



**Centrum voor Wiskunde en Informatica**  
Centre for Mathematics and Computer Science

---

M.J. Coster

Supercongruences

The Centre for Mathematics and Computer Science is a research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a nonprofit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands Organization for the Advancement of Research (N.W.O.).

# Supercongruences

Matthijs J. Coster

Centre for Mathematics and Computer Science  
P.O. Box 4079, 1009 AB Amsterdam, the Netherlands

## ABSTRACT.

In this report we will discuss special congruences. We explain how the congruences arise from formal groups and then we give some examples.

Key Words & phrases: (Super-)Congruences, Formal Groups, Conjecture of Atkin and Swinnerton-Dyer.  
1985 Mathematics Subject Classification: 14L05, 11B99

## 1. INTRODUCTION.

This paper deals with so called "supercongruences". Before we will explain this term, we give some definitions which we need in the explanation. Let  $K$  be an algebraic extension of  $\mathbb{Q}$ . Let  $p$  be a prime which splits in  $K$  as  $p = \pi\bar{\pi}$ . Let  $|\cdot|_p$  be the valuation on  $\mathbb{Q}$  in such a way that  $|\bar{\pi}|_p = 1$  and  $|\pi|_p = p^{-1}$ . We will consider  $\pi$  as an element of  $\mathbb{Z}_p$ . Let  $\{u_n\}_{n=1}^{\infty}$  be a sequence of rational or  $p$ -adic integers. In this paper we will consider the congruences

$$u(mp^r) \equiv a \cdot u(mp^{r-1}) \pmod{p^{\lambda r}}, \quad (1A)$$

and

$$u(mp^r) \equiv \alpha \cdot u(mp^{r-1}) \pmod{\pi^{\lambda r}}, \quad (1B)$$

where  $\lambda, m, r$  are positive integers and  $a$  is an integer and  $\pi$  is a  $p$ -adic integer.

Therefore (1A) is a congruence in  $\mathbb{Z}$  and (1B) is a congruence in  $\mathbb{Z}_p$ . In section 2 we will give an introduction in formal groups. We will show that congruences (1A) and (1B) with  $\lambda = 1$  arise in a natural way from formal groups. Especially, we will give a sketch of the Conjecture of Atkin and Swinnerton-Dyer. In section 3, 4 and 5 we give some examples of congruences (1A) and (1B) with coefficient  $\lambda > 1$ . In such cases we call the congruence *supercongruence*. At the moment supercongruences cannot be proved by use of formal groups. In each case a separated proof has to be given. A lot of proofs will be omitted in this paper. For these proofs we refer to [12]. In section 6 some conjectures are given.

## 2. THE CONJECTURE OF ATKIN AND SWINNERTON-DYER.

Let  $K$  be a commutative field with  $\text{char}(K) = 0$  and let  $R$  be a subring. (In our case we will choose  $R = \mathbb{Z}_p$ ). We denote by  $R[[T]]$  the set of power series in the variable  $T$  with coefficients in  $R$ .

Let  $F(X,Y) \in R[[X,Y]]$ . We call  $F(X,Y)$  a commutative formal group law if  $F(X,Y)$  satisfies the following properties.

$$\begin{aligned} F(X,Y) &= X+Y+(\text{terms of degree } \geq 2), \\ F(X,F(Y,Z)) &= F(F(X,Y),Z), \\ F(X,Y) &= F(Y,X). \end{aligned} \tag{2}$$

We derive from (2) that  $F(X,Y)$  satisfies moreover the following properties.

$$\begin{aligned} F(X,0) &= X, \\ \text{there is a unique } i(T) \in R[[T]] &\text{ such that } F(T,i(T)) = 0. \end{aligned}$$

Let  $\mathfrak{R}_T = \{X(T) \in R[[T]] : X(0) = 0\}$ . We define a formal addition  $+_{\mathfrak{F}}$  on  $\mathfrak{R}_T$  by

$$X(T) +_{\mathfrak{F}} Y(T) = F(X(T),Y(T)).$$

It turns out that  $\mathfrak{R}_T$  with  $+_{\mathfrak{F}}$  is a group. This group is called a formal commutative group in one variable over  $R$ . From now on let  $\mathfrak{F}$  be a formal group over  $R$  (i.e.

