ON A CONJECTURE OF MARSHALL HALL

BY S. CHOWLA

PENNSYLVANIA STATE UNIVERSITY

Communicated by Deane Montgomery, June 8, 1966

Let $p$ be a prime $\geq 7$ such that the class-number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ is 1. At a seminar on complex multiplication at the Institute for Advanced Study (1957–58), I pointed out that the following theorem is true:

If $p$ is a prime with the property stated above, then the equation

$$x^3 - py^2 = -1728$$

(1)

has a solution with

$$x = \{e^{\sqrt{p}/3}\},$$

(2)

where $\{w\}$ denotes the integer nearest to $w$.

As a matter of fact, this theorem can be read off from Weber’s classical Lehrbuch der Algebra, volume 3.

In a recent paper (by Birch, Chowla, Hall, and Schinzel), we cited M. Hall’s conjecture that if $x$, $y$ are integers, then

$$|x^3 - y^2| > \sqrt{|x|} (|x| > x_0),$$

(3)

provided $x^2 \neq y^2$.

We wish to point out a connection between our theorem and Hall’s conjecture. It is well known that it is still an unsolved problem $(P)$ to find a determinable constant $c$ such that $h > 1$ for $p > c$. Here $h$ is the class-number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

Set $x = p^{-1}u$, $y = p^{-2}v$ in (2). Then (2) becomes

$$u^3 - v^2 = -1728 p^3.$$  

(4)

Thus if the class-number $h$ of $\mathbb{Q}(\sqrt{-p})$ is 1, we conclude that (4) has a solution in integers $u$, $v$ and further with

$$u = p \{e^{\sqrt{p}/3}\}.$$  

(5)

Now (4) and (5) contradict (3) for large $p$. Thus we see that a proof of Hall’s conjecture would immediately, in conjunction with our observation, lead to a new proof of the theorem (conjectured by Gauss, proved by Heilbronn) that $h > 1$ for $p > c$. Our theorem also shows that if $x_0$ in Hall’s conjecture is a determinable constant, then the $c$ above is also a determinable constant, i.e., problem $P$ would then be solved.

If the positive integers $x$ and $y$ tend to infinity through values for which $x^3 \neq y^2$, it is known that

$$|x^3 - y^2| \to \infty.$$  

(6)

Our method shows, for example, that if we can replace (6) by

$$|x^3 - y^2| > c \log^2 x,$$  

(7)

417
where $c$ is a computable positive constant, then the unsolved problem $P$ would be solved.

1 Professor A. Borel has informed me that the seminar notes will be published by Springer-Verlag.