178. Über die Fermatsche Vermutung.

By Taro MORISHIMA.
Shizuoka Kotogakko.

(Rec. Nov. 1, 1928. Comm. by T. TAKAGI, M.I.A., Dec. 2, 1928.)

Der bekannte *Satz*: «*Es sei*

$$x^p+y^p+z^p=0, \quad (x, y, z)=1, \quad p\nmid xyz, \quad p>5, \tag{1}$$

dann ist

$$5^{p-1}\equiv 1 \pmod{p^2},$$»

lässt sich sehr einfach beweisen, wenn noch die Voraussetzung

$$2^{p-1}\not\equiv 1 \pmod{p^4}. \tag{2}$$

hinzugenommen wird.

Vorbereitung zum Beweise:

I. Es sei

$$x^p+y^p+z^p=0, \quad (x, y, z)=1, \quad r\mid x, \quad p\nmid x, \quad p>3.$$

Dann ist (nach Furtwängler)

$$r^{p-1}\equiv 1 \pmod{p^2}.$$

II. Es sei

$$x^p+y^p+z^p=0, \quad (x, y, z)=1, \quad r\mid x-y, \quad p\nmid x^2-y^2, \quad p>3.$$

Dann ist (nach Furtwängler)

$$r^{p-1}\equiv 1 \pmod{p^2}.$$

III. Es sei

$$x^p+y^p+z^p=0, \quad (x, y, z)=1, \quad p>3.$$

Dann ist (nach Vandiver)

$$x^p\equiv x, \quad y^p\equiv y, \quad z^p\equiv z \pmod{p^3}.$$

Hilfssatz 1: Es sei

$$x^p+y^p+z^p=0, \quad (x, y, z)=1, \quad p>3,$$
$$x\equiv y \pmod{p}.$$

Dann ist

$$x\equiv y \pmod{p^3}.$$

Beweis: Nach Voraussetzung ist

$$x\equiv y \pmod{p},$$
$$\therefore \quad x^p\equiv y^p \pmod{p^2},$$

also nach III

$$x \equiv x^p \equiv y^p \equiv y \pmod{p^2},$$
$$\therefore \quad x^p \equiv y^p \pmod{p^3},$$

also nach III

$$x \equiv x^p \equiv y^p \equiv y \pmod{p^3}.$$

Hilfssatz 2: Es sei

$$x^p+y^p+z^p=0, \quad (x, y, z)=1, \quad p \nmid xyz, \quad p>3,$$
$$2^{p-1} \not\equiv 1 \pmod{p^4}.$$

Dann ist

$$x \not\equiv y, \quad y \not\equiv z, \quad z \not\equiv x \pmod{p}.$$

Beweis: Aus Symmetriegründen sei ohne Beschränkung der Allgemeinheit

$$x \equiv y \pmod{p}.$$

Dann wäre nach Hilfssatz 1

$$x \equiv y \pmod{p^3},$$
$$\therefore \quad x^p \equiv y^p \pmod{p^4}.$$

Wegen $x^p+y^p+z^p=0$, wäre also

$$2x^p \equiv -z^p \pmod{p^4},$$
$$2^{p-1}x^{p(p-1)} \equiv z^{p(p-1)} \pmod{p^4}.$$

Nach III wäre also

$$2^{p-1} \equiv 1 \pmod{p^4}$$

gegen (2).

Beweis des Satzes: Nach Voraussetzung

$$x^p+y^p+z^p=0, \quad (x, y, z)=1, \quad p \nmid xyz, \quad p>5,$$
$$2^{p-1} \not\equiv 1 \pmod{p^4}.$$

Wir unterscheiden zwei Fälle.

1) Es sei

$$5 \mid xyz.$$

Ohne Beschränkung der Allgemeinheit sei alsdann

$$5 \mid x.$$

Dann ist nach I mit $r=5$

$$5^{p-1} \equiv 1 \pmod{p^2}.$$

2) Es sei

$$5 \nmid xyz .$$

Dann ist

$$x, y, z \equiv \pm 1 \quad \text{oder} \quad \pm 2 \qquad (\text{mod } 5).$$

2, 1) Es sei

$$x \equiv \pm 1, \quad y \equiv \pm 1, \quad z \equiv \pm 1 \qquad (\text{mod } 5)$$

oder

$$x \equiv \pm 2, \quad y \equiv \pm 2, \quad z \equiv \pm 2 \qquad (\text{mod } 5).$$

Dann ist

$$0 \equiv x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \qquad (\text{mod } 5)$$

oder

$$0 \equiv x^p + y^p + z^p \equiv \pm 2^p \pm 2^p \pm 2^p \qquad (\text{mod } 5).$$

Das geht nicht, da $5 \nmid \pm 1$, $5 \nmid \pm 3$, $5 \nmid \pm 2^p$.

2, 2) Ohne Beschränkung der Allgemeinheit sei

$$x \equiv \pm 1, \quad y \equiv \pm 1, \quad z \equiv \pm 2 \qquad (\text{mod } 5)$$

oder

$$x \equiv \pm 2, \quad y \equiv \pm 2, \quad z \equiv \pm 1 \qquad (\text{mod } 5).$$

Dann ist

$$x \equiv y \equiv \pm 1 \quad \text{oder} \quad \pm 2 \qquad (\text{mod } 5),$$

denn sonst wäre, wegen $x \equiv -y \pmod 5$,

$$0 \equiv x^p + y^p + z^p \equiv \pm 2^p \quad \text{oder} \quad \pm 1 \qquad (\text{mod } 5).$$

Nach Hilfssatz 2 ist

$$p \nmid x - y.$$

Wegen $p \nmid z$ ist

$$p \nmid x + y ,$$

also

$$p \nmid x^2 - y^2 .$$

Ausserdem ist

$$5 \mid x - y .$$

Nach II mit $r = 5$ ist also

$$5^{p-1} \equiv 1 \qquad (\text{mod } p^2).$$