ON THE FACTORIZATION OF INTEGRAL FUNCTIONS WITH p-ADIC COEFFICIENTS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, September 6, 1910.)

1. IF $F(x)$ is an integral function of degree n with integral p-adic coefficients, then for any integer k we have a congruence

$$(1) \qquad F(x) \equiv F^{(k)}(x) = F_0(x) + pF_1(x) + p^2F_2(x) + \cdots + p^kF_k(x) \qquad (\text{mod } p^{k+1}),$$

in which each $F_i(x)$ is an integral function of degree $\leqq n$ with coefficients belonging to the set $0, 1, \cdots, p-1$. The function $F^{(k)}(x)$ is called the convergent of rank k of $F(x)$. If

$$(2) \qquad F(x) = f(x) \cdot g(x) \qquad (p),$$

in which the factors are integral functions with integral p-adic coefficients, then for any integer k we obviously have

$$(3) \qquad F^{(k)}(x) \equiv f^{(k)}(x) \cdot g^{(k)}(x) \qquad (\text{mod } p^{k+1}).$$

The following converse theorem plays a fundamental rôle in Hensel's new theory of algebraic numbers:* *If*

$$(4) \qquad F(x) \equiv f_0(x) \cdot g_0(x) \qquad (\text{mod } p^{s+1})$$

for † $s + 1 > 2\rho$, *where* ρ *is the order of the resultant* R *of* $f_0(x)$ *and* $g_0(x)$, *then* $F(x)$ *is the product* (2) *of two integral functions with integral p-adic coefficients whose convergents of rank* $s - \rho$ *are* $f_0(x)$ *and* $g_0(x)$.

Hensel's proof is in effect a process to construct the successive convergents of $f(x)$ and $g(x)$. Each step of the process requires the solution of a linear equation in two unknowns with p-adic coefficients. The object of this note is to furnish a decidedly simpler process, which dispenses with these linear

* Hensel, Theorie der algebraischen Zahlen, Leipzig, Teubner, 1908, p. 71.

† This condition is satisfied if $s = \delta$, where δ is the order of the discriminant of $F(x)$. Hence we obtain as a corollary the theorem of Hensel, page 68.

equations, and requires only the solution of a single linear congruence.

By the remark of Hensel, bottom of page 64, we may assume that the leading coefficients in $F(x)$, $f_0(x)$, and $g_0(x)$ are powers of p, so that $F-f_0g_0$ is of degree less than n.

2. For the sake of simplicity, we first establish the theorem for the important case $s=\rho=0$: *If* $F(x)=F_0(x)+pF_1(x)+\cdots$, *in which the coefficient of* x^n *in* F_0 *is unity and* $F_i(i>0)$ *is of degree less than* n, *and if*

$$F_0(x) \equiv f_0(x)\cdot g_0(x) \pmod{p}, \tag{5}$$

in which f_0 *and* g_0 *are integral functions of degrees* μ *and* ν *respectively, with integral coefficients, while* f_0 *and* g_0 *have no common factor modulo* p, *then integral functions* $f_i(x)$ *of degrees* $<\mu$ *and* $g_i(x)$ *of degrees* $<\nu$ *with integral coefficients can be so determined that*

$$f=f_0+pf_1+p^2f_2+\cdots,\quad g=g_0+pg_1+p^2g_2+\cdots.$$

have as their product $F(x)$. It is meant by the last statement that congruence (3) holds for every integer k.

