QUESTIONS, DISCUSSIONS, AND NOTES

EDITED BY R. E. GILMAN, Brown University, Providence, Rhode Island

The department of Questions and Discussions in the Monthly is open to all forms of activity in collegiate mathematics, including the teaching of mathematics, except for specific problems, especially new problems, which are reserved for the department of Problems and Solutions.

ON THE VANISHING OF THE SUM OF THE NTH POWERS OF THE ROOTS OF A CUBIC EQUATION

By MORGAN WARD, California Institute of Technology

1. Suppose that

$$x^3 - Px^2 + Qx - R = 0, \tag{1.1}$$

P, Q, R rational integers, is a cubic equation with three distinct non-vanishing roots. Then it is a fundamental problem of considerable arithmetical interest to determine whether or not a given rational integer A may be represented as a sum of nth powers of the roots of (1.1), and—granted that such a representation is possible—to find out in how many ways it can occur.

More precisely, if α_1, α_2, α_3 are the roots of (1.1) and if $S_n = \alpha_1^n + \alpha_2^n + \alpha_3^n$ is the sum of their nth powers, we wish to solve the diophantine equation

$$S_x = A \tag{1.2}$$

in positive integers x, given P, Q, R and A.

The great difficulty of this general problem is at once apparent. For if we restrict the roots of (1.1) to be rational integers, then the special case $A = 0$ is the Fermat problem, and Fermat's conjecture is equivalent to asserting that the diophantine equation

$$S_x = 0 \tag{1.3}$$

can have only the solutions $x = 1$ and $x = 2$ if the roots of (1.1) are rational integers.

2. A simpler preliminary problem is to ascertain whether or not (1.2) and (1.3) can have an infinite number of solutions. In case all of the roots of (1.1) are real, the answer is apparent; *for any A, there are only a finite number of values of x satisfying* (1.2). For since the roots α are distinct, and $|\alpha_1\alpha_2\alpha_3| = |R| \geq 1$, the magnitude of the arithmetically largest root of (1.1) is greater than one, and since S_n is clearly of the same order as the nth power of this root, $|S_n|$ tends to infinity with n.[1]

In case two of the roots of (1.1) are complex, nothing general seems to be known as to the number of solutions of (1.2). However, in the special case when $R = \pm 1$, Siegel[2] has shown by the use of Thue's theorem that (1.3) *can have*

[1] A trivial exception occurs if we have $\alpha_1 = -\alpha_2 > |\alpha_3|$, as then $S_{2n+1} = \alpha_3^{2n+1}$. Hence if $\alpha_3 = \pm 1$, $S_x = \pm 1$ will have an infinite number of solutions.

[2] Tohôku Journal, Vol. 20 (1921), p. 29.

only a finite number of solutions unless (1.1) *is of the form* $(x\pm 1)(x^2+1)$ *or* $(x\pm 1)(x^2\pm x+1)$.[1]

3. We can set ourselves the still more modest task of finding values of x for which (1.2) and (1.3) are insoluble—a common enough type of procedure in other problems in diophantine analysis.

For example, let p be a prime number, and r a positive integer. Then

$$S_{p^{r-1}} \equiv S_{p^{r-1}}^{p} \equiv (\alpha_1^{p^{r-1}} + \alpha_2^{p^{r-1}} + \alpha_3^{p^{r-1}})^p = \alpha_1^{p^r} + \alpha_2^{p^r} + \alpha_3^{p^r} \pmod{p}.$$

Since $S_1 = P$, we see that[2]

$$S_{p^r} \equiv P \pmod{p}, \qquad (r = 0, 1, 2, \cdots).$$

Accordingly, if (1.2) has a solution for x a power of a prime p, we have the restriction $A \equiv P \pmod{p}$. In particular, (1.3) can have a solution in such a case only if $P \equiv 0 \pmod{p}$. Therefore if $P \not\equiv 0$, for a given cubic equation (1.1), *S_x can vanish for only a finite number of values of x which are primes or powers of primes.*

If $P = 0$, we obtain a restriction on the value of A in (1.2), but no restriction upon x in (1.3). In this case, I shall conclude by proving the following theorem, the main point of novelty in the paper.

