UNIVERSITATIS IAGELLONICAE ACTA MATHEMATICA, FASCICULUS XLV
2007

INTEGRAL DIFFERENTIALS AND FERMAT CONGRUENCES

by Ernst Kunz and Rolf Waldi

Abstract. For an odd prime number p let k be the p-th cyclotomic number field over $\mathbb{Q}$, A its ring of integers, $X_p := \operatorname{Proj} A[X_0, X_1, X_2]/(X_1^p + X_2^p - X_0^p)$ the p-th Fermat scheme over A, $\bar{X}_p$ its normalisation and $\omega^1_{\bar{X}_p/A}$ the sheaf of regular differentials of $\bar{X}_p/A$. We give an explicit description of its A-module $H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A})$ of global sections and study its relation to the module $D^1_s(\frac{K_p}{A})$ of integral differentials of the Fermat field $K_p = k(x, y)$ $(x^p + y^p = 1)$ introduced by Bost [**2**]. The two modules are equal if and only if the Fermat congruence $x^p + y^p \equiv 1 \bmod p^2$ has at most two solutions $(x, y) \in \mathbb{N}^2$ with $1 \leq x, y \leq p - 1$.

1. Introduction. Let p be an odd prime number, $k := \mathbb{Q}[\zeta]$ the p-th cyclotomic number field, where ζ is a primitive p-th root of unity, $A := \mathbb{Z}[\zeta]$ the ring of integers of k and $K_p := k(x, y)$ with $x^p + y^p = 1$ the p-th Fermat field.

We study the module of integral differentials $D^1_s(\frac{K_p}{A})$ introduced (in much greater generality) by Bost [**2**]. It is defined as follows: Let V be the set of all discrete valuation rings R with quotient field K_p such that R is essentially of finite type over A, and let

$$V_s := \{R \in V | R \text{ is smooth over} A\}.$$

Smoothness means that the module of Kähler differentials $\Omega^1_{R/A}$ is free (necessarily of rank 1). Then

$$D^1_s(\frac{K_p}{A}) := \bigcap_{R \in V_s} \Omega^1_{R/A},$$

the intersection being taken inside $\Omega^1_{K_p/k}$. It turns out that this A-module is connected to Fermat congruences of order 2

$$x^p + y^p \equiv 1 \bmod p^2.$$

Let $N(p)$ be the number of all $(x, y) \in \mathbb{N}^2$ with $1 \le x, y \le p-1$ which solve the congruence. We consider the following as the main observation of this paper (see 5.2 for a more general assertion):

THEOREM 1. *Let* $\pi := \zeta - 1, w := \frac{x+y-1}{\pi}$ *and* $\omega := \frac{dx}{y^{p-1}} = -\frac{dy}{x^{p-1}}$. *Then* $x^i w^k \frac{\omega}{\pi} \in D_s^1(\frac{K_p}{A})$ *for* $i + k \le p - 3$. *We have*

$$D_s^1(\frac{K_p}{A}) = (\bigoplus_{i+k \le p-3} Ax^i w^k)\frac{\omega}{\pi}$$

if and only if $N(p) \le 2$.

For its proof we have first to determine the $R \in V_s$ and their modules of differentials which will be done in Section 2 in a slightly more general situation. In our considerations the normalization $\bar{X}_p$ of the Fermat scheme $X_p := \mathrm{Proj} A[X_0, X_1, X_2]/(X_1^p + X_2^p - X_0^p)$ over A plays an important role. It will be studied in Section 3. If $\omega^1_{\bar{X}_p/A}$ is the sheaf of regular differentials of $\bar{X}_p/A$ we find (3.9)

THEOREM 2. $H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A}) = (\bigoplus_{i+k \le p-3} Ax^i w^k)\frac{\omega}{\pi}$.

For technical reasons we have to investigate the behaviour of D_s^1 under base change which is done in Section 4. The proof of Theorem 1 is given in Section 5.

For informations about Fermat congruences we refer to the book [**5**] of Ribenboim, in particular to Chapter X: The local and modular Fermat problem, pp. 287–358. It mentions that Klösgen [**3**] has computed $N(p)$ for the prime numbers $p < 20000$. He found that more than 84 percent of these p satisfy $N(p) \le 2$. The smallest p with $N(p) > 2$ is 59. In fact, $N(59) = 12$.

Finally, let us introduce some notation which will be valid in the whole text. For a local ring R we write $\mathfrak{m}_R$ for its maximal ideal and $\mathfrak{k}(R)$ for its residue field. If R is a discrete valuation ring, then v_R denotes the normed discrete valuation associated with it. If $\mathfrak{p}$ is a maximal ideal in a Dedekind ring A, then $v_{\mathfrak{p}}$ is the valuation belonging to $A_{\mathfrak{p}}$. Further $Q(R)$ denotes the quotient field of a domain R. For an ideal I in a noetherian ring $h(I)$ denotes its height.

2. Smooth discrete valuation rings of Fermat fields over number fields. We start with somewhat more general assumptions than those formulated in the introduction.

