

(d) *Hurwitz's coincidence formula.* Thanks to a theorem proved elsewhere<sup>7</sup> it is a direct corollary of (4) in the case  $n = 2$ .<sup>8</sup>

In conclusion let us state that most results obtained along this line by Brouwer and his school follow from (3) and (4).

<sup>1</sup> These PROCEEDINGS, 9, p. 99 (1923).

<sup>2</sup> In the present volume of these PROCEEDINGS.

<sup>3</sup> See my Borel Series Monograph: *L'Analyse Situs et la géométrie algébrique*, p. 15 (1924).

<sup>4</sup> *Trans. Amer. Math. Soc.*, 25 (1923)540.

<sup>5</sup> *Trans. Amer. Math. Soc.*, 25 (1923)173.

<sup>6</sup> *Trans. Amer. Math. Soc.*, 18 (1917)287.

<sup>7</sup> *Monograph*, p. 19.

<sup>8</sup> The product manifold was indeed used for the first time in the same manner as here in connection with algebraic correspondences by Severi in his well-known paper of the *Torino Memorie* of 1903.

## LAWS OF RECIPROCITY AND THE FIRST CASE OF FERMAT'S LAST THEOREM

BY H. S. VANDIVER

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS

Communicated April 15, 1925

Suppose that

$$x^p + y^p + z^p = 0 \quad (1)$$

is satisfied in rational integers  $x$ ,  $y$  and  $z$ , none zero and each prime to the odd prime  $p$ . Then

$$(x + \alpha y) (x + \alpha^2 y) \dots (x + \alpha^{p-1} y) = u^p$$

where  $\alpha = e^{2i\pi/p}$ , and  $u$  is a rational integer. It follows from the unique decomposition of an ideal into its prime ideal factors that the ideal  $(x + \alpha^a y)$  is the  $p^{\text{th}}$  power of an ideal in the field  $\Omega(\alpha)$ ,  $a \not\equiv 0 \pmod{p}$ . If  $\omega$  is an integer in  $\Omega(\alpha)$ ,  $\mathfrak{q}$  an ideal prime in  $\Omega(\alpha)$  which is prime to  $(\omega)$  and  $(p)$  then we set

$$\omega \frac{N(\mathfrak{q})-1}{p} \equiv \left\{ \frac{\omega}{\mathfrak{q}} \right\} \pmod{\mathfrak{q}},$$

where  $N(\mathfrak{q})$  is the norm of  $\mathfrak{q}$  and  $\{\omega/\mathfrak{q}\}$  is some power of  $\alpha$ . It follows that  $\omega$  is congruent to a  $p^{\text{th}}$  power in  $\Omega$ , modulo  $\mathfrak{q}$ , if and only if,

$$\left\{ \frac{\omega}{\mathfrak{q}} \right\} = 1.$$

Also if  $Q = q_1 q_2 \dots q_s$ , where the  $q$ 's are prime ideals prime to  $(\omega)$  and  $(p)$ , then

$$\left\{ \frac{\omega}{Q} \right\} = \left\{ \frac{\omega}{q_1} \right\} \left\{ \frac{\omega}{q_2} \right\} \dots \left\{ \frac{\omega}{q_s} \right\}.$$

Consequently since  $(x + \alpha^a y)$  is the  $p^{\text{th}}$  power of an ideal in  $\Omega(\alpha)$  then

$$\left\{ \omega / (x + \alpha^a y) \right\} = 1.$$

Hilbert<sup>1</sup> defined the norm residue symbol

$$\left\{ \frac{\nu, \mu}{p} \right\} = \alpha^L \tag{2}$$

where

$$L \equiv \sum_{s=1}^{p-1} (-1)^{s-1} l^{(s)}(\nu) l^{(p-s)}(\mu) \pmod{p},$$

$$l^{(g)}(\omega) = \left[ \frac{d^g \log(\omega(e^x))}{dx^g} \right]_{x=0}$$

$g = 1, 2, \dots, p-1$ ;  $p = (1-\alpha)$ ;  $\nu \equiv 1 \pmod{p}$ ,  $\mu \equiv 1 \pmod{p}$ ;  $\nu$  and  $\mu$  integers in the field  $\Omega(\alpha)$ ,  $\alpha = e^{2\pi i/p}$ .

