Pure and Applied Mathematics Quarterly
Volume 8, Number 3
689—691, 2012

A Dibisibility Problem Concerning Group Theory*

Maohua Le

Abstract: Let p be an odd prime with $p \neq 3$. In this paper we prove that $p^2 + p + 1 \nmid 3^p - 1$.
Keywords: divisibility, binary quadratic diophantine equation, cubic residue, solvable group.

Let $\mathbf{Z}, \mathbf{N}$ be the sets of all integers and positive integers respectively. Let p and q be distinct odd primes. E.T.Parker observed that the very long proof by W.Feit and J.Thompson [2] that every group of odd order is solvable would be shortened if it could be proved that $(p^q - 1)/(p - 1)$ never divides $(q^p - 1)/(q - 1)$(see Problem B25 of [3]). This is a very difficult problem. For the special case of $q = 3$, J.McKay has established that

$$p^2 + p + 1 \nmid 3^p - 1 \tag{1}$$

for $p < 53 \times 10^6$. But, in general, the problem is not solved as yet. In this paper we completely solve the case of $q = 3$ as follows.

Theorem For any odd prime p with $p \neq 3$, (1) holds.

The proof of our theorem depends on the following two lemmas.

Lemma 1 Let l be an odd prime with $l \equiv 1 (\bmod 3)$. Then the equation

$$x^2 + 3y^2 = 4l \ , \quad x, y \in \mathbf{N} \ , \gcd(x, y) = 1 \tag{2}$$

Received August 19, 2008.
2000 Mathematics Subject Classification: 11A05, 20D10
*Supported by the National Natural Science Foundation of China(10771186,10971184)

has exactly two solutions (x, y).

Proof Let m be a positive odd integer. By Theorem 12.4.1 and Exercise 12.4.4 of [4], the equation

$$x^2 + 3y^2 = 4m \ , \quad x, y \in \mathbf{N} \ \ , 2 \nmid xy \tag{3}$$

has exactly $E(m)$ solutions (x, y), where $E(m)$ is the difference between the numbers of divisors of m with the forms $3k+1$ and $3k+2$. If $m = l$, then $E(l) = 2$, the equations (2) and (3) have the same solutions . The lemma is proved.

Lemma 2 Let l be an odd prime with $l \equiv 1 (\mathrm{mod}\ 3)$. If 3 is a cubic residue modulo l, then $4l = a^2 + 243b^2$, where a and b are coprime positive integers.

Proof This is an early result of F.G.Eisenstein [1](see Theorem 9.3.1 and Exercise 9.23 of [5]).

Proof of Theorem. We assume that p is an odd prime satisfying $p \neq 3$ and

$$p^2 + p + 1 \mid 3^p - 1 \ . \tag{4}$$

Let $l = p^2 + p + 1$. Since $l < (p+1)^2$, if l is not a prime, then l has a prime divisor k with $3 < k < p$. But, since $3^{k-1} \equiv 1 (\mathrm{mod}\ k)$ and $3^p \equiv 1 (\mathrm{mod}\ k)$ by (4), we get $k - 1 \equiv 0 (\mathrm{mod}\ p)$ and $k > p$, a contradiction. Therefore, if (4) holds, then l must be a prime.

If $p \equiv 1 (\mathrm{mod}\ 3)$, then $3 \mid l$. But, since l is a prime with $l > 3$, it is impossible. So we have

$$p \equiv 2 \pmod 3 \tag{5}$$

and

$$l \equiv 1 \pmod 3 \ . \tag{6}$$

Let g denote a primitive root modulo l. By (4), we get

$$3^p \equiv 1 \pmod l \ . \tag{7}$$

Since $l - 1 = p(p+1)$, we see from (7) that

$$3 \equiv g^{(p+1)r} \pmod l \ , \quad r \in \mathbf{Z} \ . \tag{8}$$

Further, since $3 \mid p+1$ by (5), we find from (8) that 3 is a cubic residue modulo l. Therefore, by Lemma 2 with (6), then the equation (2) has a solution (x, y) satisfying

$$3^2 \mid y \ . \tag{9}$$

However, since $4l = (2p+1)^2 + 3 = (p+2)^2 + 3p^2$, by Lemma 1, (2) has only the solutions$(x, y) = (2p+1, 1)$ and $(p+2, p)$ which do not satisfy (9). Thus, (1) holds for any odd prime p with $p \neq 3$. The theorem is proved.

Acknowledgement. The author would like to thank the referees for their valuable suggestions.

References

[1] F.G.Eisenstein, Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wuzeln der Einheit zusammengesetzten complexen Zahlen, J.Reine Angew.Math.27(1844), 289-310.

[2] W.Feit and J.Thompson, Solvability of groups of odd order, Pacific J. Math.13(1963), 775-1029.

[3] R.K.Guy, Unsolved problems in number theory, Springer Verlag, New York, 1981.

[4] L.-K.Hua, Introduction to number theory, Springer Verlag, Berlin, 1982.

[5] K.lreland and M.Rosen, A classical introduction to modern number theory, Springer Verlag, New York, 1982.

Maohua Le
Department of Mathematics
Zhanjiang Normal College
Zhanjiang, Guangdong 524048
P.R.China
Email: lemaohua2008@163.com