$$\mathfrak{F} = (\mathfrak{R}_T, +_{\mathfrak{F}}).$$

We define the logarithm  $f(T)$  of the formal group  $\mathfrak{F}$  by

$$\begin{aligned} f(T) &\in K[[T]], \\ f(T) &= T+(\text{terms of degree } \geq 2), \\ f(F(X,Y)) &= f(X)+f(Y). \end{aligned} \tag{3}$$

The last condition can be replaced by

$$F(X,Y) = f^{-1}(f(X)+f(Y)) ,$$

where  $f^{-1}(T) \in K[[T]]$  is the power series such that  $f^{-1}(f(T)) = T$ . We find that  $f(T)$  satisfies the property

$$f(T) = \sum_{n=1}^{\infty} \frac{u(n)}{n} T^n \text{ with } u(n) \in R. \quad (4)$$

We call

$$\omega = f'(T)dT \quad (5)$$

the differential form related to the formal group  $\mathcal{F}$ . We consider the formal Dirichlet series

$$L(s, \mathcal{F}) = \sum_{n=1}^{\infty} \frac{u(n)}{n^s} \quad (6)$$

where  $\mathcal{F}(T) = \sum_{n=1}^{\infty} u_n T^n / n$  is the logarithm of the formal group  $\mathcal{F}$ .

Two formal groups  $\mathcal{F}$  (with  $f$  and  $L(s, \mathcal{F})$ ) and  $\mathcal{G}$  (with  $g$  and  $L(s, \mathcal{G})$ ) are isomorphic over  $R$  if there is a formal group homomorphism  $h: \mathcal{F} \rightarrow \mathcal{G}$  with  $h(T) \in R[[T]]$  and  $h(F(X, Y)) = G(h(X), h(Y))$ . In our case (that

$\text{char}(K) = 0$ ) we have  $h(T) = g^{-1}(f(T))$  and  $L(s, \mathcal{F})/L(s, \mathcal{G}) = \sum_{n=1}^{\infty} \frac{v(n)}{n^s}$ , with  $|v(n)|_p \leq |n|_p$ .

We have a theorem due to Honda which says that for each formal group  $\mathcal{F}$  there exists a formal group  $\mathcal{G}$  such that the Dirichlet series related to  $\mathcal{G}$  has  $p$ -adic numbers as coefficients. In formula:

**Theorem 1. (Honda).** *Let  $\mathcal{F}$  be a formal group over  $\mathbb{Z}_p$ . Then there exists a formal group  $\mathcal{G}$ , isomorphic to  $\mathcal{F}$  over  $\mathbb{Z}_p$  such that*

$$L(s, \mathcal{G}) = \frac{1}{1 - \sum_{j=1}^{\infty} p^{j-1-j^s} b(j)} \quad (7)$$

where  $b(j)$  are  $p$ -adic integers.

**Proof.** See [20, pp. 441-445] or [12, pp. 18-23]. ■

**Corollary 2.** *Let  $\mathcal{F}$  be a formal group over  $\mathbb{Z}_p$ . Let  $f(T) = \sum_{n=1}^{\infty} u(n) \cdot T^n / n$  be the related formal group. Then there exists  $p$ -adic numbers  $b(j)$  such that*

$$u(mp^r) - b(1) \cdot u(mp^{r-1}) - \dots - p^{r-1} \cdot b(r) \cdot u(m) \equiv 0 \pmod{p^r}, \quad (8)$$

for  $m, r$  positive integers and  $p$  is not a divisor of  $m$ .

