ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 1, Winter 1985

KUMMER CONGRUENCES IN FORMAL GROUPS AND ALGEBRAIC GROUPS OF DIMENSION ONE

C. Snyder

0. Introduction. Kummer congruences for the Bernoulli numbers and the coefficients in the expansion of the secant function were discovered by E.E. Kummer around 1850. Subsequently much work has been done to show similar types of congruences for the coefficients of various generating functions.

L. Carlitz was the first to treat Kummer congruences for "Hurwitz series" systematically. We briefly outline the history and definitions here.

Let k be an algebraic number field, i.e., a finite degree extension of $\mathbf{Q}$, the field of rational integers. Let R be an integral domain in k containing $\mathbf{Z}$, the ring of rational integers. (Normally R will be 0_k, the ring of integers of k, or perhaps a subring of $0_k[1/h]$ for some nonzero rational integer h. The important point here is that almost all rational primes are not units so that congruences mod pR are not trivial except for finitely many primes.)

We define a Hurwitz series over R as a power series $f(t)$ of the form

$$f(t) = \sum_{n=0}^{\infty} a_n \frac{t^n}{n!} \text{ where } a_n \in R.$$

If $a_0 = 0$ and $a_1 = 1$, then $f(t)$ has an inverse $\lambda(t)$, i.e., $f(\lambda(t)) = t = \lambda(f(t))$, of the form $\lambda(t) = \sum_{n=0}^{\infty} e_n t^n/n!$ where $e_0 = 0$, $e_1 = 1$, and $e_n \in R$ for all $n \geqq 0$. We consider only those $f(t)$ with $a_0 = 0$, $a_1 = 1$ satisfying the Hypothesis: For all $n \geqq 1$, $(n-1)!|e_n$, i.e., the inverse $\lambda(t) = \sum_{n=1}^{\infty} \varepsilon_n t^n/n$ where $\varepsilon_n \in R$.

This hypothesis is equivalent to the "integrality condition" that the formal derivative

$$f'(t) = \sum_{\nu=0}^{\infty} d_\nu f^\nu \text{ with } d_\nu \in R.$$

(The d_ν are a priori in k.) In particular if there exists a nonzero polynomial $P(X, Y) \in k[X, Y]$ such that $P(f, f') = 0$, then f satisfies the hypothesis for an appropriate choice of R, cf. e.g., [7].

Received by the editors on January 24, 1983, and in revised form on November 1, 1983.
Partially supported by a University of Maine Summer Faculty Research Grant.

Suppose $f(t)$ is a Hurwitz series satisfying the above hypothesis. Then we say $f(t)$ has Kummer congruences at p, a rational prime, if and only if

$$\sum_{i=0}^{r}(-1)^{r-i}\binom{r}{i}\varepsilon_p^{r-i}a_{m+i(p-1)} \equiv 0 \bmod p^r$$

for all positive integers r and all $m \geqq$ r. (The congruences are to be interpreted ideal theoretically in R.)

We now ask, which Hurwitz series $f(t)$ have Kummer congruences at all primes p? Carlitz showed that if $f(t)$ and $f'(t)$ are related as $f' = 1 + a_1f + a_2f^2$, $a_j \in k$ or $(f')^2 = 1 + b_1f + b_2f^2 + b_3f^3 + b_4f^4$, $b_j \in k$ then f has Kummer congruences at all primes p. To show this Carlitz defined an operator Ω_p by $\Omega_pf = f^{(p)}(t) - \varepsilon_pf'(t)$. (Here $f^{(p)}(t)$ means the pth derivative of f with respect to t.) It is easy to see that $\Omega_p f = \sum_{\nu=0}^{\infty}\eta_\nu f^\nu$ where $\eta_\nu \in R$. If, in addition, $\eta_\nu \equiv 0 \bmod p$ for all $\nu \geqq 0$, Carlitz showed $f(t)$ has Kummer congruences at p.

We now give four examples of Hurwitz series $f(t)$ satisfying Carlitz's conditions above and thus having Kummer congruences at all primes p.

Example 1. Let $f(t) = t$. Then $\lambda(t) = t$. Notice $f'(t) = 1$. In this case Kummer congruences are completely trivial as $\sum_{i=0}^{r}(-1)^{r-i}\binom{r}{i}\varepsilon_p^{r-i}\, a_{m+i(p-i)} = 0$.

Example 2. Let $f(t) = e^t - 1 = \sum_{n=1}^{\infty} 1 \times t^n/n!$. Then $\lambda(t) = \ln(1 + t) = \sum_{n=1}^{\infty}(-1)^{n-1}\, t^n/n$. Notice $f'(t) = 1 + f$. Again Kummer congruences are trivial since $\sum_{i=0}^{r}(-1)^{r-i}\binom{r}{i}\varepsilon_p^{r-i}\, a_{m+1(p-1)} = 0$.