The symbol  $\omega(x)$  is defined follows: If

$$\omega = c_0 + c_1 \alpha + \dots + c_{p-2} \alpha^{p-2},$$

then

$$\omega(x) = \sum_{r=0}^{p-2} c_r x^r - \frac{\sum_{r=0}^{p-2} c_r - 1}{p} \cdot \frac{x^p - 1}{x - 1}. \tag{3}$$

If  $\nu$  and  $\mu$  are any integers in the field prime to  $p$  then

$$\left\{ \frac{\nu, \mu}{p} \right\} = \left\{ \frac{\nu, \mu^{p-1}}{p} \right\}. \tag{4}$$

Now if  $(\gamma)$  is a principal ideal and the  $p^{\text{th}}$  power of any ideal in  $\Omega(\alpha)$  then  $(\gamma)$ ,  $(x + \alpha^a y)$  being prime to each other and to  $p$ ,

$$\left\{ \frac{\gamma}{x + \alpha^a y} \right\} = 1 = \left\{ \frac{x + \alpha^a y}{\gamma} \right\}. \tag{5}$$

Furtwängler<sup>2</sup> gave a law of reciprocity between two integers in a field containing  $\Omega(\alpha)$ , which for the special case where the field is  $\Omega(\alpha)$  itself becomes

$$\left\{ \frac{\omega}{\theta} \right\} \left\{ \frac{\theta}{\omega} \right\}^{-1} = \left\{ \frac{\theta, \omega}{p} \right\}, \tag{6}$$

$\omega$  and  $\theta$  being any two integers in  $\Omega(\alpha)$  such that  $(\omega)$  and  $(\theta)$  are prime to each other and to  $p$ . Setting  $\omega = \gamma^{p-1}$  and  $\theta = (x + \alpha^g y)^{p-1}$  then (4), (5) and (6) give

$$\left\{ \frac{x + \alpha^g y, \gamma}{p} \right\} = 1$$

or

$$L \equiv 0 \pmod{p}, \tag{7}$$

for

$$\gamma = \theta, \mu = \omega.$$

Let

$$\omega = \gamma^{p-1} = \sum_{r=0}^{p-2} c_r \alpha^r, (x + \alpha^g y)^{p-1} = \sum_{r=0}^{p-2} d_r \alpha^r = \theta.$$

Then (Hilbert,<sup>1</sup> p. 413)

$$l^{(g)}(\omega) \equiv \left[ \frac{d^g \log \sum_{r=0}^{p-2} c_r e^{vr}}{dv^g} \right]_{v=0} \pmod{p},$$

$g = 1, 2, \dots, p-2$ , and similar relations for  $\theta$ . Also if we set  $\gamma(e^v)$  for the function obtained when  $\alpha$  is replaced by  $e^v$  in  $\gamma$  then evidently

$$\left[ \frac{d^g \log \sum_{r=0}^{p-2} c_r e^{vr}}{dv^g} \right]_{v=0} \equiv - \left[ \frac{d^g \log \gamma(e^v)}{dv^g} \right]_{v=0} \pmod{p}, \tag{8}$$

$$\begin{aligned} \left[ \frac{d^g \log \sum_{r=0}^{p-2} d_r e^{vr}}{dv^g} \right]_{v=0} &\equiv - \left[ \frac{d^g \log (x + e^{gv} y)}{dv^g} \right]_{v=0} \pmod{p}, \\ &\equiv - a^g \left[ \frac{d^g \log (x + e^v y)}{dv^g} \right]_{v=0} \pmod{p}. \end{aligned} \tag{9}$$

Now also

$$\left[ \frac{d^{p-1} \log \gamma^{p-1}(e^v)}{dv^{p-1}} \right]_{v=0} \equiv l^{(p-1)}(\omega) + \frac{1 - \gamma^{p-1}(1)}{p}, \tag{10}$$

modulo  $p$ . We also have

$$N(\gamma^{p-1}) = b^{p(p-1)}$$

where  $b$  is an integer, since  $(\gamma)$  is the  $p^{\text{th}}$  power of an ideal in  $\Omega(\alpha)$ . Hence if  $u$  is an indeterminate

$$[\gamma(u)\gamma(u^2) \dots \gamma(u^{p-1})]^{p-1} = b^{p(p-1)} + k \frac{u^p - 1}{u - 1} + V(u)(u^p - 1), \tag{11}$$

where  $k$  is a rational integer, and  $V(u)$  is a polynomial in  $u$  with rational integral coefficients. Set  $u = 1$ , then

$$(\gamma(1))^{(p-1)^2} \equiv 1 + kp \pmod{p^2}$$

since  $b^{p(p-1)} \equiv 1 \pmod{p^2}$ , whence

$$\frac{(\gamma(1))^{(p-1)^2} - 1}{p} \equiv k \pmod{p}.$$

Now in (11) set also  $u = e^v$ , take logarithms and differentiate  $(p-1)$  times with respect to  $v$ , then

$$\begin{aligned} & (1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1}) \left[ \frac{d^{p-1} (\log \gamma (e^v)^{p-1})}{dv^{p-1}} \right]_{v=0} \\ & \equiv k(1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1}) \pmod{p}, \end{aligned}$$

or

$$\left[ \frac{d^{p-1} (\log \gamma (e^v)^{p-1})}{dv^{p-1}} \right]_{v=0} \equiv \frac{(\gamma(1))^{(p-1)^2} - 1}{p} \pmod{p}. \tag{12}$$