**Proof.** See [20, pp. 441-445]. ■

We will apply Theorem 1 and Corollary 2 on formal groups related to elliptic curves. Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{Z}$  and let  $\omega$  be a holomorphic differential form on  $\mathcal{E}$ . Let  $\mathcal{F}_\omega$  be the formal group related to  $\omega$ . Suppose that  $\mathcal{F}_\omega$  is a formal group over  $\mathbb{Z}$ . Let

$$L_p(s) = (1 - a_p \cdot p^{-s} + p \cdot b_p \cdot p^{-2s})^{-1}$$

be the Dirichlet series related to the Hasse-Weil zeta-function of the elliptic curve. Then a theorem of Honda Cartier and Hill says that the formal series related to the Dirichlet series is isomorphic to the formal group  $\mathcal{F}_\omega$ .

**Corollary 3. (Conjecture of Atkin and Swinnerton-Dyer).** *Let  $\mathcal{F}_\omega$  be the formal group as defined above.*

(i) *We have*

$$u(mp^r) - a_p \cdot u(mp^{r-1}) + p \cdot b_p \cdot u(mp^{r-2}) \equiv 0 \pmod{p^r}. \quad (9)$$

(ii) *If  $\mathcal{E}$  is ordinary over  $\mathbb{Z}_p$  (i.e.  $b_p = 1$  and  $a_p \neq 0$ ) then we have*

$$u(mp^r) \equiv \bar{\pi} \cdot u(mp^{r-1}) \pmod{p^r}, \quad (10)$$

where  $\bar{\pi}$  such that  $|\bar{\pi}|_p = 1$  and  $\bar{\pi}$  is a root of  $X^2 - a_p X + 1 = 0$ .

**Proof.** (i) Corollary 2 says that (9) must be a congruence of form (8). Then we use the theorem of Honda Cartier and Hill, which was mentioned above. This theorem says that the coefficients  $b(1)$  and  $b(2)$  coincide with the integers  $a_p$  and  $b_p$  of the Dirichlet series and that the other coefficients  $b(n)$  equal zero.

(ii) Notice that

$$L_p(s) = (1 - \pi \cdot p^{-s})^{-1} \cdot (1 - \bar{\pi} \cdot p^{-s})^{-1}.$$

It is not difficult to see that the formal group related to  $L_p(s)$  is isomorphic to the formal group which is related to the Dirichlet series  $(1 - \bar{\pi} \cdot p^{-s})^{-1}$ . (See [20]). ■

### 3. GENERALIZED APÉRY NUMBERS.

The numbers  $b(n) = \sum_{k=1}^n \binom{n}{k}^2 \cdot \binom{n+k}{k}$  and  $d(n) = \sum_{k=1}^n \binom{n}{k}^2 \cdot \binom{n+k}{k}^2$  were introduced by Roger Apéry and played a role in the proof of the irrationality of  $\zeta(2)$  and  $\zeta(3)$  respectively. Many papers deal with congruences on these numbers. We mention Chowla, Cowles and Cowles [9] and Gessel [16]. For these numbers Mimura [21] proved some congruences of the form  $u_{p-1} \equiv 1 \pmod{p^3}$ , where  $p$  is a prime,  $p \geq 5$ . F. Beukers [4] generalized these congruences to

$$u(mp^r - 1) \equiv u(mp^{r-1} - 1) \pmod{p^{3r}},$$

where  $m$  and  $r$  are any positive integers. Now we consider the so called *generalized Apéry numbers*, which are defined by

$$w_{AB\varepsilon}(n) = \sum_{k=1}^n \binom{n}{k}^A \cdot \binom{n+k}{k}^B \cdot \varepsilon^k \quad (11)$$

where  $A, B \in \mathbb{Z}_{\geq 0}$  and  $\varepsilon = \pm 1$ .

We have for the generalized Apéry numbers the following theorem.

