JOURNAL OF NUMBER THEORY **21**, 141–155 (1985)

Some Congruences for the Apery Numbers

F. BEUKERS

Mathematisch Instituut, University of Leiden, P.O. Box 9512, 2300 RA Leiden, Netherlands

Communicated by M. Waldschmidt

Received September 7, 1983; revised December 12, 1983

In 1979 R. Apéry introduced the numbers $a_n = \sum_0^n \binom{n}{k}^2 \binom{n+k}{k}$ and $u_n = \sum_0^n \binom{n}{k}^2 \binom{n+k}{k}^2$ in his irrationality proof for $\zeta(2)$ and $\zeta(3)$. We prove some congruences for these numbers which generalize congruences previously published in this journal.

1. An Account of the Congruences

This paper deals with congruences for the numbers

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} \qquad n = 0, 1, 2, \ldots, \tag{1}$$

and

$$u_n = \sum_{k=0}^{u} \binom{n}{k}^2 \binom{n+k}{k}^2 \qquad n = 0, 1, 2, \ldots. \tag{2}$$

The first few values of a_n are given by 1, 3, 19, 147, 1251,..., and for u_n they read 1, 5, 73, 1445, 33001,.... As is well known these numbers occur in Apéry's irrationality proof of $\zeta(2)$ and $\zeta(3)$, respectively (see [9]).

The first to consider congruences for u_n were Chowla, Cowles, and Cowles [4]. They found a number of congruences and conjectured a few others, which were proved subsequently by Radoux [10] (partly), Gessel [6], and Mimura [8]. One of these congruences, which is of particular interest to us, reads

$$u_{p-1} \equiv 1 \pmod{p^3} \qquad \text{for all primes } p > 3.$$

For a_n we have a similar one, namely

$$a_{p-1} \equiv 1 \pmod{p^2} \qquad p \geqslant 3.$$

0022-314X/85 $3.00

Both congruences are quite easy to prove by using the explicit expressions (1) and (2). In this paper we shall prove

THEOREM 1. *Let $m, r \in \mathbb{N}$ and $p > 3$ prime. Then*

$$u_{mp^r-1} \equiv u_{mp^{r-1}-1} \pmod{p^{3r}}, \qquad a_{mp^r-1} \equiv a_{mp^{r-1}-1} \pmod{p^{3r}}.$$

The proof of these congruences is quite involved and we defer its presentation to Sections 2 and 3. It would be very nice if a more natural proof of Theorem 1 were found instead of the "brute force method" we employed.

It is possible however, to prove in a simple way a somewhat weaker statement, which unlike Theorem 1 holds for all primes.

THEOREM 2. *Let $m, r \in \mathbb{N}$ and let p be any prime. Then*

$$u_{mp^r-1} \equiv u_{mp^{r-1}-1} \pmod{p^r}, \qquad a_{mp^r-1} \equiv a_{mp^{r-1}-1} \pmod{p^r}.$$

Proof. We require the congruences

(i) $\binom{mp^r}{k} \equiv 0 \pmod{p^r}$ $\forall m \in \mathbb{Z}$, $k, r \in \mathbb{N}$, $k \not\equiv 0 \pmod{p}$

(ii) $\binom{mp^r}{kp} \equiv \binom{mp^{r-1}}{k}(-1)^{k(p-1)} \pmod{p^r}$ $\forall m \in \mathbb{Z}$, $k, r \in \mathbb{N}$

(iii) $\binom{mp^r-1}{k} \equiv \binom{mp^{r-1}-1}{[k/p]}(-1)^{k-[k/p]} \pmod{p^r}$ $\forall m \in \mathbb{Z}$, $k, r \in \mathbb{N}$.

Congruence (i) is trivial since $\binom{mp^r}{k} = (mp^r/k)\binom{mp^r-1}{k-1} \equiv 0 \pmod{p^r}$. By induction on r one proves $(1-X)^{mp^r} \equiv (1-X^p)^{mp^{r-1}} \pmod{p^r}$, from which (ii) follows by comparison of the coefficients of X^{kp}. The third congruence follows from comparison of the coefficients of X^k in

$$\begin{aligned}(1-X)^{mp^r-1} &\equiv (1-X^p)^{mp^{r-1}-1}\frac{1-X^p}{1-X}\\ &\equiv (1-X^p)^{mp^{r-1}-1}(1+X+\cdots+X^{p-1}) \pmod{p^r}.\end{aligned}$$

We now have, on noticing that $\binom{n+k}{k} = (-1)^k\binom{-n-1}{k}$,

$$a_{mp^r-1} = \sum_{k=0}^{mp^r-1} \binom{mp^r-1}{k}^2 \binom{-mp^r}{k}(-1)^k.$$

Since, by (i) the summand $\equiv 0 \pmod{p^r}$ if $p \nmid k$, we have

$$a_{mp^r-1} \equiv \sum_{l=0}^{mp^{r-1}-1} \binom{mp^r-1}{lp}^2 \binom{-mp^r}{lp}(-1)^{lp} \pmod{p^r}.$$

Use (ii) and (iii) to obtain

$$a_{mp^r-1} \equiv \sum_{l=0}^{mp^{r-1}-1} \binom{mp^{r-1}-1}{l}^2 \binom{-mp^{r-1}}{l} (-1)^{lp}((-1)^{l(p-1)}$$

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

The proof runs similarly for the u_ns. Q.E.D.