Now if

$$(\gamma(1))^{p-1} = 1 + rp$$

then

$$(\gamma(1))^{(p-1)^2} \equiv 1 + r(p-1)p \pmod{p^2}$$

and

$$\frac{\gamma(1)^{(p-1)^2} - 1}{p} \equiv - \frac{(\gamma(1))^{p-1} - 1}{p} \pmod{p},$$

and from (10) with (12),

$$l^{(p-1)}(\omega) \equiv 0 \pmod{p}. \tag{13}$$

We may prove in a similar manner that

$$l^{p-1}(\theta) \equiv 0 \pmod{p}. \tag{14}$$

Hence (7) gives

$$\sum_{s=2}^{p-2} (-1)^{s-1} l^{(s)}(\omega) l^{(p-s)}(\theta) \equiv 0 \pmod{p},$$

or from (8) and (9)

$$\sum_{s=2}^{p-2} (-1)^{s-1} a^s \left[ \frac{d^s \log(x + e^v y)}{dv^s} \right]_{v=0} \left[ \frac{d^{p-s} \log \gamma(e^v)}{dv^{p-s}} \right]_{v=0} \equiv 0 \pmod{p}.$$

Set  $a = 1, 2, 3, \dots, p-2$  in turn, we obtain  $(p-2)$  congruences, and since the determinant

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 2 & 2^2 & 2^3 & \dots & 2^{p-2} \\ \dots & \dots & \dots & \dots & \dots \\ (p-2) & (p-2)^2 & (p-2)^3 & \dots & (p-2)^{p-2} \end{vmatrix} = \pi_{i,j} (i-j) (p-2)!$$

$i, j = 1, 2, \dots, p-2,$   
 $i > j$

is not divisible by  $p$ , then we have

$$\left[ \frac{d^s \log(x + e^y)}{dv^s} \right]_{v=0} - \left[ \frac{d^{p-s} \log \gamma(e^y)}{dv^{p-s}} \right]_{v=0} \equiv 0 \pmod{p},$$

$s = 2, 3, \dots, p-2$ . But we also have (Vandiver<sup>3</sup>), if we set  $-x/y = t$ ,

$$f_s(t) \left[ \frac{d^{p-s} \log \gamma(e^y)}{dv^{p-s}} \right]_{v=0} \equiv 0 \pmod{p}, \tag{15}$$

$s = 2, 3, \dots, p-2; f_s(t) = \sum_{i=1}^{p-1} i^{s-1} t^i$ . We may then state the

**THEOREM.** *If (1) is satisfied in rational integers  $x, y, z$ , none zero and all prime to the odd prime  $p$  then*

$$f_{p-n}(t) \left[ \frac{d^n \log \gamma(e^y)}{dv^n} \right]_{v=0} \equiv 0 \pmod{p},$$

$n = 2, 3, \dots, p-2; -t = x/y$ . Here  $\gamma(\alpha)$  is an integer in the field  $\Omega(\alpha)$  and the principal ideal  $(\gamma(\alpha))$  is the  $p^{\text{th}}$  power of any ideal in  $\Omega(\alpha)$  which is prime to  $(z)$  and  $(p)$ .

If there exists two solutions of (1) say

$$\begin{aligned} x^p + y^p + z^p &= 0 \\ x_1^p + y_1^p + z_1^p &= 0 \end{aligned}$$

with  $xyz \not\equiv 0 \pmod{p}, x_1 y_1 z_1 \not\equiv 0 \pmod{p}$ , where  $z$  is prime to  $z_1$ , then in the above theorem we may take  $\gamma(\alpha) = x + \alpha y$  and we obtain

**COROLLARY I.** *If there exists in addition to the solution  $(x, y, z)$  of (1) ( $xyz$  prime to  $p$ ) another solution  $(x_1, y_1, z_1)$   $z_1$  prime to  $z$  and  $x_1 y_1 z_1 \not\equiv 0 \pmod{p}$ , then*

$$f_{p-n}(t) f_n(t_1) \equiv 0 \pmod{p}$$

$t_1 = -x_1/y_1, n = 2, 3, \dots, p-2$ .

If we take  $\gamma(\alpha) = z + \alpha y$ , which is prime to  $(x + \alpha y)$  and to  $(p)$ , then we have

**COROLLARY II.** *If (1) is satisfied for  $xyz \not\equiv 0 \pmod{p}$*

then

$$f_{p-n}(t) f_n(1-t) \equiv 0 \pmod{p}$$

$n = 2, 3, \dots, p-2$ .

