ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

PROBLEMS AND SOME RESULTS CONCERNING THE DIOPHANTINE EQUATION $1 + A + A^2 + \cdots + A^{x-1} = P^y$.

HUGH EDGAR

Dedicated to the memory of E. G. Straus and R. A. Smith

We assume throughout the paper that a, x, p and y are positive integers, that $a > 1$ and that p is an odd prime. The primary purpose of the paper is to raise several as yet unsettled questions concerning the equation of the title and to try to induce people to solve these problems.

As a first, and perhaps not very important, example we notice that $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2$. In the time-honoured spirit of Erdös, we offer $25 for any other such example in which a is an odd prime and in which $y > 1$.

It has been known for quite some time (see, for instance, [1] that x must be prime, say $x = Q$, and that $Q = \mathrm{ord}_p a$. (Here $\mathrm{ord}_m a$ is defined to be the least t such that $a^t \equiv 1 \pmod{m}$.) We now specialize by assuming that "a" is from Southern California*, i.e., $a = r^b$, where r is an odd prime. In this case it is possible to prove that $b = Q^\lambda$ for some $\lambda \geqq 0$, as the following argument shows:

Suppose that there exists a prime $R \neq Q$ such that $R|b$ and write $b = RB$. Then

$$\begin{aligned} p^y &= \frac{a^x - 1}{a - 1} = \frac{(r^b)^Q - 1}{r^b - 1} = \frac{(r^{RB})^Q - 1}{r^{RB} - 1} = \frac{[(r^B)^Q]^R - 1^R}{(r^B)^R - 1^R} \\ &= \frac{((r^B)^Q - 1)}{(r^B - 1)} \cdot \frac{\{1 + (r^B)^Q + ((r^B)^Q)^2 + \cdots + ((r^B)^Q)^{R-1}\}}{\{1 + r^B + (r^B)^2 + \cdots + (r^B)^{R-1}\}} \\ &= \frac{(r^B)^Q - 1}{r^B - 1} \cdot \frac{\Phi_R((r^B)^Q)}{\Phi_R(r^B)} = \frac{(r^B)^Q - 1}{r^B - 1} \cdot \Phi_{QR}(r^B), \end{aligned}$$

where $\Phi_n(x)$ denotes the nth cyclotomic polynomial (see, for instance, [2]). Thus

Received by the editors on March 28, 1984.

* (This terminology has been adopted in honour of the research done on the title equation and related matters by Dennis Estes, Bob Guralnick, Murray Schacher and Ernst Straus. The current paper owes a lot to the work of these people.)

$$p^y = \frac{r^{BQ} - 1}{r^B - 1} \cdot \Phi_{QR}(r^B),$$

and since $(r^{BQ} - 1)/(r^B - 1) > 1$ it must be the case that $(r^{BQ} - 1)/(r^B - 1)$ is some positive integral power of p and thus $p|(r^{BQ} - 1)$. However Bang's Theorem [3] guarantees that $(r^{BQR} - 1) = a^x - 1$ has a primitive prime diversor, which is necessarily p, and hence p cannot divide $(r^{BQ} - 1)$ since $BQ < BQR$. This contradiction completes the argument. (This is a Southern California result, to the best of my knowledge. The proof given here is from Northern California.)

For convenience, we quote the following facts [1]:

(1) $y = u \operatorname{ord}_a p$ for some positive integer u

(2) $y = z$, where $p^z \| (a^{\operatorname{ord}_p a} - 1)$ (i.e., $p^z | (a^{\operatorname{ord}_p a} - 1)$ and $p^{z+1} \nmid (a^{\operatorname{ord}_p a} - 1)$).

We offer \$50 for the resolution of the conjecture that u is invariably equal to one.

In any case u cannot be "too big", for suppose that $u \geqq \operatorname{ord}_p a$. Then

$$a^{\operatorname{ord}_p a} - 1 = p^{u \operatorname{ord}_a p}(a - 1) \geqq p^{u \operatorname{ord}_a p}$$

which implies that

$$a^{\operatorname{ord}_p a} > (p^{\operatorname{ord}_a p})^{\operatorname{ord}_p a}$$

from which it follows that $a > p^{\operatorname{ord}_a p} \equiv 1 (\operatorname{mod} a)$ and finally $a > a + 1$, a contradiction. Thus $u \leqq (\operatorname{ord}_p a) - 1$.

Estes and Guralnick [4] have proved, on the assumption that "a" is from Southern California, that $Q \nmid y$. It is apparently not known whether the exponent λ in $b = Q^\lambda$ can be positive, i.e., on the assumption that the common ratio "a" of the geometric progression is a prime power it isn't known whether it must actually be prime. We offer \$50 for a resolution of this problem. If we assume that $\lambda = 0$ then we can easily deduce that $Q \nmid y$ via the following argument. Since $y = u \operatorname{ord}_a p$ and $u \leqq (\operatorname{ord}_p a) - 1$ and $Q = \operatorname{ord}_p a$, $Q \nmid u$. If

$$Q \mid \operatorname{ord}_a p = \operatorname{ord}_{rQ^\lambda}(p) = \operatorname{ord}_r p \mid \phi(r) = r - 1$$

then $r \equiv 1 \pmod{Q}$ so that $1 + r + r^2 + \cdots + r^{Q-1} \equiv 0 (\operatorname{mod} Q)$ whereas $p^y \not\equiv 0 \pmod{Q}$.

Guralnick [5] has done a considerable amount of research which proves that there is a strong connection between the equation of the title and the existence (or nonexistence) of arithmetically equivalent algebraic number fields (two algebraic number fields are said to be arithmetically equivalent if their Dedekind Zeta functions are equal).

Straus [6] has shown, via Baker's method, that for given p there are effective bounds on a, x and y for possible solutions of the title equation.

Finally it should be mentioned that the author's original interest in this subject came from Professor D. Suryanarayana [7], [8].

REFERENCES

1. H. Edgar, *On a Theorem of Suryanarayana*, Proc. Washington State Univ. Conf., Number Theory, Pullman (1971) 52–54.

2. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965, 207.

3. G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math. **5** (1904) 173–180.

4. Private communication.

5. R. Guralnick, *Subgroups Inducing the Same Permutation Representation*;———and David B. Wales, *Subgroups Inducing the Same Permotation Representation* II, to appear in Journal of Algebra.

6. Private Communication.

7. D. Suryanarayana, *Problems in theory of numbers* **17**.(**3**), Bull. Amer. Math. Soc. **76** (1970) 977.

8. D. Suryanarayana, *Certain Diophantine Equations*, Math. Student **35** (1967) 197–199.

9. T. Shorey and R. Tijdeman, *New applications of Diophantine approximations to Diophantine equations*, Math. Scand. **39** (1976) 5–18.

SAN JOSE STATE UNIVERSITY, WASHINGTON SQUARE, SAN JOSE, CA 95192–0103