Since f_0 and g_0 have no common factor, integral functions $a(x)$ and $b(x)$ with integral coefficients can be determined (for example, by Euclid's process) such that

$$af_0+bg_0\equiv 1 \pmod{p}. \tag{6}$$

By (5), $F_0-f_0g_0$ is the product of p by an integral function with integral coefficients which may be designated $L_1(x)-F_1(x)$,

$$F_0-f_0g_0=p(L_1-F_1). \tag{7}$$

By the remark at the end of § 1, L_1 like F_1 is of degree less than n. The congruence

$$F_0+pF_1\equiv(f_0+pf_1)(g_0+pg_1) \pmod{p^2}$$

is equivalent, in view of (7), to

$$L_1\equiv f_0g_1+g_0f_1 \pmod{p}. \tag{8}$$

In view of (6), every set of solutions is given by

$$f_1\equiv bL_1-\rho_1f_0,\quad g_1\equiv aL_1+\rho_1g_0. \tag{9}$$

We choose $\rho_1(x)$ so that the degree of f_1 shall be less than the degree μ of f_0. Then the final term of (8) is of degree $<\mu+\nu$, so that the degree of g_1 is $< \nu$. Hence the required functions f_1 and g_1 are given by (9).

To make the general step by induction, suppose that, for $i=1, \cdots, k$, functions f_i of degrees $< \mu$ and g_i of degrees $< \nu$ have been determined so that (3) holds. Hence we may set

$$F^{(k)} = f^{(k)}g^{(k)} + p^{k+1}(L_{k+1} - F_{k+1}), \tag{10}$$

where L_{k+1} is of degree less than n. Since

$$\begin{gathered} F^{(k+1)} = F^{(k)} + p^{k+1}F_{k+1}, \quad f^{(k+1)} = f^{(k)} + p^{k+1}f_{k+1}, \\ g^{(k+1)} = g^{(k)} + p^{k+1}g_{k+1}, \end{gathered} \tag{11}$$

the condition for the congruence

$$F^{(k+1)} \equiv f^{(k+1)}g^{(k+1)} \pmod{p^{k+2}}$$

becomes, upon applying (10),

$$L_{k+1} \equiv f^{(k)}g_{k+1} + g^{(k)}f_{k+1} \equiv f_0 g_{k+1} + g_0 f_{k+1} \pmod{p}.$$

The general set of solutions is

$$f_{k+1} \equiv bL_{k+1} - \rho_{k+1}f_0, \quad g_{k+1} \equiv aL_{k+1} + \rho_{k+1}g_0.$$

We determine ρ_{k+1} so that the degree of f_{k+1} shall be less than the degree μ of f_0; then the degree of g_{k+1} will be less than the degree ν of g_0. Since the induction is complete, our theorem is proved.

3. We readily deduce recursion formulas for the functions L_i. We have proved that functions L_i and ρ_i can be determined so that

$$f_i = bL_i - \rho_i f_0, \quad g_i = aL_i + \rho_i g_0 \qquad (i \geqq 1) \tag{12}$$

give functions f_i of degrees $< \mu$ and g_i of degrees $< \nu$ for which congruence (3) holds for every k. From (6),

$$af_0 + bg_0 = 1 + p\lambda(x). \tag{13}$$

In (10) we replace $F^{(k)}, f^{(k)}, g^{(k)}$ by the values obtained by replacing k by $k-1$ in (11) and then replace $F^{(k-1)}$ by the value obtained by replacing k by $k-1$ in (10). After deleting the factor p^k, we get

$$L_k = f_k g^{(k-1)} + g_k f^{(k-1)} + p^k f_k g_k + pL_{k+1} - pF_{k+1}.$$

In the terms $f_k g_0 + g_k f_0$ we replace f_k and g_k by their values

(12) and apply (13). After deleting the factor p we get

(14) $L_{k+1} = F_{k+1} - \lambda L_k - f_k[g]_{k-1} - g_k[f]_{k-1} - p^{k-1}f_k g_k,$

in which we have employed the abbreviation

(15) $[z]_i = z_1 + pz_2 + p^2 z_3 + \cdots + p^{i-1}z_i, \quad [z]_0 = 0.$

If in (10) we set

$$F^{(k)} = F_0 + p[F]_k, \quad f^{(k)} = f_0 + p[f]_k, \quad g^{(k)} = g_0 + p[g]_k,$$
$$\gamma = (F_0 - f_0 g_0)/p,$$

and then delete the factor p, we get

$$f_0[g]_k + g_0[f]_k + p^k L_{k+1} = \gamma + [F]_k + p^k F_{k+1} - p[f]_k[g]_k.$$

By (12), (15), the sum of the first two terms equals

$$\sum_{i=1}^{k} p^{i-1}(af_0 + bg_0)L_i = (1 + p\lambda)\sum_{i=1}^{k} p^{i-1}L_i = (1 + p\lambda)[L]_k.$$

Hence we obtain the formula

(16) $[L]_{k+1} = \gamma + [F]_{k+1} - p\lambda[L]_k - p[f]_k[g]_k.$

It is also easy to establish this formula by induction.

