und daraus folgt, wie im Falle 1),

$$\mathfrak{N}_{2k}(x, r) = i^{2-r}\frac{(2\pi)^r}{r!}\{Z(k)\}^{-1}\Psi_{k,r}(x).$$

Wegen (25) und (3) ist Satz 6 auch in diesem letzten Fall bewiesen.

TIFLIS, DEN 5. NOVEMBER 1959
MATHEMATISCHES INSTITUT

Literatur

[1] А. П. Лурсманашвили, *О числе целых точек в многомерных шарах*, Труды Тбилисского Математического Института 19 (1953), 79-120.

[2] H. Petersson, *Über die Anzahl der Gitterpunkte in mehrdimensionalen Ellipsoiden*, Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität 5 (1926), 116-150.

[3] A. Walfisz, *Über Gitterpunkte in mehrdimensionalen Kugeln*, Mathematische Zeitschrift 27 (1927), 469-480.

[4] — *О представлении чисел суммами квадратов. Асимптотические формулы*, Успехи математических наук 7 (1952), 97-178. Auch englisch: *On the representation of numbers by sums of squares. Asymptotic formulas*, American Mathematical Society Translations, Series 2, 3 (1956), 163-248.

[5] — *Gitterpunkte in mehrdimensionalen Kugeln*, Warszawa 1957.

Reçu par la Rédaction le 17. 11. 1959

ACTA ARITHMETICA
VI (1960)

On a Pellian equation conjecture

by

L. J. MORDELL (Boulder, Colo.)

In a joint paper by Ankeny, Artin, and Chowla (see [1]), there is enunciated the following:

CONJECTURE. *Let p be a prime $\equiv 1 \pmod 4$, and let $\varepsilon = \frac{1}{2}(t+u\sqrt{p}) > 1$ be the fundamental unit in the quadratic field $K(\sqrt{p})$ over the rational field K. Then $u \not\equiv 0 \pmod p$.*

Here $(y, x) = (t, u)$ is that solution of

$$y^2 - px^2 = -4 \tag{1}$$

with $y > 0$ and with least positive integer value for x. The equation is of course known to be solvable and an explicit solution is given in (8) and (11) below. It is also stated that when $p \equiv 5 \pmod 8$, the conjecture has been verified for all $p < 2000$. The only further explicit result about the conjecture seems to be that Professor Taussky-Todd has had it verified for $p \equiv 1 \pmod 4$ with $p < 100{,}000$ by Dr. Goldman.

I prove here the

THEOREM I. *If p is a regular prime, i. e. the number of classes of ideals in the cyclotomic field $K(e^{2\pi i/p})$ is not divisible by p, then $u \not\equiv 0 \pmod p$, i. e. the conjecture is true.*

As is well known, Kummer has proved that p is regular if and only if none of the numerators of the first $\frac{1}{2}(p-3)$ Bernoulli numbers as defined in (2) is divisible by p. He has shown that the only non-regular primes < 100 are 37, 59, 67.

Theorem IV of the joint paper contains the result that if h is the class number for the quadratic field $K(\sqrt{p})$, then if $p \equiv 5 \pmod 8$,

$$-2h\frac{u}{t} \equiv C_{(p-3)/2} \pmod p, \tag{1a}$$

where for this particular case, $C_{(p-3)/2}$ is defined by

$$\sum_{n=-1}^{\infty}\frac{C_n t^n}{n!} = 1 + \frac{1}{e^t - 1}.$$

In Kummer's notation,

$$(2)\qquad \frac{1}{e^t-1} = \frac{1}{t} - \frac{1}{2} + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}B_n}{(2n)!} t^{2n-1}.$$

Put $2n-1 = \frac{1}{2}(p-3)$, $n = \frac{1}{4}(p-1)$, then $C_{(p-3)/2} = \pm B_{(p-1)/4}$. Hence from (1a), it follows that $hu \equiv 0$ if and only if $B_{(p-1)/4} \equiv 0 \pmod{p}$. I cannot find any reference to the fact that, as I prove here, this implies $u \equiv 0$ if and only if $B_{(p-1)/4} \equiv 0 \pmod{p}$. Thus, this seems to be unknown to Carlitz [3] who gives, inter alia, a different form of (1a). Professor Chowla, however, informs me that at the time the joint paper was written, he had noticed but not published the result that $h < p$. He gives now a proof in the paper following this. We have then

