ACTA ARITHMETICA
XVIII (1971)

Some results and problems in number theory

by

S. CHOWLA (State College, Pa)

Dedicated to the memory of
my friend H. Davenport

§ 1. Let p denote a prime $\equiv 1(4)$. By Fermat we have

(1) $$p = a^2+b^2$$

where w.l.o.g.

(2) $$a \equiv 1 (\mathrm{mod}\, 4).$$

As an application of ideas of Tate–Dwork on the "Hasse-invariant" we note the following formula for the base a in (1) in this classical theorem of Fermat:

(3) $$a \equiv \frac{(-1)^{(p-1)/4}}{2} F_{(p+1)/2}(\tfrac{1}{2}, \tfrac{1}{2}, 1, -1)$$

where the congruence is $(\mathrm{mod}\, p)$ and $F_N(a, \beta, \gamma, x)$ denotes the sum of the first N terms in the hypergeometric series of Gauss.

EXAMPLE. $p = 5$. Then $a = 1$. And

$$1 \equiv -\tfrac{1}{2}\{1-(\tfrac{1}{2})^2+(\tfrac{1\cdot 3}{2\cdot 4})^2\}$$

is certainly true $(\mathrm{mod}\, 5)$.

§ 2. One may ask, as Galois might have asked what are the non-trivial linear relations between the roots of an irreducible equation (c's $\in Q$)

(4) $$x^n + c_{n-2}x^{n-2}+\ldots+c_0 = 0 ?$$

Here a trivial relation is (call the roots $a_1, a_2, \ldots, a_n$)

(5) $$a_1+a_2+\ldots+a_n = 0.$$

In particular, suppose that[1]

$$a_m = \cot\frac{m\pi}{p} \quad (1 \leqslant m \leqslant p-1).$$

[1] p is an odd prime.

Here besides (5) we have the other trivial relations

$$(6) \qquad a_m + a_{p-m} = 0 \qquad [m < \tfrac{1}{2}p).$$

It is reasonable to suppose that all the trivial linear relations between the a's in this special case are "derived" from (6), as (5) certainly may. In the special case when both p and $\frac{p-1}{2}$ are primes I proved this in a letter to Prof. C. L. Siegel (1949). Prof. Siegel considerably generalized my result. Recently Prof. Hasse has found simple and elegant proofs of such "tan-cot" theorems. See his paper in this volume. As one may expect all the proofs rely on the non-vanishing of series $\sum_{1}^{\infty} \frac{\chi(n)}{n}$ where $\chi(n)$ is a character (mod p).

§ 3. Recently Prof. Hasse and I have found the following result which will appear in Crelles journal. Let $x = x_0(p)$, $y = y_0(p)$ be the *smallest* positive solution of the Pellian equation

$$x^2 - py^2 = \pm 1.$$

One may conjecture that there are infinitely many primies p such that

$$x_0(p) > p^A$$

where A is an arbitrary real number. We prove that this conjecture is true if one assumes the "reasonable" conjecture that there are infinitely many primes of the form x^2+36.

For a superficial connection of this result with a Davis–Putnam hypothesis concerning Hilbert's Tenth problem, see a paper by me in the Proceedings of the Number-theory Conference at Boulder, Colorado, in 1963.

Received on 15. 3. 1970

ACTA ARITHMETICA
XVIII (1971)

On a question of S. Chowla

by

HELMUT HASSE (Ahrensburg)

To the memory of my friend Harold Davenport

0. S. Chowla has raised the question whether for an odd prime $p = 2n+1$ the n division values

$$(1) \qquad \tan\frac{r\pi}{p}, \qquad \cot\frac{r\pi}{p} \qquad (r = 1, \ldots, n),$$

respectively, are linearly independent over the rationals.

I shall prove here:

THEOREM. *Necessary and sufficient for the linear independence over the rationals of the n values* (1) *is that the sums*

$$(2) \qquad \sum_{s=1}^{n} (-1)^s \chi(s) = \chi(2) \sum_{s=1}^{n} \chi(s), \qquad \sum_{s=1}^{n} (2s-p)\chi(s) = \sum_{s=1}^{n} s\chi(s),$$

respectively, over the values of the n odd characters χ mod p *are all different from zero.*

Since the second sums in (2) are known to be the factors of $-(-2p)^{n-1}h^*(p)$ where $h^*(p)$ is the relative class-number of the pth cyclotomic field $C(p)$ (1), it follows from this Theorem that *the answer to Chowla's question for the* cot*-values is in the positive.*

For the tan-values, however, I succeeded to answer it only in the special cases where n is either an odd prime or a power of 2, again in the positive (2). In these special cases I could moreover give a proof of the positive answer for the cot-values, which is not based on the analytic class-number formula, but proceeds quite elementarily.

1. The values (1) belong to the cyclotomic field $C(2^2p)$ but can be brought to $C(p)$ by a factor i which is irrelevant for Chowla's question.

(1) Cf. the author's monography *Über die Klassenzahl abelscher Zahlkörper*, Berlin 1952, p. 12, (3b) and p. 68, Satz 23.

(2) See, however, the Addendum at the end.