TOKYO J. MATH.
VOL. 11, NO. 1, 1988

The Diophantine Equation $x^2 \pm ly^2 = z^l$ Connected with Fermat's Last Theorem

Norio ADACHI

Waseda University

Dedicated to late Professor M. Kinoshita

Introduction.

Let l be an odd prime number and put $l^* = (-1)^{(l-1)/2} l$. Fermat's Last Theorem was proved by Euler for the exponent $l=3$ ([3]) and by Dirichlet for the exponent $l=5$ ([1]). Their proofs, which will be reproduced in §2 in modern terms (cf. Edwards [2]), are based on the fact that the implication

$$a^2 - l^* b^2 = l\text{-th power} \quad \Rightarrow \quad \exists u,\ v;\ a + b\sqrt{l^*} = (u + v\sqrt{l^*})^l$$

is justified for $l=3$ or $l=5$ under some subsidiary conditions. It is often said that their success is due to the unique factorization property in the maximal order of the quadratic field $\boldsymbol{Q}(\sqrt{l^*})$ for $l=3$ or $l=5$, respectively. But, this point of view is not exact, as will be seen in §1; for the above implication is true virtually for any prime l (Theorem 1, Theorem 2). The examples in §2 will show that the difficulty lies in finding the step of "infinite descent", not in the failure of the unique factorization.

§1. The Diophantine equation $x^2 - l^* y^2 = z^l$.

Let l be an odd prime number fixed throughout the present paper and put $l^* = (-1)^{(l-1)/2} l$. We use roman small letters such as $a, b, u, v, \cdots$ to designate rational integers. We say that a and b have the property (P), if they are relatively prime, of opposite parity, and $a^2 - l^* b^2$ is an l-th power of a rational integer.

We consider here whether the following implication $(*)$ is justified:

$$(*) \qquad (\mathrm{P}) \quad \Rightarrow \quad \exists u,\ v;\ a + b\sqrt{l^*} = (u + v\sqrt{l^*})^l$$

Received March 12, 1987