THEOREM II. *If p is a prime $\equiv 5 \pmod 8$, the fundamental unit $\frac{1}{2}(t+u\sqrt{p})$ in the field $K(\sqrt{p})$ has $u \equiv 0 \pmod{p}$, if and only if*

$$(3)\qquad B_{(p-1)/4} \equiv 0 \pmod{p}.$$

This can also be written as

$$1^{(p-1)/2} + 2^{(p-1)/2} + \ldots + (p-1)^{(p-1)/2} \equiv 0 \pmod{p^2}.$$

I give a simpler proof of (3). It is based essentially on the same ideas employed by the other writers, i. e. that of a p'adic logarithm, but this is presented rather differently. Moreover, the present proof depends on explicit formulae for units in the quadratic field $K(\sqrt{p})$ given at once by putting $x = \pm 1$ in the factorization of $(x^p-1)/(x-1)$, and these are much simpler than formulae for a fundamental unit.

I show also that when the field $K(e^{2\pi i/p})$ is regular, the fundamental solution $(y, x) = (T, U)$ of

$$(4)\qquad y^2 - px^2 = 1$$

has $U \not\equiv 0 \pmod{p}$. It suffices to prove the existence of any solution of (4) with $x \not\equiv 0 \pmod{p}$. For since the general solution of (4) is given by

$$y + x\sqrt{p} = \pm(T \pm U\sqrt{p})^n,$$

where n is a positive integer, it is clear that if $U \equiv 0 \pmod{p}$, then $x \equiv 0 \pmod{p}$, i. e. all the solutions of (4) would have $x \equiv 0 \pmod{p}$.

Next it suffices to find any solution (x, y) with $x \not\equiv 0 \pmod{p}$ of

$$(5)\qquad y^2 - px^2 = -1.$$

This is known to be solvable and an explicit solution is given by (6a) and (11). Then

$$y_1 + x_1\sqrt{p} = (y + x\sqrt{p})^2$$

gives a solution (x_1, y_1) of (4) with $x_1 = 2xy$ and clearly $x_1 \not\equiv 0 \pmod{p}$.

Finally it suffices to find any solution (x, y) with $x \not\equiv 0 \pmod{p}$ of

$$(6)\qquad y^2 - px^2 = -4.$$

For if x, y are both even, then $x_1 = \frac{1}{2}x$, $y_1 = \frac{1}{2}y$ is a solution of (5) with $x_1 \not\equiv 0 \pmod{p}$. This certainly occurs when $p \equiv 1 \pmod 8$. We may suppose then that $p \equiv 5 \pmod 8$, and that x and y are both odd. A solution (x_1, y_1) of (5) is given by

$$y_1 + x_1\sqrt{p} = \left(\frac{y + x\sqrt{p}}{2}\right)^3,$$

i. e.

$$(6a)\qquad x_1 = \frac{x}{8}(3y^2 + px^2).$$

Clearly $3y^2 + px^2 \equiv 0 \pmod 8$, and so x_1 is an integer, and x_1 is divisible by p if and only if x is.

Since the general solution of (6) is given by

$$\frac{y + x\sqrt{p}}{2} = \pm\left(\frac{t \pm u\sqrt{p}}{2}\right)^{2n+1},$$

clearly we need only find a solution of (6) with $x \not\equiv 0 \pmod{p}$, for if $u \equiv 0 \pmod{p}$, then $x \equiv 0 \pmod{p}$. Hence also a solution with $x \not\equiv 0$ of any one of the equations (4), (5), (6) leads to a similar solution for the other equations.