The congruences given in Theorem 2 have an elegant interpretation implied by the following.

PROPOSITION. *Let* $c_1, c_2, c_3, ..., \in \mathbb{Z}$, $c_1 = 1$. *Then*

$$c_{mp^r} \equiv c_{mp^{r-1}} \pmod{p^r} \qquad \forall m, r \in \mathbb{N}, \ \forall \text{ primes } p \Leftrightarrow \exp\left(\sum_1^\infty \frac{c_n}{n} T^n\right) \in \mathbb{Z}[\![T]\!].$$

Thus, for example, the congruences in Theorem 2 imply that

$$\exp\left(\sum_1^\infty \frac{a_{n-1}}{n} T^n\right) \in \mathbb{Z}[\![T]\!].$$

The proof of this Proposition can be derived from a lemma of Dwork [5, Lemma 1] or from Hazewinkel's functional equation lemma [7, Chap. 1.2.2]. We give a separate proof however.

Proof of the Proposition. Our assertion is proved if we show that for each prime p,

$$c_{mp^r} \equiv c_{mp^{r-1}} \pmod{p^r} \qquad \forall m, r \in \mathbb{N} \Leftrightarrow \exp\left(\sum_1^\infty \frac{c_n}{n} T^n\right) \in \mathbb{Z}_p[\![T]\!], \tag{3}$$

where $\mathbb{Z}_p$ denotes the ring of p-adic integers.

Let $f(T) = \sum_1^\infty c_n n^{-1} T^n$. Notice that the congruences in (3) are equivalent to the statement

$$f(T) - \frac{1}{p} f(T^p) \in \mathbb{Z}_p[\![T]\!]. \tag{4}$$

Let $\exp(f(T)) = 1 + h(T)$, where $h(T) = T + \sum_2^\infty \beta_n T^n$, $\beta_n \in \mathbb{Q}_p$. Statement (4) now becomes

$$\log(1 + h(T)) - \frac{1}{p} \log(1 + h(T^p)) \in \mathbb{Z}_p[\![T]\!]$$

or

$$\frac{(1+h(T))^p}{1+h(T^p)} \in 1 + p\mathbb{Z}_p[\![T]\!]. \tag{5}$$

We thus see that the congruences in (3) are equivalent to statement (5). In order to prove our proposition we must show that (5) is equivalent to $h(T) \in \mathbb{Z}_p[\![T]\!]$ for any prime p, which is precisely the contents of Dwork's lemma.

By Fermat's theorem (5) holds if $h(T) \in \mathbb{Z}_p[\![T]\!]$. Now suppose conversely, that (5) holds. We shall prove, by induction on k, that $h(T) \in \mathbb{Z}_p[\![T]\!]$ (mod T^k) for any k, and thus $h(T) \in \mathbb{Z}_p[\![T]\!]$. Suppose that $h(T) \in \mathbb{Z}_p[\![T]\!]$ (mod T^k) for some $k \geqslant 2$. Then $(h(T))^n \in \mathbb{Z}^p[\![T]\!]$ (mod T^{k+1}) for all $n \geqslant 2$ and $h(T^p) \in \mathbb{Z}_p[\![T]\!]$ (mod T^{k+1}). Using these facts it follows from (5) that

$$1 + ph(T) \in 1 + p\mathbb{Z}[\![T]\!] \pmod{T^{k+1}},$$

hence $h(T) \in \mathbb{Z}_p[\![T]\!]$ (mod T^{k+1}). By noticing that $h(T) = T$ (mod T^2) our induction proces is completed. Q.E.D.

The condition $\exp(\sum_1^\infty c_n n^{-1} T^n) \in \mathbb{Z}[\![T]\!]$ has a well-known interpretation in formal group theory. A commutative formal group law over $\mathbb{Z}$ is a formal power series in two variables $F(X, Y) \in \mathbb{Z}[\![X, Y]\!]$ of the form

$$F(X, Y) = X + Y + \sum_{i,j \geqslant 1} c_{ij} X^i Y^j$$

such that

(i) $F(X, Y) = F(Y, X)$

(ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

Well-known examples are given by

$$G_a(X, Y) = X + Y \qquad \text{(additive group)}$$

$$G_m(X, Y) = X + Y + XY \qquad \text{(multiplicative group)}.$$

Given a formal group law over $\mathbb{Z}$, there exists a series $f(X) = \sum_1^\infty c_n n^{-1} X^n$, $c_1 = 1$, $c_n \in \mathbb{Z}$ such that $F(X, Y) = f^{-1}(f(X) + f(Y))$. This series f is called the logarithm of the group law. For the multiplicative group G_m the logarithm is given by $\log(1 + X)$. Let $F(X, Y)$ and $G(X, Y)$ be two formal group laws over $\mathbb{Z}$ and f and g their corresponding logarithms. Then F and G are called isomorphic over $\mathbb{Z}$ if there exists a power series $\alpha(T) \in \mathbb{Z}[\![T]\!]$, $\alpha(T) \equiv T$ (mod T^2) such that

$$G(\alpha(X), \alpha(Y)) = \alpha(F(X, Y))$$

or, equivalently,

$$f(X) = g(\alpha(X)).$$

These definitions can be found in Hazewinkel's book on formal group theory [7].