Example 3. Let $f(t) = \tan\, t = \sum_{n=1}^{\infty}(-1)^{(n-1)/2}\, 2^{n+1}(2^{n+1} - 1)(B_{n+1}/n+1)(t^{n-1}/n!)$. Then $\lambda(t) = \arctan\, t = \sum_{n=1}^{\infty}(-1)^{n-1}t^{2n-1}/(2n - 1)$. Notice that $f' = 1 + f^2$. Thus f has Kummer congruences at all primes p. This time the congruences are nontrivial.

Example 4. Let $f(t) = sn(t) = \sum_{n=1}^{\infty} a_nt^n/n!$ where $sn(t)$ is the Jacobi elliptic function associated with the curve $y^2 = 1 + x^4$. Then $(f')^2 = 1 + f^4$ and $\lambda(t) = \int_0^t du/\sqrt{1 + u^4}$. Kummer congruences for $sn(t)$ were studied by Carlitz in [2].

In [8], we established negative results about Kummer congruences. Suppose $f(t)$ and $f'(t)$ are related as $(f')^2 = 1 + df^m$ where $m \geqq 5$, $d \in k - \{0\}$. If $m = 6$, f has Kummer congruences at all primes p. However for all other $m \geqq 5$, there exist infinitely many primes p at which Kummer congruences fail. The reason for the exceptional case $m = 6$ is explained in [9].

An argument similar to the one given in [8] shows that if $f' = 1 + df^m$ where $m \geqq 3$, $d \in k - \{0\}$, then f does not have Kummer congruences at infinitely many primes.

These results followed from a closer analysis of the Ω_p operator. In [8], we showed that f has Kummer congruences at p if and only if $\Omega_p f = \sum_{\nu=0}^{\infty} \eta_\nu f^\nu$ where $\eta_\nu \equiv 0 \bmod p$ for $\nu < p^2$. This is much weaker than Carlitz's condition on Ω_p. We say that f has strong Kummer congruences at p if and only if $\Omega_p f = \sum_{\nu=0}^{\infty} \eta_\nu f^\nu$ where $\eta_\nu \equiv 0 \bmod p$ for all $\nu \geqq 0$.

In all the cases of Hurwitz series considered above, the problem of the existence of Kummer congruences at all primes is answered on rather technical grounds. It seems natural to ask if there is a more transparent reason for the existence of Kummer congruences. An indication of an answer to this question appears in the four examples above. Each of those Hurwitz series satisfies an algebraic law of addition. As we shall see (in more generality) this implies Kummer congruences.

In general, if $f(t)$ is a Hurwitz series over R (satisfying the above hypothesis, as always), then it is easy to see that there exists a unique power series $F_f(X, Y) \in k[[X, Y]]$ such that $f(s + t) = F_f(f(s), f(t))$. Moreover $F_f(X, Y)$ is a formal group.

We now define this concept and related concepts. Let A be a commutative ring with 1. By a formal group over A we mean a power series $F(X, Y) \in A[[X, Y]]$ in two variables satisfying:

1. $F(X, Y) = X + Y +$ "higher degree terms";
2. $F(F(X, Y), Z) = F(X, F(Y, Z))$;
3. $F(X, Y) = F(Y, X)$

For example, let $G_a(X, Y) = X + Y$ and $G_m(X, Y) = X + Y + XY$. $G_a(X, Y)$ and $G_m(X, Y)$ are called the additive and multiplicative formal groups, respectively.

Next we define the logarithm of a formal group. Let $F(X, Y)$ be a formal group defined over a field K of characteristic 0. It can easily be shown that there exists a unique power series $L(X) \in K[[X]]$ such that

1. $L(X) = X +$ "higher degree terms in X";
2. $L(F(X, Y)) = L(X) + L(Y)$.

$L(X)$ is called the logarithm of $F(X, Y)$. We furthermore define the canonical invariant differential, ω, of the formal group $F(X, Y)$ as $\omega = L'(X)dX$. (For more details see [5].)

The connection between the theory of Hurwitz series $f(t)$ and the theory of formal groups is as follows: $F_f(X, Y)$ is a formal group defined over k. The series $\lambda(t)$ is the logarithm of $F_f(X, Y)$ as can be seen by applying λ to both sides of the equation $F_f(f(s), f(t)) = f(s + t)$. Hence the hypothesis we imposed on $\lambda(t)$ is equivalent to the assumption that the canoncial invariant differential ω of $F_f(X, Y)$ be defined over R, i.e., $\lambda'(t) \in R[[t]]$. Conversely if $F(X, Y)$ is a formal group defined over k with canonical invariant differential $\omega = L'(X)dX$ defined over R, then the inverse of the logarithm can be shown to be a Hurwitz series over R satisfying the hypothesis above.