We now consider the cyclotomic field $K(\zeta)$ where $\zeta = e^{2\pi i/p}$. We have the ideal factorization,

$$(p) = (P)^{p-1} \quad \text{where} \quad P = 1 - \zeta,$$

which of course easily follows from

$$(7)\qquad \frac{x^p - 1}{x - 1} = \prod_{m=1}^{p-1} (x - \zeta^m).$$

The cyclotomic field $K(\zeta)$ contains the quadratic field $K(\sqrt{p})$ as a subfield. On putting $x = 1$ in (7), we have

$$(8)\qquad p = \prod_r (1 - \zeta^r) \prod_n (1 - \zeta^n) = RN,$$

say, where r refers to the quadratic residues of p and n to the non-quadratic residues. Here R and N are integers in $K(\sqrt{p})$, and so

$$(9)\qquad 2R = X_1 + Y_1\sqrt{p}, \quad 2N = X_1 - Y_1\sqrt{p},$$

where X_1, Y_1 are rational integers, and

$$4p = X_1^2 - pY_1^2.$$

Put $X_1 = pX$, $Y_1 = Y$, whence,

$$Y^2 - pX^2 = -4. \tag{10}$$

Hence

$$E_1 = R/\sqrt{p} = \tfrac{1}{2}(Y + X\sqrt{p}), \qquad E_2 = N/\sqrt{p} = \tfrac{1}{2}(-Y + X\sqrt{p}), \tag{11}$$

are both units in $K(\sqrt{p})$ and so also in $K(\zeta)$.

Let us suppose that the conjecture is false and so $X \equiv 0 \pmod{p}$. Then $E = -E_1/E_2$ is a cyclotomic unit for which $E \equiv 1 \pmod{p^{3/2}}$. We prove as a particular case of a general result that when p is a regular prime, E is the p'th power of a unit in $K(\zeta)$. Suppose this is not true, and so there exists a non-degenerate Kummer field $K(\zeta, \sqrt[p]{E})$. Then from Theorem 148 in Hilbert's report on algebraic numbers, the relative discriminant of $K(\zeta, \sqrt[p]{E})$ with respect to $K(\zeta)$ is unity since $E \equiv 1 \pmod{P^p}$. Then from Theorem 94, there is in $K(\zeta)$ an ideal J which is not a principal ideal in $K(\zeta)$ but J^p is. Also J is a principal ideal in $K(\zeta, \sqrt[p]{E})$ and the class number of $K(\zeta)$ is divisible by p. Hence on considering the Kummer field $K(\zeta, \sqrt[p]{E/E'})$ where E' is the conjugate of E, we have Kummer's result, Theorem 156, that if there exists a unit E in $K(\zeta)$ congruent to a rational number mod p, then E is the p'th power of a unit in $K(\zeta)$ provided that p is a regular prime. This gives a contradiction.

Hence

$$\frac{Y + X\sqrt{p}}{Y - X\sqrt{p}} = E_3^p,$$

where E_3 is a unit in $K(\zeta)$. Since E_3 is an element of algebraic fields of orders $p-1$ and $2p$, E_3 must be a unit in $K(\sqrt{p})$, i. e., $E_3 = \tfrac{1}{2}(\eta + \xi\sqrt{p})$, where ξ, η are integers. Hence

$$|E_3|^p = \left|\frac{Y + X\sqrt{p}}{2}\right|^2 = \frac{|R|^2}{p} \leqslant \frac{2^{p-1}}{p}.$$

Hence $|E_3| < 2$, and so $|\xi + \eta\sqrt{p}| < 4$.

Similarly from the unit conjugate to E_3, $|\eta - \xi\sqrt{p}| < 4$, and so $|\eta| < 4$, $|\xi\sqrt{p}| < 4$. Then either $p = 5$ and $\xi = 1$, $\eta = 1$, or $p = 13$, and $\xi = 1$, $\eta = 3$, or $p > 13$, and then $\xi = 0$, and no solution arises. This concludes the proof of the theorem.