Now, let $c_1, c_2, c_3, \ldots, \in \mathbb{Z}$, $c_1 = 1$. Let $h(T)$ be defined by $\sum c_n n^{-1} T^n = \log(1 + h(T))$. It is now easy to see that the statement $h(t) \in \mathbb{Z}[\![T]\!]$ is equivalent to saying that $\sum c_n n^{-1} T^n$ is the logarithm of a formal group law over $\mathbb{Z}$, which is isomorphic over $\mathbb{Z}$ to G_m.

Let $\mathscr{A}(t) = \sum_0^\infty a_n t^n$, $\mathscr{U}(t) = \sum_0^\infty u_n t^n$. Then Theorem 2 and the above remarks on formal groups imply that $\int_0^T \mathscr{A}(t)\, dt$ and $\int_0^T \mathscr{U}(t)\, dt$ are logarithms of formal groups over $\mathbb{Z}$ which are isomorphic over $\mathbb{Z}$ to G_m. Further investigations shows that $\mathscr{A}(t)$ and $\mathscr{U}(t)$ can be considered as periods of certain holomorphic differential forms on families of elliptic curves and algebraic K3-surfaces respectively (see [1, 2]). From such an algebraic–geometric approach one may hope to obtain some more insight into the numbers a_n and u_n. As a result of this viewpoint it turned out that there exist more congruences for the numbers a_n. In a joint paper with Stienstra [3] we study the formal Brauer group of some elliptic K3-surfaces and one of the consequences of that paper is the following

THEOREM 3. *Let p be an odd prime and let $m, r \in \mathbb{N}$, m odd. Define*

$$\begin{aligned} \alpha_p &= 0 && \text{if } p \equiv 3 \pmod 4 \\ &= 4a^2 - 2p && \text{if } p \equiv a^2 + b^2 \text{ with } a, b \in \mathbb{Z},\ a \equiv 1 \pmod 2 \end{aligned}$$

Then,

$$a_{(1/2)(mp^r-1)} - \alpha_p a_{(1/2)(mp^{r-1}-1)} + (-1)^{(1/2)(p-1)} p^2 a_{(1/2)(mp^{r-2}-1)} \equiv 0 \pmod{p^r}, \tag{6}$$

where $a_{(1/2)(mp^s-1)}$ is taken zero if $s < 0$.

These congruences are similar to the Atkin–Swinnerton–Dyer congruences for the coefficients of the holomorphic 1-form on an elliptic curve [7, Chap. VI.33.2].

The congruences in Theorem 1 are stronger than the ones suggested by formal group theory. For that reason we named them supercongruences. Also in the case of Theorem 3 we seem to have such supercongruences. Some numerical experimenting suggests that congruence (6) holds mod p^{2r} instead of mod p^r if $p \geqslant 5$. However, we have no idea to prove this.

Finally we would like to draw attention to another point which also came up through some numerical computations. It seems that if we take

$(m, p) = (1, 5)$, $(3, 5)$, $(4, 5)$, $(5, 7)$, or $(2, 11)$ we have $a_{mp^r} \equiv a_{mp^{r-1}} \pmod{p^{3r+1}}$ $\forall r \in \mathbb{N}$. If $(m, p) = (2, 5)$ or $(7, 5)$ one may even have $a_{mp^r} \equiv a_{mp^{r-1}} \pmod{p^{3r+2}}$ $\forall r \in \mathbb{N}$. It would be very interesting to know whether these congruences are true and for which other pairs (m, p) they hold.

2. Some Lemmas

In the lemmas and proofs of this section we will use the following notations throughout

p	fixed prime $\geqslant 5$
r	fixed natural number
$[x]$	largest integer not exceeding x
$\{x\}$	$x - [x]$
$\prod'_{k \in V}$ or $\sum'_{k \in V}$	take the product or sum over those values $k \in V$ for which $p \nmid k$
$v_p(n)$	number of prime factors p in n.

Lemma 1. *For any $l \in \mathbb{Z}$ we have*

$$\sum'_{[\lambda p^{-r}] = l} \frac{1}{\lambda} \equiv 0 \pmod{p^{2r}}.$$

Proof. We have

$$\begin{aligned}
\sum'_{[\lambda p^{-r}] = l} \frac{1}{\lambda} &= \frac{1}{2} \sum'_{[\lambda p^{-r}] = l} \left(\frac{1}{\lambda} + \frac{1}{(2l+1)\, p^r - \lambda} \right) \\
&\equiv \frac{1}{2} \sum'_{[\lambda p^{-r}] = l} \frac{1}{\lambda} - \frac{1}{\lambda} \left(1 + \frac{(2l+1)\, p^r}{\lambda} + \cdots \right) \pmod{p^{2r}} \\
&\equiv -\frac{p^r}{2} (2l+1) \sum_{\lambda=1}^{p^r - 1}{}' \frac{1}{\lambda^2} \equiv 0 \pmod{p^{2r}}. \qquad \text{Q.E.D.}
\end{aligned}$$