Notice that for the first three examples given above, the corresponding formal groups are $G_a(X, Y)$, $G_m(X, Y)$, and $F_f(X, Y) = (X + Y)/(1 - XY) = (X + Y) \sum_{\nu=0}^{\infty}(XY)^2$. The formal group for $sn(t)$ is too complicated to bother to compute.

Our first result exhibits a relationship between strong Kummer congruences and congruences among the coefficients ε_ν in the expansion of the canonical invariant differential ω of the corresponding formal group.

THEOREM 1. *$f(t)$ has strong Kummer congruences at p if and only if*

$$\varepsilon_{p\nu} \equiv \varepsilon_p \varepsilon_\nu^p \bmod pR \text{ for all } \nu \geqq 1.$$

Our second result shows that certain integrality conditions on the coefficients of $F_f(X, Y)$ imply that $f(t)$ has strong Kummer congruences, which in turn implies that the canonical invariant differential has coefficients in its expansion satisfying the congruences in Theorem 1.

THEOREM 2. *Suppose $F(X, Y)$ is defined over $R_{(p)}$, the localization of R with respect to $\mathbf{Z} - (p)$. Then $f(t)$ has strong Kummer congruences at p. Hence the coefficients in the expansion of ω must satisfy the congruences*

$$\varepsilon_{p\nu} \equiv \varepsilon_p \varepsilon_\nu^p \bmod pR \text{ for all } \nu \geqq 1.$$

This theorem provides a partial generalization of the congruences of Atkin and Swinnerton-Dyer. They showed in particular the congruences as in our theorem when ω is a differential of the first kind on an elliptic curve defined over $\mathbf{Z}$. See [3] for more details.

It is also interesting to notice that our proof of Theorem 2 is elementary. Proofs of similar types of congruences usually seem to be more arithmetic in nature.

We then give two major applications of these results to algebraic groups of dimension one and related algebraic curves. For the relevant definitions, see §2. below.

THEOREM 3. *Let C be a connected algebraic group of dimension one defined over an algebraic number field k, with an invariant differential ω. Then for any k-rational point a on C and any rational function f on C regular at the point a, f has Kummer congruences with respect to ω at a.*

We generalize Theorem 3 to include certain curves which are not necessarily algebraic groups.

THEOREM 4. *Let C be an irreducible algebraic curve defined over an algebraic number field k and let ω denote a differential on C. Suppose there exists a k-rational mapping, ϕ, from C onto a dense subset of a connected algebraic group C' of dimension one defined over k, with an invariant differential ω' such that $\phi^*\omega' = \omega$. Then for all k-rational simple points a on C in the domain of ϕ at which ϕ is unramified and for any rational* *function f on C regular at the point a. f has Kummer congruences with respect to ω at a.*

In other words, Theorem 4 states that if the function field of C contains a subfield which is the function field of an algebraic group for which the differential ω is the unique extension of an invariant differential of the group, then any function on C regular at an unramified simple point has Kummer congruences with respect to ω at that point.

Other applications are given throughout this article which we shall not state here.

I would like to express my gratitude to my colleague, Henrik Bresinsky, for his time and patience in explaining to me many aspects of algebraic geometry. I would also like to thank the referee for many valuable suggestions.

1. Kummer congruences in formal groups. For the concepts and notation in this section we refer to the Introduction.

Theorem 1. *$f(t)$ has strong Kummer congruences at p if and only if*

$$\varepsilon_{p\nu} \equiv \varepsilon_p \varepsilon_\nu^p \bmod pR \text{ for all } \nu \geqq 1.$$

Proof. The proof will be established by obtaining a string of equivalent formulations to $D_t^p f \equiv \varepsilon_p D_t f \bmod pR[[f]]$. Here $D_t f$ means f'. First notice that $\varepsilon_p D_t f = \varepsilon_p f'$. On the other hand, $D_t^p f = (f'D_f)^p f = (f'D_f)^{p-1} f' = f'D_f((f'D_f)^{p-2} f')$. By Theorem 2 in [8], $(f'D_t)^{p-2} f' \equiv D_f^{p-2} f^{p-1} \bmod pR[[f]]$ and thus $(f'D_f)^{p-1} f' \equiv -(f')D_f^{p-1}(f')^{p-1}$. ($J-P$. Serre pointed out to me that the last congruence has already occurred in Dieudonne's work on formal Lie groups; see Lemma 3 in [4]). From this congruence and the fact that f' is a unit mod $pR[[x]]$, we conclude that $D_t^p f \equiv \varepsilon_p D_t f$ is equivalent to $D_f^{p-1}(f')'^{p-1} \equiv -\varepsilon_p$. Next notice that $D_f^{p-1}((f')^{-1}) = D_f^{p-1}((f')^{p-1}(f')^{-p}) \equiv (f')^{-p} D_f^{p-1}(f')^{p-1}$, whence $D_t^p f \equiv \varepsilon_p D_t f$ if and only if $D_f^{p-1}((f')^{-1}) \equiv -\varepsilon'(f')^{-p}$. This latter congruence is equivalent to $\sum_{\nu=0}^{\infty}(\nu+(p-1))\cdots(\nu+1)\varepsilon_{\nu+p} f^\nu = -\varepsilon_p \sum_{\nu=0}^{\infty} \varepsilon_{\nu+1}^p f^{p\nu}$. From this congruence and Wilson's theorem, the theorem follows easily.