4. THEOREM. *Let α_1, α_2, α_3 be the roots of an irreducible cubic equation*

$$x^3 + Qx - R = 0, \tag{4.1}$$

Q, R rational integers. Then if R is greater in absolute value than two, and prime to Q, the sum of the nth powers of the roots of (4.1), *$S_n = \alpha_1^n + \alpha_2^n + \alpha_3^n$, can never vanish if n is even, or if n is a prime.*

PROOF. By hypothesis, α_1, α_2 and α_3 are distinct and not zero, and

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \qquad \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = Q, \qquad \alpha_1\alpha_2\alpha_3 = R, \tag{4.2}$$

$$|R| \geqq 3, \qquad (R, Q) = 1. \tag{4.3}$$

Consider first the case when (1) has only one real root. Denote it by α_1. Then we may write

$$\alpha_2 = re^{i\theta}, \qquad \alpha_3 = re^{-i\theta}, \qquad r > 0, \qquad 0 < \theta < 2\pi. \tag{4.4}$$

By (4.2), $\alpha_1 = -re^{i\theta} - re^{-i\theta} = -2r\cos\theta$. Therefore

$$\begin{aligned} S_n &= \alpha_1^n + \alpha_2^n + \alpha_3^n = (-2r\cos\theta)^n + (re^{i\theta})^n + (re^{-i\theta})^n \\ &= 2r^n\{\cos n\theta + (-1)^n 2^{n-1}(\cos\theta)^n\}. \end{aligned}$$

[1] We may if we please regard $S_0, S_1, S_2, \cdots, S_n, \cdots$ as a sequence (S) giving that particular solution of the difference equation $\Omega_{n+3} = P\Omega_{n+2} - Q\Omega_{n+1} + R\Omega_n$ with the initial values $S_0 = 3$, $S_1 = P$, $S_2 = P^2 - 2Q$, and ask more generally about the solutions of the diophantine equations $U_x = A$, $U_x = 0$ for any particular rational integral solution $U_0, U_1, U_2, \cdots, U_n, \cdots$ of the difference equation. Siegel in the paper referred to studies the U_n as coefficients in the infinite series $\sum_{n=0}^{\infty} U_n t^n$. The two theorems just stated for carry over to the general sequence (U).

[2] Lucas, *Theorie des Nombres*, p. 422.

Hence $S_n=0$ when and only when

$$\cos n\theta + (-1)^n 2^{n-1}(\cos\theta)^n = 0.$$

Now by a familiar formula of elementary trigonometry,

$$\cos n\theta = (\cos\theta)^n\left\{1 - \binom{n}{2}\tan^2\theta + \binom{n}{4}\tan^4\theta - \binom{n}{6}\tan^6\theta + \cdots\right\},$$

the last term in the bracket being

$$(-1)^{(n/2)}\tan^n\theta \quad \text{or} \quad (-1)^{(n-1)/2}\binom{n}{n-1}\tan^{n-1}\theta$$

according as n is even or odd. Hence S_n vanishes when and only when $z=\tan^2\theta$ is a root of the algebraic equation

$$(4.5)\qquad F(z) = 1 + (-1)^n 2^{n-1} - \binom{n}{2}z + \binom{n}{4}z^2 - \binom{n}{6}z^3 + \cdots = 0.$$

From (4.4) we see that $i\tan\theta=(\alpha_2-\alpha_3)/(\alpha_2+\alpha_3)$, or

$$(4.6)\qquad \tan^2\theta = -\left(\frac{\alpha_2-\alpha_3}{\alpha_2+\alpha_3}\right)^2.$$