Lemma 2. *For any $m \in \mathbb{Z}$, $k \in \mathbb{N}$ we have*

(i) $$\binom{mp^r - 1}{k} = \binom{mp^{r-1} - 1}{[k/p]} \prod_{\lambda=1}^{k}{}' \frac{mp^r - \lambda}{\lambda}.$$

If $p|k$, then

(ii) $$\binom{mp^r}{k}=\binom{mp^{r-1}}{k/p}\prod_{\lambda=1}^{k}{}' \frac{mp^r-\lambda}{\lambda}.$$

Proof. Notice that by splitting the product into a product with $p\nmid\lambda$ and one with $\lambda=\mu p$, we find

$$\binom{mp^r-1}{k}=\prod_{\lambda=1}^{k}\frac{mp^r-\lambda}{\lambda}=\prod_{\lambda=1}^{k}{}'\frac{mp^r-\lambda}{\lambda}\prod_{\mu=1}^{[k/p]}\frac{mp^{r-1}-\mu}{\mu}.$$

The last product equals $\binom{mp^{r-1}-1}{[k/p]}$, which proves (i). Now write

$$\binom{mp^r}{k}=\frac{mp^r}{k}\binom{mp^r-1}{k-1}=\frac{mp^{r-1}}{k/p}\binom{mp^{r-1}-1}{[k-1/p]}\prod_{\lambda=1}^{k-1}{}'\frac{mp^r-\lambda}{\lambda}$$

and assertion (ii) follows from $\prod'^{k-1}_{\lambda=1}=\prod'^{k}_{\lambda=1}$ and $[k-1/p]=(k/p)-1$.

Q.E.D.

LEMMA 3. *Let $a_k\in\mathbb{Z}_p$ $(k=0,1,2,3,...)$ be such that*

$$\sum_{[kp^{-s}]=l} a_k\equiv 0 \pmod{p^s}\qquad \text{for any } s, l\in\mathbb{Z}_{\geqslant 0}.$$

Let $e\in\mathbb{N}$. Then

(i) $$\sum_{[kp^{-r}]=l} a_k\binom{mp^r-1}{k}^2\binom{-mp^r-1}{k}^e(-1)^{ke}\equiv 0 \pmod{p^r}\ \forall l, m\in\mathbb{Z}_{\geqslant 0}. \tag{7}$$

If, in addition $a_k=0$ for all $k\equiv 0 \pmod p$, then

(ii) $$\sum_{[kp^{-r}]=l} a_k\binom{mp^r-1}{k}^2\binom{-mp^r-1}{k-1}^e(-1)^{ke}\equiv 0 \pmod{p^r}\quad \forall l, m\in\mathbb{Z}_{\geqslant 0}. \tag{8}$$

Proof. (i) We proceed by induction on r. For $r=0$ our assertion is trivial. Suppose we have shown it for $0,1,..., r-1$. We now show that the left-hand side of (7), which we denote by A, is zero mod p^r. To this end we apply the congruence

$$\binom{mp^r-1}{k}\equiv\binom{mp^{r-1}-1}{[k/p]}(-1)^{\{k/p\}p}\qquad m\in\mathbb{Z}$$

which is a consequence of the congruence (iii) in the proof of Theorem 2. We obtain,

$$A \equiv \sum_{[kp^{-r}]=l} a_k \binom{mp^{r-1}-1}{[k/p]}^2 \binom{-mp^{r-1}-1}{[k/p]}^e (-1)^{ke}(-1)^{e\{k/p\}p} (\text{mod } p^r).$$

Note that $k+\{k/p\}\, p \equiv [k/p]$ (mod 2). Collect all terms having the same $[k/p]$. Then

$$A \equiv \sum_{[np^{-r+1}]=l} \left(\sum_{[kp^{-1}]=n} a_k \right) \binom{mp^{r-1}-1}{n}^2 \binom{-mp^{r-1}-1}{n}^e (-1)^{en} \ (\text{mod } p^r).$$

We now apply the induction hypothesis for $r-1$ with the new coefficients

$$\bar{a}_n = \frac{1}{p} \sum_{[kp^{-1}]=n} a_k.$$

The $\bar{a}_n$ satisfy the hypothesis of our lemma, since

$$\sum_{[np^{-s}]=l} \bar{a}_n = \frac{1}{p} \sum_{[kp^{-s-1}]=l} a_k \equiv 0 \ (\text{mod } p^s) \qquad \forall s, l \in \mathbb{Z}_{\geqslant 0},$$

and we obtain

$$A \equiv p \sum_{[np^{-r+1}]=l} \bar{a}_n \binom{mp^{r-1}-1}{n}^2 \binom{-mp^{r-1}-1}{n}^e (-1)^{en} \equiv 0 \ (\text{mod } p^r)$$

which proves (i).