Theorem 2. *Suppose $F_f(X, Y)$ is defined over $R_{(p)}$. Then $f(t)$ has strong Kummer congruences at p. Hence the coefficients in the expansion of the canonical invariant differential ω must satisfy the congruences*

$$\varepsilon_{p\nu} \equiv \varepsilon_p \varepsilon_\nu^p \bmod pR \text{ for all } \nu \geqq 1.$$

Proof. Assume $F(X, Y)$ has coefficients in $R_{(p)}$. Since $f(s+t) = F(f(s), f(t))$, we have $f'(s+t) = \partial f/\partial s(s+t) = \partial F/\partial X\,(f(s), f(t))\, df/ds$. We claim that

$$\frac{\partial^p f}{\partial s^p}(s+t) \equiv \frac{\partial^p F}{\partial X^p}(f(s), f(t))\left(\frac{df}{ds}\right)^p + \frac{\partial F}{\partial X}(f(s), f(t))\frac{d^p f}{ds^p} \bmod pR_{(p)}[[f(s), f(t)]].$$

This follows at once from the following two observations about partial derivatives, the first of which can be proved by induction (on m). Let $G = G(u, v)$, $u = u(s, t)$, and $v = v(s, t)$, then

$$\frac{\partial^m G}{\partial s^m} = \sum \frac{m!}{i_1!j_1!\cdots(mi_m)!(mj_m)!} \cdot \frac{\partial^{i_1+j_1+\cdots i_m+j_m}G}{\partial^{i_1+\cdots+i_m}u\,\partial^{j_1+\cdots+j_m}v}\left(\frac{\partial u}{\partial s}\right)^{i_1}\cdots$$

$$\left(\frac{\partial^m u}{\partial s^m}\right)^{i_m}\left(\frac{\partial v}{\partial s}\right)^{j_1}\cdots\left(\frac{\partial^m v}{\partial s^m}\right)^{j_m} c_{ij}$$

where the sum runs over nonnegative integers $i_1, \ldots, i_m, j_1, \ldots, j_m$ satisfying the equation $(i_1 + j_1) + \cdots + m(i_m + j_m) = m$ and $c_{ij} = \pi_{y=1}^{m} F_v(i_y)F_v(j_v)$, where $F_n(k) = \pi_{l=1}^{k}\binom{ln-1}{n-1}$. If $m = p$, a prime, then we have

$$\frac{\partial^p G}{\partial s^p} = \frac{\partial^p G}{\partial u^p}\left(\frac{\partial u}{\partial s}\right)^p + \frac{\partial G}{\partial u}\left(\frac{\partial^p u}{\partial s^p}\right) + \frac{\partial^p G}{\partial v^p}\left(\frac{\partial v}{\partial s}\right)^p + \frac{\partial G}{\partial v}\left(\frac{\partial^p v}{\partial s^p}\right)$$

+ terms with coefficients divisible by p.

Now in the established claim set $s = 0$. Since

$$\frac{\partial^p f}{\partial s^p}(s + t)\bigg|_{s=0} = D_t^p f,\ \frac{df}{ds}\bigg|_{s=0} = f'(0) = 1,\ \frac{d^p f}{ds^p} = \sum_{n=0}^{\infty} a_{n+p}\frac{s^n}{n!}$$

so

$$\frac{d^p f}{ds^p}\bigg|_{s=0} = a_p \equiv \varepsilon_p, \text{ and since } \frac{\partial^p F}{\partial X^p}(0, f(t)) \equiv 0 \bmod pR_{(p)}[[f]]$$

by hypothesis, we conclude that $D_t^p f \equiv \varepsilon_p D_t f \bmod pR_{(p)}[[f]]$. Since $pR_{(p)} \cap R = pR$, the theorem is established.

Let us now apply this theorem to obtain a negative result concerning a generalization of Theorem 4 in [5] on Dirichlet L-series.