I now prove (3). Let x be any integer in $K(\zeta)$. Then if $x \equiv 1 \pmod{P}$, $g(x) = (x^p - 1)/p$ is an integer. For if $x = 1 + aP$,

$$pg(x) = apP + \frac{p \cdot p-1}{2!} a^2P^2 + \ldots + pa^{p-1}P^{p-1} + a^pP^p.$$

The result follows since $(P^{p-1}) = (p)$. Also $g(x) \equiv 0 \pmod{P}$. We next define for $x \equiv 1 \pmod{P}$,

$$f(x) \equiv \frac{x^p - 1}{p} \pmod{p}.$$

This defines residue classes (mod p) and has been long (see Bachmann [2]) known for rational integers x. For if $x \equiv y \pmod{p}$, $x = y + ap$ and

$$f(x) - f(y) \equiv \frac{y^{p-1}pap + y^{p-2}\frac{p \cdot p-1}{2!}a^2p^2 + \ldots + a^pp^p}{p} \pmod{p}$$
$$\equiv 0 \pmod{p}.$$

Clearly, $f(1) \equiv 0 \pmod{p}$. Further, $f(x)$ has the characteristic property of a logarithm, i. e. if $x \equiv 1 \pmod{P}$, and $y \equiv 1 \pmod{P}$, then

$$f(xy) \equiv f(x) + f(y) \pmod{p}. \tag{12}$$

For

$$f(xy) - f(x) - f(y) \equiv \frac{(x^p - 1)(y^p - 1)}{p} \equiv 0 \pmod{p}.$$

Then also

$$f\left(\frac{y}{x}\right) \equiv f(y) - f(x) \pmod{p}. \tag{13}$$

The function $f(x)$ is equivalent to the p'adic logarithm of x, and this is used in the joint paper.

In $\dfrac{x^p - 1}{x - 1} = \prod_r (x - \zeta^r) \prod_n (x - \zeta^n)$, put $x = -1$, then we have with rational integers x, y,

$$2\prod_r (1 + \zeta^r) = y + x\sqrt{p}, \qquad 2\prod_n (1 + \zeta^n) = y - x\sqrt{p},$$

and

$$4 = y^2 - px^2.$$

Hence $\tfrac{1}{2}(y + x\sqrt{p})$ is a unit (which may be ± 1). Since for such x, y, there exists a solution X, Y of (6) with $\dfrac{y + x\sqrt{p}}{2} = \left(\dfrac{Y + X\sqrt{p}}{2}\right)^2$, then $p \mid X$ only if $p \mid x$.

Suppose now that $x \equiv 0 \pmod{p}$, then

$$\prod_r \left(\frac{1+\zeta^r}{2}\right) - \prod_n \left(\frac{1+\zeta^n}{2}\right) \equiv 0 \pmod{p^{3/2}}.$$

Since $\dfrac{1+\zeta^r}{2} \equiv 1 \equiv \dfrac{1+\zeta^n}{2} \pmod{P}$, we can apply equations (12) and (13),

and so since $\prod_n \left(\dfrac{1+\zeta^n}{2}\right) \not\equiv 0 \pmod{P}$,

$$\frac{\sum_r (1+\zeta^r)^p - \sum_n (1+\zeta^n)^p}{p} \equiv 0 \pmod{p}.$$

Write

$$\sqrt{p} = \sum_r \zeta^r - \sum_n \zeta^n,$$

and then

$$\sqrt{p}\left(\frac{a}{p}\right) = \sum_r \zeta^{ar} - \sum_n \zeta^{an},$$

where a is any integer. Hence

$$\frac{\sqrt{p}}{p}\left(p + \frac{p\cdot p-1}{2!}\left(\frac{2}{p}\right) + \ldots + p\left(\frac{p-1}{p}\right)\right) \equiv 0 \pmod{p},$$

or

$$1 + \frac{p-1}{2!}\left(\frac{2}{p}\right) + \frac{p-1\cdot p-2}{3!}\left(\frac{3}{p}\right) + \ldots + \left(\frac{p-1}{p}\right) \equiv 0 \pmod{p^{1/2}}.$$

The left-hand side is a rational number, and so

$$1 - \frac{1}{2}\left(\frac{2}{p}\right) + \frac{1}{3}\left(\frac{3}{p}\right) - \ldots - \frac{1}{p-1}\left(\frac{p-1}{p}\right) \equiv 0 \pmod{p}.$$

Since $\left(\dfrac{a}{p}\right) \equiv a^{(p-1)/2}$ and $1/a \equiv a^{-1}$,

(13a) $\quad S = 1 - 2^{(p-3)/2} + 3^{(p-3)/2} - \ldots - (p-1)^{(p-3)/2} \equiv 0 \pmod{p}.$

This is a necessary and sufficient (⁰) condition that $x \equiv 0 \pmod{p}$.