Assertion (ii) can be proved in the same way as above. Apply the first induction step to the left-hand side of (8) and notice that we may put $[k-1/p]=[k/p]$ since we sum essentially over $(k, p)=1$. After this step we are back again in the situation of Lemma 3(i). Q.E.D.

LEMMA 4. *Let $s, t \in \mathbb{Z}_{\geqslant 0}$. Then*

$$\text{(i)} \quad \sum_{[np^{-t}]=i} \left(\sum_{[kp^{-s}]=n}' \frac{1}{k} \right) \left(\sum_{\lambda=1}^{n}{}' \frac{1}{\lambda} \right) \equiv 0 \ (\text{mod } p^{t+2s}) \qquad \forall i \in \mathbb{Z}. \qquad (9)$$

$$\text{(ii)} \quad \sum_{[kp^{-t}]=i}' \frac{1}{k} \sum_{\lambda=1}^{kp^s}{}' \equiv 0 \ (\text{mod } p^{t+s}) \qquad \forall i \in \mathbb{Z}.$$

Proof. We first prove (i) for $s \geqslant 1$. The case $s=0$ is contained in (ii). Write

$$\sum_{[kp^{-s}]=n}' \frac{1}{k} = \sum_{\kappa=1}^{p^s-1}{}' \frac{1}{\kappa+np^s} = \sum_{\kappa=1}^{p^s-1}{}' \frac{1}{\kappa} - \frac{np^s}{\kappa^2} + \frac{n^2p^{2s}}{\kappa^3} + \cdots.$$

Hence the left-hand side of (9) becomes

$$\sum_{\kappa=1}^{p^s-1}{}' \sum_{[np^{-t}]=i} \left(\frac{1}{\kappa}-\frac{np^s}{\kappa^2}+\frac{n^2p^{2s}}{\kappa^3}-\cdots\right)\left(\sum_{\lambda=1}^{n}{}' \frac{1}{\lambda}\right)$$
$$\equiv \sum_{\kappa=1}^{p^s-1}{}' \sum_{n=0}^{p^t-1} \left(\frac{1}{\kappa}-\frac{np^s}{\kappa^2}+\frac{n^2p^{2s}}{\kappa^3}-\cdots\right)\left(\sum_{\lambda=1}^{n}{}' \frac{1}{\lambda}\right) \pmod{p^{t+2s}}.$$

Since $\sum' 1/\kappa \equiv 0 \pmod{p^{2s}}$, $\sum' 1/\kappa^2 \equiv 0 \pmod{p^s}$, etc., we see that it suffices to show

$$\sum_{n=0}^{p^t-1} n^k \sum_{\lambda=1}^{n}{}' \frac{1}{\lambda} \equiv 0 \pmod{p^t} \qquad \forall k \in \mathbb{Z}_{\geqslant 0}$$

or, equivalently,

$$\sum_{n=0}^{p^t-1} k! \binom{n}{k}\left(\sum_{\lambda=1}^{n}{}' \frac{1}{\lambda}\right) \equiv 0 \pmod{p^t} \qquad \forall k \in \mathbb{Z}_{\geqslant 0}. \tag{10}$$

We can write the left-hand side as

$$\sum_{n=0}^{p^t-1} k!\left\{\binom{n+1}{k+1}-\binom{n}{k+1}\right\}\left(\sum_{\lambda=1}^{n}{}' \frac{1}{\lambda}\right)$$
$$=\sum_{n=0}^{p^t-1}\left\{k!\binom{n+1}{k+1}\sum_{\lambda=1}^{n+1}{}'\frac{1}{\lambda}-k!\binom{n}{k+1}\sum_{\lambda=1}^{n}{}'\frac{1}{\lambda}\right\}-\sum_{n=0}^{p^t-1}\frac{k!}{n+1}\binom{n+1}{k+1}$$
$$=k!\binom{p^t}{k+1}\sum_{\lambda=1}^{p^t-1}{}'\frac{1}{\lambda}-\frac{k!}{k+1}\sum_{n=0}^{p^t-1}\binom{n}{k}$$
$$\equiv -\frac{k!}{k+1}\binom{p^t}{k+1} \equiv -\frac{k!}{(k+1)^2}p^t\binom{p^t-1}{k} \pmod{p^t}.$$

Since $v_p((k+1)^2) \leqslant v_p(k!)$ if $p \geqslant 5$, we see that the left-hand side of (10) is indeed zero mod p^t.

To prove (ii) notice that

$$\sum_{1}^{kp^s}{}'\frac{1}{\lambda} \equiv -\sum_{kp^s+1}^{p^{t+s}-1}{}'\frac{1}{\lambda} \equiv -\sum_{1}^{(p^t-k)p^s-1}{}'\frac{1}{p^{t+s}-\lambda} \equiv \sum_{1}^{(p^t-k)p^s}{}'\frac{1}{\lambda} \pmod{p^{t+s}}.$$

Hence

$$2\sum_{k=1}^{p^t-1}{}'\frac{1}{k}\sum_{1}^{kp^s}{}'\frac{1}{\lambda} \equiv \sum_{k=1}^{p^t-1}{}'\left(\frac{1}{k}+\frac{1}{p^t-k}\right)\sum_{1}^{kp^s}{}'\frac{1}{\lambda} \equiv 0 \pmod{p^{t+s}}$$

as desired.