Proposition. *Let $L(s, \chi)$ be a Dirichlet series where χ is a numerical character such that $\chi(n) \notin \mathbf{Q}$ for some integer n. Let $\mathbf{Q}(\chi) = \mathbf{Q}(\{\chi(n): n \in \mathbf{Z}\})$ whence $\mathbf{Q}(\chi) = \mathbf{Q}(\zeta_d)$ for some primitive d-th root of unity. Let $F(X, Y)$ be the formal group defined over $\mathbf{Q}(\chi)$ corresponding to $\omega = \sum_{n=1}^{\infty}\chi(n)x^{n+1}dx$ (cf.* [5], *p.* 209).*Then for all primes $p \not\equiv 1 \bmod d$ and not dividing the modulus of χ, $F(X, Y)$ is not defined over $0_{(p)}$ where 0 is the ring of integers of $\mathbf{Q}(\chi)$.*

Proof. Suppose $F(X, Y)$ were defined over $0_{(p)}$ where p does not divide the modulus of χ whence $\chi(p) \neq 0$. By Theorem 2, $\chi(pn) \equiv \chi(p)\chi(n)^p \bmod P$ for P a prime ideal of 0 over p. On the other hand, $\chi(pn) = \chi(p)\chi(n)$ for all $n \in \mathbf{Z}$ since χ is completely multiplicative. Hence since $\chi(p) \not\equiv 0 \bmod P$ we must have $\chi(n) = \chi(n)^p \bmod P$. But since $\{\chi(n): n \in \mathbf{Z}\}$ generates 0 over $\mathbf{Z}$ we have $[0/P: F_p] = 1$. Therefore $p \equiv 1 \bmod d$, as desired.

2. Applications to algebraic groups of dimension one and related algebraic curves. We now investigate the existence of Kummer congruences associated with a differential on certain algebraic curves. To this end, we shall use the following definitions and notation.

To simplify things we shall make the assumption that our curves are plane curves. This does not cause any loss of generality as our definitions and results below may be interpreted in the function field of the curve (which is the function field of some plane curve).

Let C be an irreducible algebraic plane curve (affine or projective) defined over an algebraic number field k. We note by $k(C)$ the field of rational functions on C. Moreover, if a is a k-rational simple point, then we denote by 0_a the (discrete) valuation ring at a, i.e., the ring of functions in $k(C)$ which are regular at a; we also denote by P_a the place at a, i.e., the functions in 0_a which vanish at a. The completion of $k(C)$ with respect to the P_a-adic topology will be denoted by $k(C)_{P_a}$. By a local uniformizing parameter in the completion we shall mean an element of $k(C)_{P_a}$ which generates the completion of P_a in $k(C)_{P_a}$.

Next suppose that ϕ is a k-rational mapping from C_1 to a dense subset of C_2 where C_i $(i = 1, 2)$ are irreducible algebraic curves over k. Then ϕ^* will denote the corresponding comapping from $k(C_2)$ into $k(C_1)$. Suppose, now, that a is a k-rational simple point on C_1 such that $\phi(a)$ is a simple point on C_2. We say ϕ is unramified at a if P_a is unramified over $\phi^* P_{\phi(a)}$.

Now we introduce the notion of Kummer congruences. Let C be an irreducible algebraic curve defined over an algebraic number field k. Let ω be a nonzero differential on C. Suppose a is a k-rational simple point on C at which the differential is regular and does not vanish. We say that a rational function f on C regular at a has Kummer congruences with respect to ω at a if and only if the following is satisfied: if $f = \sum_{n=0}^{\infty} a_n t^n/n!$ where t is a local uniformizing parameter at a in the completion $k(C)_{P_a}$ such that $\omega = dt$ near a, i.e., $\omega = dx/y$ implies $dx/dt = y$, and if $\omega = \sum_{\nu=1}^{\infty} \varepsilon_\nu z^{\nu-1}\, dz$ where $\varepsilon_1 = 1$ and z is a local unformizing parameter (in $k(C)$) at some place, then

$$\sum_{i=0}^{r} (-1)^{r-i}\binom{r}{i} \varepsilon_p^{r-i}\, a_{m+i(p-1)} \equiv 0 \bmod p^r$$

for all primes p, all $r \geqq 1$, and all $m \geqq r$. The congruences are interpreted as follows: All the individual elements in the congruences lie in some ring $R = 0_k[1/h]$ where h is a positive integer and 0_k is the ring of integers of k. (For Proposition 3 in [7] shows that $\{\varepsilon_\nu : \nu \geqq 1\}$ is contained in a finitely generated **Z**-subalgebra of k. Also $\omega = dz/w = \sum_{\nu=1}^{\infty} \tilde{\varepsilon}_\nu z^{\nu-1}$ where $\tilde{\varepsilon}_1 = 1$, and z is a local unformizing parameter in $k(C)$ at a. Hence $\{\tilde{\varepsilon}_\nu : \nu \geqq 1\}$ is contained in a finitely generated **Z**-subalgebra of k. If $z = \sum_{n=1}^{\infty} \tilde{a}_n t^n/n!$ $(\tilde{a}_1 = 1)$, then it is not hard to see that $\{\tilde{a}_n : n \geqq 1\}$ is generated over **Z** by $\{\tilde{\varepsilon}_\nu : \nu \geqq 1\}$. Now $f = \sum_{\nu=0}^{\infty} c_\nu z^\nu$ where $\{c_\nu : \nu \geqq 0\}$ is contained in a finitely generated $\mathbf{Z}$-subalgebra of k. Finally, $\{a_n: n \geqq 0\}$ lies in the $\mathbf{Z}$-algebra generated by $\{c_\nu: \nu \geqq 0\} \cup \{\bar{\varepsilon}_\nu: \nu > 1\}$. Any finitely generated $\mathbf{Z}$-subalgebra of k is easily seen to be in $0_k[1/h]$ for some h.) The congruences are therefore interpreted ideal theoretically in R. It should also be noted that the congruences above are independent of the choice of the expansion of ω, see e.g., **[9]**, Proposition 5.

