod P^r) involving a kth power and an arbitrary number of squares [2].

If $r=1$, the congruence (1) amounts to an equation in a Galois field of order q. For discussions of general trinomial congruences in a finite field, particular reference is made to Vandiver [7] who has published several pertinent papers in recent years. A number of authors have considered the special case of (1) with $r=1$ and K the rational field; in particular we mention Frattini [3], E. Lehmer [5], and Manin [6]. For a discussion of trinomial congruences in algebraic number fields, see Cohen's paper [1].

We need the following notation:

$$(3) \qquad b = Lk + I \quad (0 \leqq I < k); \qquad \zeta = (-\alpha/P), \qquad \tau = (-\eta/P),$$

where (β/P) denotes the Legendre symbol in D.

Let $Q(\eta)=Q_1(\eta)$ denote the number of solutions of

$$(4) \qquad X^k + \alpha Y^2 \equiv \eta \pmod{P}, \qquad (\eta, P) = 1.$$

Theorems 1–4 and 7–8 below contain explicit formulas for the number of solutions of (1), while Theorems 5 and 6 are reduction formulas which give the number of solutions of (1) in terms of the number of solutions of (4). Theorems 5 and 6 apply if $d>2$, $\rho\not\equiv 0 \pmod{P^r}$, $b\equiv 0 \pmod{k}$, and bk is even; under these conditions it is not possible to give explicit formulas for $Q_r(\rho)$. Davenport and Hasse [4] have shown that $Q(\eta)\geqq q-(d-1)\sqrt{q}$, a result which we utilize in Corollary 7.

THEOREM 1. *If k is odd and $r>b\not\equiv 0 \pmod{k}$, then* $Q_r(\rho)(q^{k-2}-1)/q^{r-1} = (q-1)(q^{(k/2-1)L+k-2}-1)$ *for L even, I odd or for L even, I even, $\tau\zeta=-1$;* $(q-1)(q^{(k/2-1)L+k-2}-1)+2(q^{k-2}-1)q^{(k/2-1)L+I/2}$ *for L even, I even, $\tau\zeta=1$;* $(q-1)(q^{(k/2-1)(L+1)}-1)$ *for L odd, I even, or for L odd, I odd, $\tau\zeta=-1$;* $(q-1)(q^{(k/2-1)(L+1)}-1)+2(q^{k-2}-1)q^{(k/2-1)L+I/2}$ *for L odd, I odd, $\tau\zeta=1$.*

COROLLARY 1. *If k is odd and $b\not\equiv 0 \pmod{k}$, then (1) is solvable.*

THEOREM 2. *If $k=2$ and $r>b\not\equiv 0 \pmod{2}$, then $Q_r(\rho)/q^{r-1}=0$ for $\zeta=-1$; $2(q-1)(L+1)$ for $\zeta=1$. If k is even, $k>2$, and $r>b\not\equiv 0 \pmod{k}$, then $Q_r(\rho)(q^{k/2-1}-1)/q^{r-1}=0$ for I odd, $\zeta=-1$, or for I even, $\zeta=-1=-\tau$; $2(q-1)(q^{(k/2-1)(L+1)}-1)$ for I odd, $\zeta=1$, or for I even, $\zeta=1=-\tau$; $2q^{(k/2-1)L+I/2}(q^{k/2-1}-1)$ for I even, $\zeta=-1=\tau$; $2(q-1)(q^{(k/2-1)(L+1)}-1)+2q^{(k/2-1)L+I/2}(q^{k/2-1}-1)$ for I even, $\zeta=1=\tau$.*

COROLLARY 2. *If k is even and $r>b\not\equiv 0 \pmod{k}$, then* (a) *If I is odd, the congruence (1) is insolvable $\rightleftarrows \zeta=-1$.*

(b) *If I is even, the congruence (1) is insolvable $\rightleftarrows \zeta=-1=-\tau$.*

THEOREM 3. *If $k=2$ and $r>b\equiv 0 \pmod{2}$, then $Q_r(\rho)/q^{r-1} = (q-1)(1+2L)$ for $\zeta=1$; $q+1$ for $\zeta=-1$. If $d=2<k$ and $r>b\equiv 0 \pmod{k}$, then*

$$Q_r(\rho)(q^{k/2-1}-1)/q^{r-1} = (q-1)(q^{(k/2-1)(L+1)}+q^{(k/2-1)L}-2)$$

for $\zeta=$;1 $(q+1)q^{(k/2-1)L}(q^{k/2-1}-1)$ for $\zeta=-1$.

COROLLARY 3. *If $d=2$ and $b\equiv 0 \pmod{k}$, then (1) is solvable.*

THEOREM 4. *If k is odd, b is odd and $r>b\equiv 0 \pmod{k}$, then $Q_r(\rho)(q^{k-2}-1)/q^{r-1}=(q-1)(q^{(k/2-1)(L+1)}-1)$ for η not a kth power $\pmod{P}$; $(q-1)(q^{(k/2-1)(L+1)}-1)+dq^{(k/2-1)L+1/2}(q^{k-2}-1)$ for η a kth power $\pmod{P}$.*

COROLLARY 4. *If k is odd, b is odd, and $b\equiv 0 \pmod{k}$, then (1) is solvable.*

THEOREM 5. *If k is even, $d>2$, and $r>b\equiv 0 \pmod{k}$, then* $Q_r(\rho)/q^{r-1} = q^{(k/2-1)L}Q(\eta)$ *for* $\zeta=-1$ *and*

$$Q_r(\rho)(q^{k/2-1}-1)/q^{r-1} = q^{(k/2-1)/L}\{q^{k/2}+q-2+(Q(\eta)-q)\cdot(q^{k/2-1}-1)\}-2(q-1) \quad \textit{for } \zeta=1.$$

COROLLARY 5. *If k is even, $d>2$, and $r>b\equiv 0 \pmod{k}$, then*
(a) *If* $\zeta=-1$, $Q_r(\rho)=0 \rightleftarrows Q(\eta)=0$.
(b) *If* $\zeta=1$, $Q_r(\rho)=0 \rightleftarrows Q(\eta)=0$ *and* $L=0$.