LEMMA 5. *For any $l \in \mathbb{Z}_{\geqslant 0}$, $m \in \mathbb{N}$ we have*

$$\sum_{[kp^{-r}]=l}' \frac{1}{k}\binom{mp^r-1}{k}^2\binom{-mp^r-1}{k-1}(-1)^k \equiv 0 \pmod{p^{2r}}. \tag{11}$$

Proof. First we show by induction, that for $s=0, 1,..., r-1$ we have

$$A_s \equiv 0 \pmod{p^{2r}},$$

where

$$A_s = \sum_{[np^{-s}]=l}\left(\sum_{[kp^{-r+s}]=n}' \frac{1}{k}\right)\binom{mp^s-1}{n}^2\binom{-mp^s-1}{n}(-1)^n.$$

For $s=0$ this is clear by Lemma 1. Suppose we have proved $A_s \equiv 0 \pmod{p^{2r}}$ for some s. We now proceed to show that $A_{s+1} \equiv 0 \pmod{p^{2r}}$. Notice that by Lemma 2(i),

$$\begin{aligned}
&\binom{mp^{s+1}-1}{n}^2\binom{-mp^{s+1}-1}{n}(-1)^n \\
&\equiv \binom{mp^s-1}{[n/p]}^2\binom{-mp^s-1}{[n/p]}(-1)^n \\
&\quad \times \prod_{\lambda=1}^{n}{}' \left(\frac{mp^{s+1}-\lambda}{\lambda}\right)^2\left(\frac{-mp^{s+1}-\lambda}{\lambda}\right) \pmod{p^{2s+2}} \\
&\equiv \binom{mp^s-1}{[n/p]}^2\binom{-mp^s-1}{[n/p]}(-1)^{[n/p]} \prod_{\lambda=1}^{n}{}'\left(1-\frac{mp^{s+1}}{\lambda}\right) \pmod{p^{2s+2}} \\
&\equiv \binom{mp^s-1}{[n/p]}^2\binom{-mp^s-1}{[n/p]}(-1)^{[n/p]} \\
&\quad \times \left(1-\sum_{\lambda=1}^{n}{}' \frac{mp^{s+1}}{\lambda}\right) \pmod{p^{2s+2}}.
\end{aligned}$$

Substitute this in A_{s+1}, and collect all terms having the same value of $[n/p]$,

$$\begin{aligned}
A_{s+1} &\equiv \sum_{[qp^{-s}]=l}\ \sum_{[n/p]=q}\left(\sum_{[kp^{-r+s+1}]=n}' \frac{1}{k}\right)\left(1-\sum_{\lambda=1}^{n}{}' \frac{mp^{s+1}}{\lambda}\right) \\
&\quad \times \binom{mp^s-1}{q}^2\binom{-mp^s-1}{q}(-1)^q \pmod{p^{2r}} \\
&\equiv A_s - mp^{s+1}\sum_{[qp^{-s}]=l} p^{2(r-s)-1}a_q \\
&\quad \times \binom{mp^s-1}{q}^2\binom{-mp^s-1}{q}(-1)^q \pmod{p^{2r}},
\end{aligned}$$

where

$$a_q = p^{-2(r-s)+1} \sum_{[n/p]=q} \left(\sum'_{[kp^{-r+s+1}]=n} \frac{1}{k} \right) \left(\sum_{\lambda=1}^{n}{}' \frac{1}{\lambda} \right).$$

Notice that by Lemma 4(i) for any $j \in \mathbb{Z}$, $t \in \mathbb{N}$,

$$\sum_{[qp^{-t}]=j} a_q = \sum_{[np^{-t-1}]=j} p^{-2(r-s)+1} \left(\sum'_{[kp^{-r+s+1}]=n} \frac{1}{k} \right) \left(\sum_{\lambda=1}^{n}{}' \frac{1}{\lambda} \right) \equiv 0 \pmod{p^t},$$

and thus we can apply Lemma 3 with a_q, s instead of a_q, r to obtain

$$A_{s+1} \equiv A_s \equiv 0 \pmod{p^{2r}}.$$

Thus our induction procedure is concluded. In particular we have $A_{r-1} \equiv 0 \pmod{p^{2r}}$. To conclude the proof of our lemma, we reduce the left-hand side of (11) in the same way as in our induction step, where in addition we replace $[k-1/p]$ by $[k/p]$ since we sum over $(k, p) = 1$. By this step the left-hand side of (11) reduces to $A_{r-1} \pmod{p^{2r}}$, which we know to be zero mod p^{2r}. Q.E.D.