Notice that if f has Kummer congruences with respect to ω at a, then f has Kummer congruences with respect to $c\omega$ at a for any c in $k - \{0\}$. For $f = \sum_{n=0}^{\infty}(a_n/n)((ct)^n/n!)$ and $c\omega = \sum_{\nu=1}^{\infty}(\varepsilon_\nu/c^{\nu-1})(cx)^{\nu-1}d(cx)$ so

$$\sum_{i=0}^{r}(-1)^{r-i}\binom{r}{i}\left(\frac{\varepsilon_p}{c^{p-1}}\right)^{r-i}\frac{a_{m+i(p-1)}}{c^{m+i(p-1)}}$$
$$=\frac{1}{c^{m+r(p-1)}}\sum_{i=0}^{r}(-1)^{r-i}\binom{r}{i}\varepsilon_p^{r-r}a_{m+i(p-1)} \equiv 0 \bmod p^r.$$

We are now ready to state and prove our results.

THEOREM 3. *Let C be a connected algebraic group of dimension one defined over an algebraic number field k with an invariant differential ω. Then for any k-rational point a on C and any rational function f on C regular at the point a, f has Kummer congruences with respect to ω at a.*

PROOF. Coordinatize C so that $(0, 1)$ (written affinely) is e, the identity of C and such that the tangent line at e is not vertical. (Recall that tangent lines at all points on C exist since these points are necessarily simple.) If $\oplus$ denotes the group operation on C, then $(x_1, y_1) \oplus (x_2, y_2) = (P_1(x_1, y_1; x_2, y_2), P_2(x_1, y_1; x_2, y_2))$ where P_1 and P_2 are regular functions on $C \times C$ and (x_1, y_1), (x_2, y_2) are independent generic points. If $0_i (i = 1, 2)$ are the local rings of e in $k(x_i, y_i)$, then by assumption $x_i (i = 1, 2)$ are generators of the maximal ideals M_i of 0_i. An extension of the arguments in **[6]**, pp. 221–222, then shows that $P_1(x_1, y_1; x_2, y_2) = F(x_1, x_2)$ where $F(u, v)$ is a formal group over k. Now since P_1 is regular and since $y_i = \sum_{\nu=0}^{\infty} c_\nu x_i^\nu$ where $\{c_\nu: \nu \geqq 0\}$ is contained in a finitely generated $\mathbf{Z}$-subalgebra of k, we see that $F(u, v)$ is defined over $R = 0_k[1/h]$ for some positive rational integer h.

From the theory of formal groups there exists a formal power series $\lambda(x) = \sum_{\nu=1}^{\infty} \varepsilon_\nu x^\nu/\nu$, with $\varepsilon_1 = 1$ and $\varepsilon_\nu \in k (\nu \geqq 1)$, such that $F(u, v) = \lambda^{-1}(\lambda(u) + \lambda(v))$, see **[5]** p. 202. Moreover, since $(\partial F/\partial u)(0, v)^{-1} = \lambda'(v)$ by Proposition 1 in **[5]** and since $F(u, v)$ is defined over R, we see that $\varepsilon_\nu \in R$ for all $\nu \geqq 1$. Let $t_i = \lambda(x_i) \in k(x_i, y_i)_{M_i}$. Then since t_i are local uniformizing parameters of M_i in the completions, we have that $x_i = \lambda^{-1}(t_i) = \sum_{n=1}^{\infty} a_n t_i^n/n!$ for some $a_n \in k$. From the identity $\lambda^{-1}(\lambda(x_i)) = x_i$ it is easy to show that $a_n \in R$ for all $n \geqq 1$ and $a_1 = 1$. Hence we have $\lambda^{-1}(t_1 + t_2) = F(\lambda^{-1}(t_1), \lambda^{-1}(t_2))$. Let $\omega_F = \lambda'(x)dx = \sum_{\nu=1}^{\infty} \varepsilon_\nu x^{\nu-1}\,dx$ so

ω_F is the canonical invariant differentiation of $F(u, v)$. Thus by Theorem 2, $x_i = \lambda^{-1}(t_i)$ has strong Kummer congruences at all primes p (with respect to ω_F).