**Theorem 4.** *Let  $w(n)$  be as defined above. Let  $p \geq 5$  be a prime. Then for any  $m, r \in \mathbb{Z}_{\geq 1}$  we have*

$$w(mp^r) \equiv w(mp^{r-1}) \pmod{p^{3r}} \text{ for } \begin{cases} A \geq 2 \\ A = 1 \text{ and } B \geq 1, \varepsilon = -1 \end{cases}$$

and

$$w(mp^r - 1) \equiv w(mp^{r-1} - 1) \pmod{p^{3r}} \text{ for } \begin{cases} B \geq 2 \\ B = 1 \text{ and } A \geq 1, \varepsilon = (-1)^A. \end{cases}$$

**Proof.** The proof is very technical. See [12, pp. 49-55]. ■

### 4. BINOMIAL COEFFICIENTS.

Since the work of Fermat it is known that every prime  $p \equiv 1 \pmod{4}$  can be written as  $p = a^2 + b^2$  for integers  $a$  and  $b$  in an essentially unique way. Without loss of generality we may assume that  $a \equiv 1 \pmod{4}$ . Gauss proved by counting the number of solutions of the elliptic curve  $\mathcal{E}: Y^2 = X^4 + 1 \pmod{p}$  in two, essentially different ways, that

$$\left(\frac{\frac{p-1}{2}}{\frac{p-1}{4}}\right) \equiv 2a \pmod{p} \quad (12)$$

By applying Corollary 3 on the elliptic curve  $\mathfrak{E}$ , congruence (12) can be generalized to

$$\left(\frac{\frac{mp^r-1}{2}}{\frac{mp^r-1}{4}}\right) \equiv (a+bi) \cdot \left(\frac{\frac{mp^{r-1}-1}{2}}{\frac{mp^{r-1}-1}{4}}\right) \pmod{p^r} \quad (13)$$

where  $m, r$  are positive integers and  $m \equiv 1 \pmod{4}$ . Here  $i$  denotes a  $p$ -adic integer such that  $i^2 = -1$  and  $bi \equiv -a \pmod{p}$ . Beukers conjectured in [4] the congruence

$$\left(\frac{-\frac{1}{2}}{\frac{p-1}{4}}\right) \equiv (a+bi) \pmod{p^2} \quad (14)$$

This was proved by Chowla, Dwork and Evans [10]. Van Hamme [18] generalized (14) to

$$\left(\frac{-\frac{1}{2}}{\frac{p^r-1}{4}}\right) \equiv (a+bi) \cdot \left(\frac{-\frac{1}{2}}{\frac{p^{r-1}-1}{4}}\right) \pmod{p^r} \quad (15)$$

for any positive integer  $r$ . This congruence can be generalized to the supercongruence

$$\left(\frac{\frac{mp^r-1}{2}}{\frac{mp^r-1}{4}}\right) \equiv (a+bi) \cdot \left(\frac{\frac{mp^{r-1}-1}{2}}{\frac{mp^{r-1}-1}{4}}\right) \pmod{p^{2r}} \quad (16)$$

We get another example by considering primes  $p \equiv 1 \pmod{3}$ . Then  $4p = e^2 + 3f^2$  for certain values  $e$  and  $f$ . Without loss of generality we may assume that  $e \equiv -1 \pmod{3}$ . Choose the  $p$ -adic number  $\bar{\pi} = (e + 3f\sqrt{3})/2$  such that  $|\bar{\pi}|_p = 1$ . Starting from the elliptic curve  $\mathfrak{E}: Y^2 = 1 - 4X^3$ , Corollary 3 implies the congruence

$$\left(\frac{\frac{2}{3}(mp^r-1)}{\frac{1}{3}(mp^r-1)}\right) \equiv \bar{\pi} \cdot \left(\frac{\frac{2}{3}(mp^{r-1}-1)}{\frac{1}{3}(mp^{r-1}-1)}\right) \pmod{p^r} \quad (17)$$

for any positive integers  $m, r$  with  $m \equiv 1 \pmod{3}$ . However congruence (17) can be improved to the supercongruence



$$\binom{\frac{2}{3}(mp^r - 1)}{\frac{1}{3}(mp^r - 1)} \equiv \bar{\pi} \cdot \binom{\frac{2}{3}(mp^{r-1} - 1)}{\frac{1}{3}(mp^{r-1} - 1)} \pmod{p^{2r}} \quad (18)$$