3. Proof of Theorem 1.

Proof of $u_{mp^r-1} \equiv u_{mp^{r-1}-1} \pmod{p^{3r}}$ $\forall m, r \in \mathbb{N}$. Write

$$u_{mp^r-1} = \sum_{l=0}^{mp^{r-1}-1} \binom{mp^r-1}{lp}^2 \binom{-mp^r}{lp}^2 + \sum_{k=0}^{mp^r-1}{}' \binom{mp^r-1}{k}^2 \binom{-mp^r}{k}^2.$$

The second summation on the right-hand side equals

$$\sum_{k=0}^{mp^r-1}{}' \frac{m^2p^{2r}}{k^2} \binom{mp^r-1}{k}^2 \binom{-mp^r-1}{k-1}^2. \tag{12}$$

Since

$$\sum'_{[kp^{-s}]=n} \frac{1}{k^2} \equiv 0 \pmod{p^s} \qquad \forall n \in \mathbb{Z},\ s \in \mathbb{N},$$

we can apply Lemma 3(ii) with $a_k = k^{-2}$ if $p \nmid k$, $a_k = 0$ otherwise, and conclude that expression (12) is zero mod p^{3r}. Hence

$$u_{mp^r-1} \equiv \sum_{l=0}^{mp^{r-1}-1} \binom{mp^r-1}{lp}^2 \binom{-mp^r}{lp}^2 \pmod{p^{3r}}.$$

Application of Lemma 2 yields

$$u_{mp^r-1} \equiv \sum_{l=0}^{mp^{r-1}-1} \binom{mp^{r-1}-1}{l}^2 \binom{-mp^{r-1}}{l}^2 \prod_{\lambda=1}^{lp}{}' \left(1-\frac{m^2p^{2r}}{\lambda^2}\right)^2 \pmod{p^{3r}}.$$

Notice that

$$\prod_{\lambda=1}^{lp}{}' \left(1-\frac{m^2p^{2r}}{\lambda^2}\right)^2 \equiv 1 - 2m^2p^{2r} \sum_{\lambda=1}^{lp}{}' \frac{1}{\lambda^2} \pmod{p^{3r}}$$

$$\equiv 1 \pmod{p^{\min(3r,\, 2r+v_p(lp))}}$$

and

$$\binom{-mp^{r-1}}{l}^2 = m^2 \frac{p^{2r-2}}{l^2} \binom{-mp^{r-1}-1}{l-1}^2 \equiv 0 \pmod{p^{2\max(r-v_p(lp),\, 0)}}.$$

Hence

$$u_{mp^r-1} \equiv \sum_{l=0}^{mp^{r-1}-1} \binom{mp^{r-1}-1}{l}^2 \binom{-mp^{r-1}}{l}^2 \equiv u_{mp^{r-1}-1} \pmod{p^{3r}}. \quad \text{Q.E.D.}$$

Proof of $a_{mp^r-1} \equiv a_{mp^{r-1}-1} \pmod{p^{3r}}$. Write

$$a_{mp^r-1} = \sum_{l=0}^{mp^{r-1}-1} \binom{mp^r-1}{lp}^2 \binom{-mp^r}{lp} (-1)^{lp} + \sum_{k=0}^{mp^r-1}{}' \binom{mp^r-1}{k}^2 \left(\binom{-mp^r}{k}\right)(-1)^k.$$

Writing $\binom{-mp^r}{k} = -(mp^r/k)\binom{-mp^r-1}{k-1}$ we see the second summation is zero mod p^{3r} according to Lemma 5. Hence

$$a_{mp^r-1} \equiv \sum_{l=0}^{mp^{r-1}-1} \binom{mp^r-1}{lp}^2 \binom{-mp^r}{lp} (-1)^{lp} \pmod{p^{3r}}$$

and application of Lemma 2 yields

$$a_{mp^r-1} \equiv \sum_{l=0}^{mp^{r-1}-1} \binom{mp^{r-1}-1}{l}^2 \binom{-mp^{r-1}}{l} (-1)^l \times \prod_{\lambda=1}^{lp}{}' \left(1-\frac{m^2p^{2r}}{\lambda^2}\right) \binom{mp^r-\lambda}{\lambda} \pmod{p^{3r}}.$$

Just as in the previous proof we know that

$$\prod_{\lambda=1}^{lp}{}' \left(1-\frac{m^2p^{2r}}{\lambda^2}\right) \equiv 1 \pmod{p^{\min(3r,\, 2r+v_p(2p))}},$$

$$\binom{-mp^{r-1}}{l} \equiv 0 \pmod{p^{\max(r-v_p(lp),\, 0)}}.$$

Hence

$$a_{mp^r-1} \equiv \sum_{l=0}^{mp^{r-1}-1} \binom{mp^{r-1}-1}{l}^2 \binom{-mp^{r-1}}{l} (-1)^l \prod_{\lambda=1}^{lp}{}' \left(1-\frac{mp^r}{\lambda}\right) \pmod{p^{3r}}.$$

Observe,

$$\prod_{\lambda=1}^{lp}{}' \left(1-\frac{mp^r}{\lambda}\right) \equiv 1 - mp^r \sum_{\lambda=1}^{lp}{}' \frac{1}{\lambda} \pmod{p^{2r+v_p(lp)}}.$$

And thus

$$a_{mp^r-1} \equiv a_{mp^{r-1}-1} - mp^r \sum_{l=0}^{mp^{r-1}-1} \left(\sum_{\lambda=1}^{lp}{}' \frac{1}{\lambda}\right) \times \binom{mp^{r-1}-1}{l}^2 \binom{-mp^{r-1}}{l} (-1)^l \pmod{p^{3r}}.$$