Now let (x, y) be any generic zero of C. By the preceding argument we see that x has Kummer congruences with respect to ω_F at e. We need to show that x has Kummer congruences with respect to ω at e or equivalently with respect to $c\omega$ where $c \in k - \{0\}$. To this end let (t, u) be a generic zero of C independent of (x, y). Clearly, any differential on $k(x, y)/k$ may be considered on $k(t, u)(x, y)/k(t, u)$. Now write $\omega = g(x, y)dx$ which is regular at e so $g(0, 1)$ is defined. Let $\tau_{(t,u)}$ denote the translation of points by this point (t, u). In particular, $\tau_{(t,u)}(x, y) = (t, u) \oplus (x, y)$. Then $g(x, y)dx = \omega = \tau^*_{(t,u)}\omega = g(P_1(t, u; x, y), P_2(t, u; x, y))dP_1(t, u; x, y)$. Thus $g(P_1(t, u; x, y), P_2(t, u; x, y))\,(\partial F/\partial x)(t, x) = g(x, y)$ By specializing (x, y) to $(0, 1)$ we obtain $g(t, u)\,(\partial F/\partial x)(t, 0) = g(0, 1)$. Then $g(0, 1) \neq 0$ and by Proposition 1 in [5], we obtain that $\omega_F = g(0, 1)\omega$ near $(0, 1)$. Therefore x has Kummer congruences with respect to $g(0, 1)\omega$ (and thus ω) at e.

Next suppose f is an arbitrary rational function on C regular at e. Then $f = \sum_{\nu=0}^{\infty} c_\nu x^\nu$, and so by the corollary to Theorem 1, p. 299 in [2], we may conclude that f has Kummer congruences with respect to ω at e.

Now suppose a is an arbitrary point on C and f is any rational function on C regular at a. Suppose $f = \sum_{n=0}^{\infty} a_n u^n/n!$ where u is a local uniformizing parameter in the completion of $k(C)$ at P_a such that $du = \omega$ near a. Then $\tau_a^* P_a = P_e$. Also since τ_a^* is continuous on $k(C)$ with respect to the P_a-adic topology, τ_a^* extends uniquely to an isomorphism from $k(C)_{P_a}$ onto $K(C)_{P_e}$. Hence $\tau_a^* f = \sum_{n=0}^{\infty} a_n(\tau_a^* u)^n/n!$. But then since $\tau_a^*\omega = \omega$, $\tau_a^* u = t$ where t is the local uniformizing parameter at e such that $dt = \omega$ near e.

Therefore we are reduced to an expansion at e and the theorem is proved.

As an application of Theorem 3, consider the curve $y = 1 + x^2$ which is given parametrically by $x = \tan t$, $y = \sec^2 t$. This curve is an algebraic group over Q with invariant differential $\omega = dt$. If $a = (x_0, y_0)$ is a point on the curve then a uniformizing parameter is $t - \alpha$ for some α. Then $\tan t = \sum_{n=0}^{\infty} a_n(\alpha)(t - \alpha)^n/n!$ where $a_n(\alpha) = \tan^{(n)}\alpha$. An expansion for ω is given by $\sum_{n=1}^{\infty} (-1)^{n-1} x^{2n-1}/(2n-1)\, dx$ where $x = \tan t$. Therefore by Theorem 3

$$\sum_{i=0}^{r} (-1)^{r-i}\binom{r}{i}(-1)^{(p+1)/2(r-i)}\; a_{m+i(p-1)}(\alpha) \equiv 0 \bmod p^r \text{ for all } m \geqq r \geqq 1.$$

(This generalizes Kummer congruences for $a_n(0)$).

As another application of this theorem, notice that any rational function on an elliptic curve regular at a point a has Kummer congruences with respect to any differential of the first kind at a, since an elliptic curve is a one-dimensional abelian variety and the differentials of the first kind are the invariant differentials of the group.

We now generalize Theorem 3 to include certain algebraic plane curves which are not necessarily algebraic groups.