In the general case we define for  $\alpha, \beta$  positive integers with  $\alpha + \beta \leq d$  the binomial coefficient

$$v(n) = \begin{cases} \binom{\frac{(\alpha + \beta)(n-1)}{d}}{\frac{\alpha(n-1)}{d}} & \text{if } n \equiv 1 \pmod{d} \\ 0 & \text{else.} \end{cases} \quad (19)$$

We have for these coefficients the congruence

$$v(mp^r) \equiv \bar{\pi} \cdot v(mp^{r-1}) \pmod{p^r} \quad (20)$$

where  $\bar{\pi} = \frac{\Gamma_p(\frac{\alpha}{d})\Gamma_p(\frac{\beta}{d})}{\Gamma_p(\frac{\alpha + \beta}{d})}$ .

This result can be found using formal group theory (namely  $f(T) = \sum_{n=1}^{\infty} \frac{v(n)}{n} \cdot T^n$  is a formal logarithm over  $\mathbb{Z}_p$  for  $p \equiv 1 \pmod{d}$ ) or the  $p$ -adic  $\Gamma$ -function (cf. [22, pp. 111-114]). In the case that  $d = 2, 3, 4$  or  $6$  we can improve congruence (20). The following theorem deals with the improvement.

**Theorem 5.** *Let  $d$  be 2, 3, 4 or 6. Let  $p$  be a prime with  $p \equiv 1 \pmod{d}$ . Let  $m$  and  $r$  be positive integers with  $m \equiv 1 \pmod{d}$ . Let  $\alpha, \beta \in \mathbb{Z}_{\geq 1}$  with  $\alpha + \beta \leq d$ . Then the binomial coefficient  $v(n)$  satisfies the supercongruence*

$$v(mp^r) \equiv g(p)^{mp^{r-1}} \cdot \bar{\pi} \cdot v(mp^{r-1}) \pmod{p^{2r}} \quad (21)$$

where  $g(p) \in \mathbb{Z}_p$  with  $g(p) \equiv 1 \pmod{p}$  and  $\bar{\pi} = \frac{\Gamma_p(\frac{\alpha}{d})\Gamma_p(\frac{\beta}{d})}{\Gamma_p(\frac{\alpha + \beta}{d})}$ .

**Proof.** We prove congruence (21) using the  $p$ -adic  $\Gamma$ -function. The proof is based on a formula of Gross and Koblitz [17] which expresses the  $p$ -adic  $\Gamma$ -function in terms of Gauss sums and on a formula of Diamond [14] which expresses the logarithmic derivative in terms of the  $p$ -adic logarithm. See [11]. ■

## 6. VALUES OF THE LEGENDRE POLYNOMIALS.

This section contains joined work with L. van Hamme. Nice supercongruences exist for the values of some Legendre polynomials. These polynomials can be defined by

$$P_n(t) = \sum_{k=0}^n \binom{n}{k} \cdot \binom{n+k}{k} \cdot \left(\frac{t-1}{2}\right)^k \quad (22)$$

and they satisfy

$$F(X) = \frac{1}{\sqrt{1-2tX+X^2}} = \sum_{n=0}^{\infty} P_n(t)X^n \quad (23)$$

Let  $K$  be an algebraic extension of  $\mathbb{Q}$ . Let  $p$  be a prime which splits in  $K$  as  $p = \pi\bar{\pi}$ . Let  $t \in K$  with  $|t|_p \leq 1$  and consider the differential form

$$\frac{dX}{\sqrt{1-2tX^2+X^4}} = \sum_{n=0}^{\infty} P_n(t)X^n dX \quad (24)$$

on the elliptic curve  $\mathfrak{E} : y^2 = x(x^2 + Ax + B)$ . The theory of formal groups predicts a congruence of the form as described in Corollary 3

$$P_{\frac{1}{2}(mp^{r-1}-1)}(t) \equiv \bar{\pi} \cdot P_{\frac{1}{2}(mp^{r-1}-1)}(t) \pmod{p^r} \quad (25)$$

for any positive integer  $r$  and positive odd integer  $m$ .

It turns out that if  $\mathfrak{E}$  has complex multiplication, congruence (25) can be changed into a congruence mod  $\pi^{2r}$ . We have the following theorem.