It suffices to show that the summation on the right-hand side is zero mod p^{2r} and then we are done. Split this summation into summations over l such that $v_p(lp)=s$ for $s=1, 2,..., r-1$ and finally $v_p(lp) \geqslant r$. If $v_p(lp) \geqslant r$ we know that $\sum{}'^{\,lp}_{1} 1/\lambda \equiv 0 \pmod{p^{2r}}$ and thus the summation over l with $v_p(lp) \geqslant r$ yields naught mod p^{3r} to a_{mp^r-1}. We must show that each of the terms

$$\sum_{k=0}^{mp^{r-s}-1} \left(\sum_{\lambda=1}^{kp^s}{}' \frac{1}{\lambda}\right) \binom{mp^{r-1}-1}{kp^{s-1}}^2 \binom{-mp^{r-1}}{kp^{s-1}} (-1)^{kp^{s-1}} \tag{13}$$

is zero mod p^{2r}. Notice that $p^{r-s} \mid \binom{-mp^{r-1}}{kp^{s-1}}$ and $\sum{}'^{\,kp^s}_{1} 1/\lambda \equiv 0 \pmod{p^{2s}}$. Furthermore,

$$\binom{mp^{r-1}-1}{kp^{s-1}} \equiv \binom{mp^{r-s}-1}{k} \pmod{p^{r-s}}$$

$$\binom{-mp^{r-1}}{kp^{s-1}} \equiv -\frac{mp^{r-1}}{kp^{s-1}} \binom{-mp^{r-1}-1}{kp^{s-1}-1} \equiv -\frac{mp^{r-s}}{k} \binom{-mp^{r-s}-1}{k-1}$$

$$\equiv \binom{-mp^{r-s}}{k} \pmod{p^{2r-2s}}.$$

Hence (13) equals

$$\sum_{k=0}^{mp^{r-s}}{}' \left(\sum_{\lambda=1}^{kp^s}{}' \frac{1}{\lambda} \right) \binom{mp^{r-s}-1}{k}^2 \binom{-mp^{r-s}}{k} (-1)^k \pmod{p^{2r}}$$

$$\equiv -mp^{r-s} \sum_{k=0}^{mp^{r-s}-1}{}' \frac{1}{k} \left(\sum_{\lambda=1}^{kp^s}{}' \frac{1}{\lambda} \right)$$

$$\times \binom{mp^{r-s}-1}{k}^2 \binom{-mp^{r-s}-1}{k-1} (-1)^k \pmod{p^{2r}}.$$

We now apply Lemma 3(ii) with

$$a_k = \frac{p^{-s}}{k} \sum_{\lambda=1}^{kp^s}{}' \frac{1}{\lambda} \qquad \text{if } p \nmid k, \qquad a_k = 0 \qquad \text{if } p \mid k,$$

to show that the latter summation is zero mod p^r, as required. To this end it suffices to show that $\sum_{[kp^{-t}]=n} a_k \equiv 0 \pmod{p^t}$ for all $t \in \mathbb{N}$. Since

$$\sum_{[kp^{-t}]=n} a_k = \sum_{[kp^{-t}]=n}{}' \frac{1}{k} \sum_{\lambda=1}^{kp^s}{}' \frac{1}{\lambda}$$

this is true according to Lemma 4(ii). Thus we have completed the proof. Q.E.D.

ACKNOWLEDGMENT

I want to express my gratitude to J. Stienstra whose guidance in the theory of formal groups has been very inspiring and has deepened my interest in the congruences.

REFERENCES

1. F. BEUKERS, Irrationality of π^2, periods of an elliptic curve and $\Gamma_1(5)$, *in* "Proc. Luminy Conf.," Progress in Math. Vol 31, pp. 47–66, Birkhäuser, Basel, 1983.
2. F. BEUKERS AND C. PETERS, A family of K3-surfaces and $\zeta(3)$, *J. Reine Angew. Math.* **351** (1984), 42–54.
3. J. STIENSTRA AND F. BEUKERS, On the Picard–Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces, *Math. Annalen* **271** (1985), 269–304.
4. S. CHOWLA, J. COWLES, AND M. COWLES, Congruence properties of Apéry numbers, *J. Number Theory* **12** (1980), 188–190.
5. B. DWORK, Norm residue symbol in local number fields, *Abh. Math. Sem. Univ. Hamburg* **22** (1958), 180–190.
6. I. GESSEL, Some congruences for Apéry numbers, *J. Number Theory* **14** (1982), 362–368.
7. M. HAZEWINKEL, "Formal Groups and Applications," Academic Press, New York, 1978.

8. Y. Mimura, Congruence properties of Apéry numbers, *J. Number Theory* **16** (1983), 138–146.
9. A. J. van der Poorten, A proof that Euler missed...Apéry's proof of the irrationality of $\zeta(3)$, *Math. Intelligencer* **1** (1979), 195–203.
10. C. Radoux, Quelques propriétés arithmétiques des nombres d'Apéry, *C. R. Acad. Sci. Paris* **A291** (1980), 567–569.