4. To prove the more general theorem of § 1, we apply the method of § 2 with congruence (6) replaced by

(17) $$af_0 + bg_0 \equiv p^\rho \pmod{p^{s+1}}.$$

Since the resultant of $f_0(x)$ and $g_0(x)$ is divisible by p^ρ, but by no higher power of p, solutions $a(x)$ and $b(x)$ of (17) can be determined by the method given by Hensel on pages 62, 63. In view of (4),

$$F^{(s+1)} - f_0 g_0 = p^{s+1}L_1,$$

where L_1 is of degree less than n. Then the congruence

(18) $$F^{(s+1)} \equiv (f_0 + pf_1)(g_0 + pg_1) \pmod{p^{s+2}}$$

is satisfied if we take

$$f_1 \equiv p^{s-\rho}(bL_1 - \rho_1 f_0), \quad g_1 \equiv p^{s-\rho}(aL_1 + \rho_1 g_0) \pmod{p^{s+1}},$$

since by (17)

(20) $$f_0 g_1 + f_1 g_0 \equiv p^s L_1 \pmod{p^{s+1}},$$

and $p^2 f_1 g_1$ is divisible by p^t, where $t = 2 + 2s - 2\rho > s + 1$. We choose $\rho_1(x)$ so that the degree of $f_1(x)$ shall be less than the degree of $f_0(x)$; then by (20) the degree of $g_1(x)$ will be less than the degree of $g_0(x)$.

Similarly, if in accord with (18) we set

$$F^{(s+1)} - (f_0 + pf_1)(g_0 + pg_1) = p^{s+2}(L_2 - F_{s+2}),$$

the congruence

$$F^{(s+2)} \equiv (f_0 + pf_1 + p^2 f_2)(g_0 + pg_1 + p^2 g_2) \pmod{p^{s+3}}$$

is satisfied if we take

$$f_2 \equiv p^{s-\rho}(bL_2 - \rho_2 f_0), \quad g_2 \equiv p^{s-\rho}(aL_2 + \rho_2 g_0) \pmod{p^{s+1}}.$$

The general step in the proof may now be made as in § 2.

HENSEL'S THEORY OF ALGEBRAIC NUMBERS.

Theorie der Algebraischen Zahlen. Von KURT HENSEL. Erster Band. Leipzig and Berlin, Teubner, 1908. xi + 346 pp.

IN the theory of functions one may investigate an analytic function in the neighborhood of a point $z = a$ by means of a power series in $z - a$. In arithmetic one usually employs only developments according to the fixed base 10. The author undertakes in the present work to introduce a corresponding mobility into arithmetic and algebra by employing expansions of numbers into power series in an arbitrary prime number p.

A positive integer D can be expressed in one and but one way in the form

$$D = d_0 + d_1 p + \cdots + d_k p^k,$$

in which each d_i is one of the integers $0, 1, \cdots, p - 1$. This equation will be said to define the representation of D as a p-adic number, for which the following symbol will be employed:

$$D = d_0,\ d_1 d_2 \cdots d_k \quad (p).$$

For example,

$$14 = 2 + 3 + 3^2 = 2{,}11 \quad (3), \qquad 216 = 2 \cdot 3^3 + 2 \cdot 3^4 = 0{,}0022 \quad (3).$$

The sum of two such p-adic numbers is readily expressed as a p-adic number. For example,

$$0{,}0022 + 0{,}1021 = 0{,}10111 \quad (3).$$