**Theorem 6.** *Let  $K = \mathbb{Q}(\sqrt{-d})$  with  $d$  a square-free positive integer. Consider the elliptic curve*

$$\mathfrak{E} : y^2 = x(x^2 + Ax + B) \text{ with } A, B \in K. \quad (26)$$

*Let  $\omega$  and  $\omega'$  be periods of  $\mathfrak{E}$  and suppose that  $\tau = \omega'/\omega$  (which implies the complex multiplication),  $\tau$  has positive imaginary part and  $A = 3\wp(\omega/2)$ , where  $\wp(z)$  is the Weierstrass  $\wp$ -function. Let  $p$  be an odd prime which does not divide  $d$  and let*

*$\pi, \bar{\pi} \in \mathbb{Q}(\sqrt{-d})$  such that  $p = \pi\bar{\pi}$ . Suppose that  $\omega = u + v\tau$  and  $\omega\tau = x + y\tau$  with  $u, v, x, y$  integers and  $v$  even. Then we have*

$$P_{\frac{1}{2}(mp^{r-1}-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \equiv \varepsilon^{mp^{r-1}} \cdot \bar{\pi} \cdot P_{\frac{1}{2}(mp^{r-1}-1)}\left(\frac{A}{\sqrt{\Delta}}\right) \pmod{p^r} \quad (27)$$

where  $\Delta = A^2 - 4B$  and  $\varepsilon = i^{y(1-x)+p-2}$ .

We first give an example in which Theorem 6 can be applied.

Let  $\mathfrak{E} : y^2 = x(x^2 + 3x + 2)$ . We can choose periods  $\omega$  and  $\omega'$  in such a way that  $\wp(\omega/2) = 1$  and  $\omega'/\omega = \tau = i$ . Let  $p \equiv 1 \pmod{4}$  be a prime. Let  $i$  be a  $p$ -adic number such that  $i^2 = -1$ . Fix the sign of  $bi$  such that  $a \equiv bi \pmod{p}$ . Let  $\pi = a - bi$ . Then we have  $\pi\tau = \pi i = b + ai$ . Hence  $\varepsilon = i^{y(1-x)+p-2} = i^{-b} = (-1)^{(p-1)/4}$ . We denote

$a(n) = \sum_{k=1}^n \binom{n}{k} \cdot \binom{n+k}{k}$ . The numbers  $a(n)$  have been used for proving that  $\log 2$  is irrational with measure of irrationality 4.622 [1]. Carlitz proved that the numbers  $a(n)$  satisfy for  $p \equiv 1 \pmod{4}$  the congruence

$$a\left(\frac{p-1}{2}\right) \equiv (-1)^{\frac{1}{4}(p-1)} \cdot 2a \pmod{p}. \quad (28)$$

Since  $a(n) = P_n(3)$ , we have for those primes the supercongruence

$$a\left(\frac{mp^r-1}{2}\right) \equiv (-1)^{\frac{1}{4}(p-1)} \cdot \bar{\pi} \cdot a\left(\frac{mp^{r-1}-1}{2}\right) \pmod{p^{2r}}. \quad (29)$$

Another proof of this supercongruence in the case  $m = r = 1$  has been given by van Hamme in [18].

**Sketch of the proof of Theorem 6.** Let  $L = \mathbb{Q}(\sqrt{-d}, i)$  and  $R = \{\alpha \in L : \text{ord}_{\pi}(\alpha) \geq 0\}$ . In this proof we will denote

$$c(n) = \sqrt{\Delta}^n \cdot P_n\left(\frac{A}{\sqrt{\Delta}}\right). \quad (30)$$

We consider the holomorphic differential form  $\omega = -\frac{dx}{2y}$ . Let  $t = \frac{x}{y}$  be a local parameter at infinity. We express  $\omega$  in terms of  $t$  and we get

$$\omega = \frac{dt}{\sqrt{1 - 2At^2 + \Delta t^4}} = \sum_{n=0}^{\infty} c(n) \cdot t^{2n} dt. \quad (31)$$