THEOREM 6. *If k is odd, b is even and $r>b\equiv 0 \pmod{k}$, then*

$$Q_r(\rho)(q^{k-2}-1)/q^{r-1} = 1-q+q^{(k/2-1)L}\{q^{k-1}-1+(Q(\eta)-q)(q^{k-2}-1)\}.$$

COROLLARY 6. *If k is odd, b is even, and $r>b\equiv 0 \pmod{k}$, then* $Q_r(\rho)=0 \rightleftarrows Q(\eta)=0$ *and* $L=0$.

Since $Q(\eta)\geqq q-(d-1)\sqrt{q}$, one obtains from Corollaries 5 and 6,

COROLLARY 7. *If $d>2$, bk is even, and $r>b\equiv 0 \pmod{k}$, then* (1) *is solvable if $q>(d-1)^2$; moreover,* (1) *is solvable for arbitrary q if $L\neq 0$ and k is odd, or if $L\neq 0$ and $\zeta=1$.*

For completeness, the following formulas in the case $b=r$ ($\rho\equiv 0 \pmod{P^r}$) are also included.

THEOREM 7. *If $k=2$ and $b=r$, then* $Q_r(\rho)/q^{r-1}=q+(q-1)r$ *for* $\zeta=1$; q *for* $\zeta=-1$, *r even*; 1 *for* $\zeta=-1$, *r odd. If k is even, $k>2$ and $b=r$, then* $Q_r(\rho)/q^{r-1}=q^{(k/2-1)L+1}$ *for* $I=0$, $\zeta=-1$;

$$\{q^{(k/2-1)L}(q^{k/2}+q-2)-2(q-1)\}/(q^{k/2-1}-1) \textit{ for } I=0,\ \zeta=1;$$

$q^{(k/2-1)L+I/2}$ *for I even,* $I>0$, $\zeta=-1$; $q^{(k/2-1)L+(I-1)/2}$ *for I odd,* $\zeta=-1$; $\{q^{(k/2-1)L}(q^{k/2}+q-2)-2(q-1)\}/(q^{k/2-1}-1)+q^{(k/2-1)L}(q^{I/2}+q-2)$ *for I even,* $I>0$, $\zeta=1$; $\{q^{(k/2-1)L}(q^{k/2}+q-2)-2(q-1)\}/(q^{k/2-1}-1)+q^{(k/2-1)L}(q^{(I-1)/2}+q-2)$ *for I odd,* $\zeta=1$.

THEOREM 8. *If k is odd and $b=r$, then*

$$Q_r(\rho)/q^{r-1} = \{q^{(k/2-1)L}(q^{k-1}-1)-q+1\}/(q^{k-2}-1) + q^{(k/2-1)L}(q^{I/2}-1) \textit{ for } L \textit{ even, } I \textit{ even};$$

$\{q^{(k/2-1)L}(q^{k-1}-1)-q+1\}/(q^{k-2}-1)+q^{(k/2-1)L}(q^{(I-1)/2}-1)$ *for L even, I odd*; $\{q^{(k/2-1)L}(q^{k-3/2}+q^{k/2}-q^{k/2-1}-q^{1/2})-q+1\}/(q^{k-2}-1)$ *for L odd,* $I=0$;

$$\left\{q^{(k/2-1)L}(q^{k-3/2}+q^{k/2}-q^{k/2-1}-q^{1/2})-q+1\right\}/(q^{k-2}-1)$$
$$+\ q^{(k/2-1)L+1/2}(q^{I/2-1}-1) \text{ for } L \text{ odd, } I \text{ even, } I>0;$$
$$\left\{q^{(k/2-1)L}(q^{k-3/2}+q^{k/2}-q^{k/2-1}-q^{1/2})-q+1\right\}/(q^{k-2}-1)$$
$$+\ q^{(k/2-1)L+1/2}(q^{(I-1)/2}-1) \text{ for } L \text{ odd, } I \text{ odd.}$$

We now apply the formulas to a few examples, letting K be the rational field. $X^3+Y^2\equiv 2\cdot 7^3 \pmod{7^4}$ has 2,058 solutions by Theorem 4; $X^4+2Y^2\equiv 25 \pmod{125}$ has no solutions by Corollary 2; $X^4+Y^2\equiv 3\cdot 5^4 \pmod{5^5}$ has 5,000 solutions by Theorem 5; $X^6+Y^2\equiv 6\cdot 7^6 \pmod{7^7}$ has no solutions by Corollary 5.

Bibliography

1. Eckford Cohen, *Binary congruences in algebraic number fields*, Proc. Nat. Acad. Sci. **42** (1956), 120–122.

2. J. T. Cross, *The number of solutions of certain types of congruences in algebraic number fields*, (to appear).

3. G. Frattini, *Intorno ad un teorema di Lagrange*, Atti Reale Accad. Lincei Rend. **1** (1885), 136–142.

4. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182.

5. Emma Lehmer, *On the number of solutions of $u^k+D=w^2$ (mod p)*, Pacific J. Math. **5** (1955), 103–118.

6. Yu. I. Manin, *On cubic congruences to a prime modulus*, Amer. Math. Soc. Transl. (2) **13** (1960), 1–7.

7. H. S. Vandiver, *On the number of solutions of certain non-homogeneous trinomial equations in a finite field*, Proc. Nat. Acad. Sci. **31** (1945), 170–175.

The University of Tennessee and
The University of the South