Next, assume that (1) has three real roots. Then two of them must be of the same sign. Denote the remaining root by α_1. If in the pair α_2, α_3, the root of greatest magnitude is α_2, we may write

$$(4.41)\qquad \alpha_2 = \pm re^{\theta}, \qquad \alpha_3 = \pm re^{-\theta}, \qquad r>0, \qquad \theta>0$$

where the upper sign is taken if α_2 and α_3 are both positive, and the lower sign if α_2 and α_3 are both negative. As in the first case, $\alpha_1=-2r\cosh\theta$ and proceeding exactly as before, we find that S_n vanishes when and only when $z=-\tanh^2\theta$ is a root of the algebraic equation (4.5), where

$$(4.61)\qquad \tanh^2\theta = \left(\frac{\alpha_2-\alpha_3}{\alpha_2+\alpha_3}\right)^2.$$

Now if n is even $=2k$, the leading coefficient of (4.5) becomes unity on multiplying through by $(-1)^k$, and the remaining coefficients are obviously rational integers. If n is an odd prime p, the leading coefficient of $F(z)$ is $(-1)^{(p-1)/2}p$ and the integers

$$\binom{p}{2}, \binom{p}{4}, \binom{p}{6}, \cdots$$

are all divisible by p. Furthermore the constant term $1-2^{p-1}$ of $F(z)$ is divisible by p by Fermat's theorem. Therefore on dividing $F(z)$ by $(-1)^{(p-1)/2}p$, we obtain again an equation with leading coefficient unity and rational integral coefficients. But any root of such an equation is an algebraic integer. Hence

referring to (4.6) and (4.61), we can state the result: *If S_n vanishes for n even or n an odd prime, it is necessary that $\zeta = -(\alpha_2-\alpha_3)/(\alpha_2+\alpha_3)$ be an algebraic integer.*

5. We finally show that the quantity ζ cannot be an algebraic integer by proving that the irreducible canonical equation with leading coefficient unity which it satisfies has non-integral coefficients.

First, since $(\alpha_2-\alpha_3)^2=(\alpha_2+\alpha_3)^2-4\alpha_2\alpha_3$ we obtain from (4.2) (iii) and (i) $\zeta=1-4R/\alpha_1^3$. Thus ζ is a root of the cubic equation

$$\Phi(z) = \left(z - 1 + \frac{4R}{\alpha_1^3}\right)\left(z - 1 + \frac{4R}{\alpha_2^3}\right)\left(z - 1 + \frac{4R}{\alpha_3^3}\right) = 0.$$

On multiplying out the right side of this expression and simplifying by the use of the relations (4.2) and (4.1), we obtain

$$\Phi(z) = z^3 + \left(9 + \frac{4Q^3}{R^2}\right)z^2 + \left(27 - \frac{8Q^3}{R^2}\right)z + 27 + \frac{4Q^3}{R^2} = 0.$$

This equation has rational integral coefficients when and only when $4Q^3\equiv 0 \pmod{R^2}$ and hence never if $|R|>2$, and $(R, Q)=1$. It only remains to show that it is irreducible. If it were reducible, it would have at least one rational root, so that for $1\leqq i\leqq 3$, we would have $1-4R/\alpha_i^3$ rational, $\alpha_i^3=R-Q\alpha_i$ rational, or α_i rational, contradicting the assumed irreducibility of (4.1).

Note added in proof. Our analysis shows also that if $S_n=0$, n cannot be prime to R. For both $n\zeta^2$ and $R^4\zeta^2$ are algebraic integers.

On the General Equation of the Parabola

H. W. Bailey, University of Illinois

Consider the general equation of the second degree

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0.$$

While it is apparent that the various elements used in sketching this curve: directrices, foci, semi-axes, etc., are functions of the constants $A, \cdots, F$, yet the explicit expression in terms of these constants is so complicated algebraically as to be worthless practically. For example, the eccentricity appears as a root of the quartic equation

$$Je^4 - (I^2 + 4J)e^2 + (I^2 + 4J) = 0,$$

where $I=A+C$, $J=B^2-AC$. However, in the case of the parabola such expression is possible in very simple form. The purpose of this note is to give these explicit formulas when we take the equation of the parabola in the form

$$A^2x^2 + 2ACxy + C^2y^2 + 2Dx + 2Ey + F = 0.$$

Let the equation of the directrix and the coordinates of the focus be $\alpha x-\beta y-\gamma=0$ and (m, n) respectively. Using the general definition of a conic, the equation of this parabola may also be written