Then we define the local parameter  $z$  at infinity by

$$dz = \omega. \quad (32)$$

Hence  $z$  can be expressed as a function of  $t$  by

$$z = \sum_{k=0}^{\infty} \frac{c(k)}{2k+1} t^{2k+1} \quad (33)$$

and  $t$  can be expressed as a function of  $z$  by

$$t = z + \dots = -2 \cdot \frac{\wp(z) - \wp(\frac{\omega}{2})}{\wp'(z)}. \quad (34)$$

Notice that  $t(z)$  is an elliptic function. Since  $\mathfrak{E}$  has complex multiplication we have  $\pi \in \text{End}(\mathfrak{E})$ . More specified we have

$$\begin{aligned} t(\pi z) &= F(t(z)) \\ &= \eta t^p(z) \cdot \frac{1 + \pi a_2 t^{-2}(z) + \pi a_4 t^{-4}(z) + \dots + \pi a_{p-1} t^{1-p}(z)}{1 - \pi d_2 t^{-2}(z) - \pi d_4 t^{-4}(z) + \dots - \pi d_{p-1} t^{1-p}(z)} \end{aligned} \quad (35)$$

where  $\eta, a_i, d_j \in R$ . This formula is due to Weber (cf. [23]). Formula (33) imply the formulas

$$\pi z = \sum_{l=0}^{\infty} \frac{c(l)}{2l+1} t^{2l+1}(\pi z) \quad (36)$$

and

$$\pi z = \sum_{k=0}^{\infty} \pi \cdot \frac{c(k)}{2k+1} t^{2k+1}. \quad (37)$$

Substitute (35) for  $t(\pi z)$  in (36). Consider in equations (36) and (37) the coefficient of  $t^{mp^r} \bmod \frac{\pi p^{2r}}{mp^r}$ . We get the coefficients

$$\frac{1}{mp^{r-1}} \cdot c\left(\frac{1}{2}(mp^{r-1} - 1)\right) \cdot \eta^{mp^{r-1}} \quad (38)$$

and

$$\frac{\pi}{mp^r} \cdot c\left(\frac{1}{2}(mp^r - 1)\right) \quad (39)$$

respectively from formulas (36) and (37) respectively. This implies the congruence of the theorem. We can calculate that  $\eta = i^{y(1-x)+p-2} \cdot (\sqrt{\Delta})^{\frac{1}{2}(p-1)}$ . See a more detailed proof in [13]. ■

There are only 8 values  $t$  with these nice supercongruences over  $\mathbb{Z}$  (cf. [12, pp. 87-89]).

## 6. CONCLUSION.

In section 5 we introduced the numbers  $a(n)$ , which are generalised Apéry numbers. They satisfy supercongruence (29). The numbers  $a(n)$  are related to an elliptic curve. The Apéry numbers  $b(n)$  and  $d(n)$  as defined in section 4 are related to  $K3$  surfaces (cf. [7]). They satisfy other congruences which are comparable to congruence (29), namely

$$b\left(\frac{mp^r - 1}{2}\right) \equiv (a + bi)^2 \cdot b\left(\frac{mp^{r-1} - 1}{2}\right) \pmod{p^r} \quad (40)$$

and

$$d\left(\frac{mp^r - 1}{2}\right) \equiv \bar{\pi} \cdot d\left(\frac{mp^{r-1} - 1}{2}\right) \pmod{p^r} \quad (41)$$

where  $a+bi$  is as defined in section 4 and  $\bar{\pi}$  is a root of some polynomial of degree 3 (see [6] or [24]). Beukers and Stienstra conjectured in [6] and [7] the supercongruences

$$b\left(\frac{mp^r - 1}{2}\right) \equiv (a + bi)^2 \cdot b\left(\frac{mp^{r-1} - 1}{2}\right) \pmod{p^{2r}} \quad (42)$$

and

$$d\left(\frac{mp^r - 1}{2}\right) \equiv \bar{\pi} \cdot d\left(\frac{mp^{r-1} - 1}{2}\right) \pmod{p^{2r}}. \quad (43)$$

Van Hamme [19] proved (42) in the case that  $m = r = 1$ . Recently Young [24] proved (43) in the case that  $m = r = 1$ . The rest of the conjectures is at the moment unproved. Perhaps, the proof of Theorem 4 gives a good possibility to prove the rest of the conjectures.

