ON THE CONGRUENCE $ax^3 + by^3 + cz^3 + dxyz \equiv n \pmod{p}$

By L. J. Mordell

Let p be a prime and let $f(x, y, z)$ be an irreducible cubic polynomial with integer coefficients which is neither a function of only two independent variables nor homogeneous in linear functions of x, y, z. Then there is the *Conjecture.*

The number N of solutions of the congruence

$$f(x, y, z) \equiv 0 \pmod{p} \tag{1}$$

satisfies

$$N = p^2 + O(p), \tag{2}$$

where the implied constant is an absolute one.

I have proved this in the special cases

$$z^2 \equiv f(x, y) \tag{3}$$

when [1], [2] [3]

$$f(x, y) \equiv ax^3 + bx^2y + cxy^2 + dy^3 + k,$$

$$f(x, y) \equiv ax^3 + bx^2y + cxy^2 + dy^3 + lx + my,$$

$$f(x, y) \equiv ax^3 + by^3 + cxy + d.$$

Surprisingly enough, in the last case, there is a simple closed expression for N. The general case (3) still awaits solution.

The case

$$ax^3 + by^3 + cz^3 \equiv n, \qquad abcn \not\equiv 0,$$

has been known for a long time. I now prove that the congruence

$$ax^3 + by^3 + cz^3 + dxyz \equiv n, \qquad abcd \not\equiv 0, \tag{4}$$

has $N = p^2 + O(p)$ solutions if $n \not\equiv 0$, and $N = p^2 + O(p^{3/2})$ solutions if $n \equiv 0$.

Suppose first that $n \equiv 0$. Clearly $N = p^2 + O(p^{3/2})$ since the number of solutions of $aX^3 + bY^3 + c + dXY \equiv 0$ is $p + O(p^{1/2})$. Suppose hereafter that $n \not\equiv 0$. The result (2) is trivially true when $p \equiv 2 \pmod{3}$. For if $z \equiv 0$, (4) has $O(p)$ solutions. When $z \not\equiv 0$, we put $x = Xz$, $y = Yz$, and then

$$z^3(aX^3 + bY^3 + c + dXY) \equiv n.$$

These are $O(p)$ values of X, Y for which the coefficient of z^3 is $\equiv 0$. Excluding these, each of the p^2 values of X, Y gives a unique value for z.

Received October 1, 1962. This research was supported by the Air Force Office of Scientific Research.