THEOREM 4. *Let C be an irreducible algebraic curve defined over an algebraic number field k and let ω be a differential on C. Suppose there exists a k-rational mapping ϕ from C onto a dense subset of C', a connected algebraic group of dimension one, defined over k, with an invariant differential ω' such that $\phi^*\omega' = \omega$. Then for any k-rational simple point a in the domain of ϕ such that ϕ is unramified at a and for any rational function f on C regular at a, f has Kummer congruences with respect to ω at the point a.*

PROOF. Let $a' = \phi(a)$ and let $z_0 \in k(C')$ be a local uniformizing parameter at a'. Then $\omega' = dz_0/w_0$ for some $w_0 \in k(C')$. Since ω' is regular and nonvanishing everywhere on C', $\omega' = \sum_{\nu=1}^{\infty} \varepsilon_\nu z_0^{\nu-1}\, dz_0$ where we assume $\varepsilon_1 = 1$ by multiplying z_0 by a constant if necessary. But then $\omega = \phi^*\omega' = \sum_{\nu=1}^{\infty} \varepsilon_\nu z^{\nu-1} dz$ where $z = \phi^* z_0$. Moreover since P_a is unramified over $\phi^* P_a$, we see that z is a local uniformizing parameter at the point a. Now let t_0 be a local uniformizing parameter at a' in $k(C')_{P_a}$ such that $dt_0 = \omega'$ near a'. Write $z_0 = \sum_{n=1}^{\infty} a_n t_0^n/n!$. By Theorem 3, z_0 has Kummer congruences with respect to ω' at a'. But $z = \phi^* z_0 = \sum_{n=1}^{\infty} a_n t^n/n!$ where $\phi^* t_0 = t$. Moreover ϕ^* since$\omega' = \omega$, $dt = \omega$ near a. Hence z has Kummer congruences with respect to ω at a. In general, if $f \in k(C)$ is regular at a, then $f = \sum_{\nu=0}^{\infty} c_\nu z^\nu$ so by [2], f has Kummer congruences with respect to ω at a, whence the theorem follows.

From the proofs of the previous two theorems we may extract the following corollary.

COROLLARY. *Assume the hypothesis of Theorem 4. Further, let $\omega = \sum_{\nu=1}^{\infty} \varepsilon_\nu x^{\nu-1} dx$ where $\varepsilon_1 = 1$ and where x is the local uniformizing parameter for any k-rational simple point a in C at which ϕ is unramified. Then*

$$\varepsilon_{p\nu} \equiv \varepsilon_p \varepsilon_\nu^p \bmod p \text{ for all } \nu \geqq 1.$$

PROOF. It suffices to consider $C = C'$ and $\phi =$ identity mapping (see proof of Theorem 4). Moreover by the invariance of ω we may assume $a = e$ the identity element on C (see the proof of Theorem 3). But then $\omega = \omega_F$ near e. Since $F(u, v)$ is defined over $R = 0_k[1/h]$, the above congruences hold by Theorem 2.

As an application of Theorem 4, consider the curve C defined by $y^2 = 1 + dx^6$ where d is some nonzero algebraic number. Then two independent differentials of the first kind include $\omega_1 = dx/y$ and $\omega_2 =$

$x(dx/y)$. Now $k(C)$ contains subfields $k(z_i, w_i)$ for $i = 1, 2$ such that $w_1^2 = 4z_1 + 4dz_1^4$ and $w_2^2 = 4 + 4dz_2^3$ and such that $\omega_i = dz_i/w_i$ for $i = 1$, 2 as is easily verified. But $k(z_i, w_i)$ are elliptic function fields and dz_i/w_i are differentials of the first kind. Therefore Kummer congruences hold with respect to ω_1 and ω_2.

Also from Proposition 11 in [**8**], we know that for any curve C of the form $y^2 = 1 + dx^m$ where d is as above and $m = 5$ or $m \geqq 7$, Kummer congruences do not hold for x with respect to ω, at (0, 1). Thus by Theorem 4, there is no subfield of $k(C)$ which is the rational function field of the coordinate ring of a connected algebraic group for which ω is the extension of an invariant differential.

References

1. L. Carlitz, *The coefficients of the reciprocal of a series*, Duke Math. J. **9** (1941), 689–700.

2. ———, *Congruences for the coefficients of the Jacobi elliptic functions*, Duke Math. J. **16** (1949), 297–302.

3. P. Cartier, *Groups formels, fonctions automorphes et fonctions zeta des courbes elliptique*, Actes, Congres intern. Math. Tome **2** (1970), 291–299.

4. J. Dieudonné, *Lie groups and Lie hyperalgebras over a field of characteristic p* > 0 (II), Amer. J. Math. **77** (1955), 218–244.

5. T. Honda, *Formal groups and zeta-functions*, Osaka J. Math. **5** (1968), 199–213.

6. S. Lang, *Introduction to Algebraic Geometry*, Reading, Mass. Addison-Wesley, 1973.

7. C. Snyder, *A concept of Bernoulli numbers in algebraic function fields*, J. reine angew. Math. **307–308** (1979), 295–308.

8. ———, *Kummer congruences for the coefficients of Hurwitz series*, Acta Arith. **40** (1982), 175–191.

9. ———, *A concept of Bernoulli numbers in algebraic function fields* (II), manuscripta math. 35 (1981), 69–89.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MAINE, ORONO, ME 04469