## 7. REFERENCES.

- [1] K. Alladi and M.L. Robinson: *On certain values of the logarithm*, Lecture Notes **751**, 1-9.
- [2] R. Apéry: Irrationalité de  $\zeta(2)$  et  $\zeta(3)$ , *Astérisque* **61** (1979), 11-13.
- [3] A.O.L. Atkin and H.P.F. Swinnerton-Dyer: *Modular forms on noncongruence subgroups*, Proc. of Symposia in Pure Math., A.M.S. **19** (1971), 1-25.
- [4] F.Beukers: *Arithmetical properties of Picard-Fuchs equations*, *Séminaire de théorie des nombres*, Paris 82-83, Birkhäuser Boston, 1984, 33-38.
- [5] F. Beukers: *Some congruences for the Apéry numbers*, *J. Number Theory* **21** (1985), 141-150.
- [6] F. Beukers: *Another congruence for the Apéry numbers*, *J. Number Theory* **25** (1987), 201-210.
- [7] F. Beukers and J. Stienstra: *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces*, *Math. Annalen* **271** (1985), 293-304.
- [8] L. Carlitz: *Advanced problem 4268*, *A.M.M.* **62** (1965) p. 186 and *A.M.M.* **63** (1956) 348-350.
- [9] S. Chowla, J. Cowles and M. Cowles: *Congruence properties of Apéry numbers*, *J. Number theory* **12** (1980), 188-190.
- [10] S. Chowla, B. Dwork and R.J. Evans: *On the mod  $p^2$  determination of  $\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$* , *J. Number theory* **24** (1986), 188-196.
- [11] M.J. Coster: *Generalisation of a congruence of Gauss*, *J. Number theory* **29** (1988), 300-310.
- [12] M.J. Coster: *Supercongruences*, [Thesis] Univ. of Leiden, the Netherlands, 1988.
- [13] M.J. Coster and L. van Hamme: *Supercongruences of Atkin and Swinnerton-Dyer type for Legendre polynomials*, submitted to *J. of Number Theory*.
- [14] J. Diamond: *The  $p$ -adic log gamma function and  $p$ -adic Euler constants*, *Trans. Amer. Math. Soc.* **233** (1977), 321-337.
- [15] C.F. Gauss: *Arithmetische Untersuchungen (Disquisitiones arithmeticae)*, [Book] Chelsea Publishing Company Bronx, New York, reprinted 1965.
- [16] I. Gessel: *Some congruences for Apéry numbers*, *J. Number theory* **14** (1982), 362-368.
- [17] B. Gross and M. Koblitz: *Gauss sums and the  $p$ -adic  $\Gamma$ -function*, *Ann. Math.* **109** (1979), 569-581.
- [18] L. van Hamme: *The  $p$ -adic gamma function and congruences of Atkin and Swinnerton-Dyer*, *Groupe d'étude d'analyse ultramétrique*, 9<sup>e</sup> année 81/82, Fasc. 3 no. J17-6p.
- [19] L. van Hamme: *Proof of a conjecture of Beukers on Apéry numbers*, *Proceedings of the conference of  $p$ -adic analysis*, Hengelhof, Belgium (1986), 189-195.

- [20] M. Hazewinkel: *Formal groups and applications*, [Book] Academic Press, New York, 1978.
- [21] Y. Mimura: *Congruence properties of Apéry numbers*, J. Number theory **16** (1983), 138-146.
- [22] W.H. Schikhof: *Ultrametric calculus*, [Book] Cambridge University Press, Cambridge, 1984.
- [23] H. Weber: *Lehrbuch der Algebra*, [Book] dritter dand, Friedrich Vieweg und Sohn, Braunschweig, 1908.
- [24] P.T. Young: *Further congruences for the Apéry numbers*, to appear, 1989.