Here $\left(\dfrac{p-3}{2}\right)!\,S$ is the coefficient of $t^{(p-3)/2}$ in the expansion in ascending powers of t of

$$-1 + e^t - e^{2t} + \ldots - e^{(p-1)t} = -\frac{1+e^{pt}}{1+e^t}.$$

(⁰) See note at end.

Since we are considering residues (mod p), we can ignore e^{pt}, and write

$$-\frac{1}{1+e^t} = \frac{1}{1-e^t} - \frac{2}{1-e^{2t}}.$$

But

$$\frac{1}{e^t-1} = \frac{1}{t} - \frac{1}{2} + \frac{B_1 t}{2!} - \frac{B_2 t^3}{4!} + \ldots + (-1)^{m-1}\frac{B_m t^{2m-1}}{(2m)!} + \ldots$$

Hence taking $m = \frac{1}{4}(p-1)$,

$$B_{(p-1)/4} - 2\cdot 2^{(p-3)/2} B_{(p-1)/4} \equiv 0 \pmod{p},$$

and so if $p \equiv 5 \pmod{8}$, since $2^{(p-1)/2} \equiv -1$,

(14) $\quad B_{(p-1)/4} \equiv 0 \pmod{p}.$

The usual summation formula gives

$$1^{2a} + 2^{2a} + \ldots + (p-1)^{2a} \equiv (-1)^{a-1} B_a p \pmod{p^2}$$

and the condition (14) becomes on putting $a = (p-1)/2$,

(15) $\quad 1^{(p-1)/2} + 2^{(p-1)/2} + \ldots + (p-1)^{(p-1)/2} \equiv 0 \pmod{p^2}.$

We have to show finally that the unit $y + x\sqrt{p}$ is not ± 2, when $p \equiv 5 \pmod{8}$. Suppose that $x = 0$. Then $\prod_r (1+\zeta^r) = \pm 1$. On taking residues (mod P), since $2^{(p-1)/2} \equiv -1$, we have the minus sign, and so $\prod_r (1+\zeta^r) = -1$. We write this as

$$\prod_{r\leqslant(p-1)/2} (1+\zeta^r)(1+\zeta^{-r}) = -1,$$

or (¹)

$$\prod_{r\leqslant(p-1)/2} (1+\zeta^r)^2 = -\zeta^b \quad \text{where} \quad b = \sum_{r\leqslant(p-1)/2}.$$

The exponent b can be replaced by an even positive number, say $2a$. Then we have identically in a variable z

$$\prod_{r\leqslant(p-1)/2} (1+z^r)^2 + z^{2a} = (1+z+z^2+\ldots+z^{p-1})\,F(z),$$

where $F(z)$ is a polynomial in z with rational integer coefficients. Put $z = 2$. Then $1+z+z^2+\ldots+z^{p-1} = 2^p - 1 \equiv 3 \pmod{4}$ must divide the left-hand side. This is impossible since for $z = 2$, z^a and $\prod_{r\leqslant(p-1)/2}(1+z^r)$ have no common factor.

(¹) I find this result is given by J. Schumacher, [4].

We have so far proved that $x \neq 0$, and that $x \equiv 0 \pmod{p}$ if and only if $B_{(p-1)/4} \equiv 0 \pmod{p}$. Hence $x \not\equiv 0$, and so $u \not\equiv 0$ if $B_{(p-1)/4} \not\equiv 0$. If, however, $B_{(p-1)/4} \equiv 0$, then $x \equiv 0$, and we prove that now $u \equiv 0$. For since

$$\frac{y+x\sqrt{p}}{2} = \pm\left(\frac{t\pm u\sqrt{p}}{2}\right)^n \quad \text{for some positive integer } n,$$

it is obvious that if $u \not\equiv 0$, then $n \equiv 0$. But

$$\left|\frac{y+x\sqrt{p}}{2}\right| < 2^p, \quad \left|\frac{y-x\sqrt{p}}{2}\right| < 2^p,$$

and so

$$\left|\frac{t+u\sqrt{p}}{2}\right| < 2, \quad \left|\frac{t-u\sqrt{p}}{2}\right| < 2.$$

The cases so arising have already been disposed of.