Put  $x + \alpha^{p-1}y = \gamma(\alpha)$ , this is prime to  $x + \alpha^a y$ ,  $0 < a < p-1$ , so that we obtain

COROLLARY III. *If (1) is satisfied for  $xyz \not\equiv 0 \pmod{p}$ , then*

$$f_n(t) f_{p-n}(t) \equiv 0 \pmod{p}, \tag{16}$$

$n = 2, 3, \dots, p-2$ .

Cf. Mirimanoff.<sup>4</sup>

We have

$$\left[ \frac{d^2 \log(x + e^y)}{dv^2} \right]_{v=0} = \frac{xy}{(x+y)^2}$$

Hence the theorem gives

$$\left[ \frac{d^{p-2} \log \lambda(e^v)}{dv^{p-2}} \right]_{v=0} \equiv 0 \pmod{p}$$

for all ideals  $(\lambda(\alpha))$  which are  $p^{\text{th}}$  powers of ideals in the field prime to  $(z)$  and  $(p)$ . Using  $x + \alpha z$  in lieu of  $x + \alpha y$  we obtain the same result for ideals which are not prime to  $(z)$ . We deal in a similar manner with the case  $n = 3$  in the theorem, and find results which are included in the following:

COROLLARY IV. *If (1) is satisfied in integers prime to the odd prime  $p$  then*

$$\left[ \frac{d^{p-a} \log \lambda(e^v)}{dv^{p-a}} \right]_{v=0} \equiv 0 \pmod{p},$$

$a = 2$  or  $3$ , and  $(\lambda(\alpha))$  is the  $p^{\text{th}}$  power of any ideal in the field  $\Omega(\alpha)$  which is prime to  $p$ .

Note that the latter criteria are independent of  $x, y$  and  $z$ . From (1) we have also

$$f_{p-1}(t) \equiv 0 \pmod{p} \tag{17}$$

for  $t = -x/y$ . This well known criterion may be deduced by elementary means. Mirimanoff deduced from the Kummer criteria

$$B_a f_{p-2a}(t) \equiv 0 \pmod{p}$$

$a = 1, 2, \dots, p-3/2$ , and where  $B_1 = 1/6, B_2 = 1/30, \dots$ , etc., are the numbers of Bernoulli, the criteria (16) using also (17). Conversely we may obtain from his relations a new derivation of the Kummer criteria by the use of (16) and (17).

The Theorem and first three corollaries of this paper were previously stated without proof by the writer.<sup>5</sup>

All the results given here have been known to the writer since 1917, but he was enabled to put the article in final form through a grant, relieving him of the duties of teaching, from the Heckscher Foundation for the Advancement of Research, established by August Heckscher at Cornell University.

<sup>1</sup> Bericht über die Theorie der algebraischen Zahlkörper, *Jahresbericht D.M.V.*, 1894, 413.

<sup>2</sup> *Math. Ann.*, 72, 1909, 386.

<sup>3</sup> *Ann. Math.*, 21, 1919, 76.

<sup>4</sup> *J. Mathematik, Crelle*, 128, 1905, 45-68.

<sup>5</sup> *Amer. Math. Soc. Bull.*, 28, 1922, 259-60.

---

## A SPECIES OF MUSA IN THE TERTIARY OF SOUTH AMERICA

BY EDWARD W. BERRY

JOHNS HOPKINS UNIVERSITY

Read before the Academy April 27, 1925

The original home of the banana (*Musa*) has always been a disputed problem, most authors inclining to the belief that it was in the southeastern Asiatic region, since there are so many cultivated varieties as well as wild forms in that region at the present time, and since the equivalent word occurs in Sanscrit, Arabic, etc.

More particularly, botanists have, almost without exception, disputed that the genus *Musa* was indigenous in the Western Hemisphere, or was cultivated here prior to its introduction into Hispaniola from the Canary Islands in 1516, as related by Oviedo in 1556.

Alexander von Humboldt was the first to question this belief and to maintain that the banana was probably a native of America in pre-Spanish times, and in recent years O. F. Cook has argued that it was an aboriginal American crop-plant, originally cultivated as a root crop, the valuable pulpy fruits normally seedless being a result of hybridization, since the so-called wild seed-bearing species have non-edible fruits more or less similar to the capsular fruits of all the other genera of the family.

I have received the fossil seeds of a species of *Musa* from Dr. Maurice A. Rollet, who collected them from the coal measures of the Cerros de Guadalupe and Montserrat, which form a part of the eastern upland border of the Sabana of Bogota in Colombia. The altitude is about 9000 feet and the geological horizon is probably Oligocene, although there is some doubt as to its precise age.