This concludes the proof.

Note. I add a proof that the condition (13a) is sufficient. Let z be an integer in $K(\zeta)$ and let $(z^p-1)/p \equiv 0 \pmod{p}$. Since $(p) = (P)^{p-1}$, this congruence can have only the p obvious roots $z \equiv \zeta \pmod{p}$, $t = 0, 1, p-1$. Hence if (13a) is satisfied,

$$\prod_r (1+\zeta^r) / \prod_n (1+\zeta^n) \equiv \zeta^t \pmod{p}.$$

Take residues $\bmod P^2$. Since $\zeta = 1-P$,

$$\prod_r (2-Pr) / \prod_n (2-Pn) \equiv 1-tP \pmod{P^2},$$

and so

$$\sum \tfrac{1}{2}P(n-r) \equiv -tP \pmod{P^2}.$$

Since $\sum(n-r) \equiv 0 \pmod{p}$, $t \equiv 0 \pmod{p}$, and so $x \equiv 0 \pmod{p}$.

References

[1] N. C. Ankeny, E. Artin, S. Chowla, *The class-number of real quadratic number fields*, Annals of Mathematics 51 (1952), p. 479-493.

[2] Bachmann, *Nieder Zahlentheorie*, Erster Teil,

[3] L. Carlitz, *Note on the class number of real quadratic fields*, Proceedings of the American Mathematical Society 4 (1953), p. 535-537.

[4] J. Schumacher, Archiv Math. Phys. 3 (23) (1914-1915), p. 80-81.

COLORADO UNIVERSITY, BOULDER, U.S.A.
ST. JOHNS COLLEGE, CAMBRIDGE, ENGLAND

Reçu par la Rédaction le 23. 11. 1959

ACTA ARITHMETICA
VI (1960)

A note on the class number of real quadratic fields

by

N. C. Ankeny (Cambridge, Mass.) and S. Chowla (Boulder, Colo.)

1. Let $h = h(p)$ denote the class-number of the real quadratic field $R(\sqrt{p})$, where p is a prime $\equiv 1 \pmod 4$ and let $\varepsilon = t+u\sqrt{p}/2 > 1$ be its fundamental unit.

Ankeny, Artin, Chowla (also Kiselev, independently) have proved that (we gave details only for $p \equiv 5 \pmod 8$)

$$\frac{uh}{t} \equiv \frac{B_{p-1}}{4} \pmod{p},$$

where B_n is a Bernoulli number defined by

$$\frac{x}{e^x-1} = 1-\frac{x}{2}+\sum_{n=1}^{\infty}\frac{B_n x^{2n}}{(2n)!}.$$

They also raised a question — still unsettled — can it happen that $u \equiv 0 \pmod{p}$ when $p \equiv 1 \pmod 4$? We had noticed at the time this paper was written that $h < p$, but we did not mention this. Hence, as Mordell has said in the preceding paper, $u \equiv 0 \pmod{p}$ if and only if $B_{p-1}/4 \equiv 0 \pmod{p}$, when $p \equiv 5 \pmod 8$. In the case when $p \equiv 5 \pmod 8$, Mordell has also given there a different proof of this. It seems now desirable to give the proof that $h < p$, especially as the work of other writers seems to indicate that this cannot be well known. Thus, Carlitz in Proc. Amer. Math. Soc. 4 (1953), p. 535-537, says (in our notation for the B's) "... $B_{p-1}/4 \equiv 0 \pmod{p}$ if and only if either $h \equiv 0$ or $u \equiv 0$". Selfridge, Nicol and Vandiver in their *Proof of Fermat's Last Theorem for all prime exponents less than 4002*, Proc. National Academy of Sciences, U. S. A. 41 (1955), p. 972, say "in particular the class number h of the field $K(\sqrt{l})$, where $l \equiv 1 \pmod 4$, is prime to l for the said l's". The "said" l's, here, are the primes < 4002.