ASSUMPTIONS 2.1. Let k be an algebraic number field, A its ring of integers and

$$K_m := k(x, y) \ (x^m + y^m = 1, m \ge 3),$$

the m-th Fermat field over k. Let $V = V(k)$ be the set of all discrete valuation rings R with $Q(R) = K_m$ which are essentially of finite type over A, and let

$$V_s = V_s(k) := \{R \in V | R \text{ is smooth over } A\}.$$

For a prime number p with $p|m$ we set $V_s(p) := \{R \in V_s | p \in \mathfrak{m}_R\}$.

Given $R \in V_s$ let $R' := R \cap k(x)$. This is a discrete valuation ring with $Q(R') = k(x)$. If $\mathfrak{m}_R \cap A = (0)$, then $\mathfrak{m}_{R'} \cap A = (0)$, i.e., $k \subset R'$. If $\mathfrak{m}_R \cap A := \mathfrak{p} \in \mathrm{Max}A$, then due to the smoothness of R over A we have $\mathfrak{m}_R = \pi R$ with a prime element π of $A_\mathfrak{p}$. Then $\mathfrak{m}_{R'} = \pi R'$.

To describe R' and its module of differentials more precisely it suffices to consider the R' with $x \in R$. Otherwise, $\tilde{x} \in R$, where $\tilde{x} := \frac{1}{x}$, and with $\tilde{y} := \frac{y}{x}$ we have $\tilde{x}^m - \tilde{y}^m = 1$. The considerations in this case are similar to those in case $x \in R$. The following cases can occur:

a) $k \subset R'$: Then $R' = k[x]_{(f)}$ with an irreducible $f \in k[x]$. Clearly, R' is smooth over A and $\Omega^1_{R'/A} = R'dx$.
b) $\mathfrak{m}_{R'} \cap A[x] = \mathfrak{p}A[x]$ with $\mathfrak{p} \in \mathrm{Max}A$: Then $R' = A[x]_{\mathfrak{p}A[x]}$. Again R' is smooth over A and $\Omega^1_{R'/A} = R'dx$.
c) $\mathfrak{m}_{R'} \cap A[x] \in \mathrm{Max}A[x]$: Then $\mathfrak{m}_{R'} \cap A[x] = (\mathfrak{p}, f)$ with $\mathfrak{p} \in \mathrm{Max}A$ and an $f \in A[x]$ which is irreducible mod$\mathfrak{p}A[x]$. Thus R' dominates the 2-dimensional regular local ring $R_0 := A[x]_{(\mathfrak{p},f)}$. We can form the sequence

$$R_0 \subset R_1 \subset \cdots \subset R_t \subset R'$$

of quadratic transformations $R_i \subset R_{i+1}$ $(i = 0, \dots, t-1)$ along R' which consists of 2-dimensional regular local rings R_i. Then there exists a smallest $t \in \mathbb{N}$ such that $\mathfrak{m}_{R'} \cap R_t$ is a prime ideal $\mathfrak{P}$ of height 1 so that $R' = (R_t)_\mathfrak{P}$. In greater generality this was proved by Abhyankar [**1**], Proposition 1, see also [**4**], Proposition 2.1 for a proof in our situation. It follows that R' is essentially of finite type and smooth over A. We call the above seqence *the quadratic sequence* that connects $A[x]$ with R' and call t its *length.* In [**4**], 2.1 it is also shown that

$$\Omega^1_{R'/A} = R'\frac{dx}{\pi^t},$$

where π is a prime element of $A_\mathfrak{p}$.

In case b) the last formula holds true with $t = 0$ which we also call the length of the quadratic sequence in that case.

In any case $R \cap k(x)$ is an element of the set $V'_s = V'_s(k)$ of all discrete valuation rings R' with $Q(R') = k(x)$ which are essentially of finite type and smooth over A, and any $R' \in V'_s$ belongs to one of the cases a)–c).

Now we have to deal with the question: Which $R' \in V'_s$ are dominated by rings $R \in V_s$, and how do these R arise from R'?

The elements $R \in V_s \setminus \bigcup_{p|m} V_s(p)$ are easy to determine. If $\mathfrak{m}_R \cap A = (0)$, i.e., $k \subset R$, then R is a local ring of the Fermat curve $x^m + y^m = 1$ over k and

$$\Omega^1_{R/A} = \begin{cases} R\omega & \text{if } x \in R, \\ R\tilde{\omega} & \text{if } x \notin R, \end{cases}$$

where

$$\omega := \frac{dx}{y^{m-1}} = -\frac{dy}{x^{m-1}}, \ \tilde{\omega} := \frac{d\tilde{x}}{\tilde{y}^{m-1}} = \frac{d\tilde{y}}{\tilde{x}^{m-1}} = -x^{m-3}\omega.$$

Suppose $\mathfrak{m}_R \cap A =: \mathfrak{p} \in \mathrm{Max}A$ with $m \notin \mathfrak{p}$ and $x \in R$. Let $\mathfrak{p}A_\mathfrak{p} = \pi A_\mathfrak{p}$ with a prime element π of $A_\mathfrak{p}$, and let $R' := R \cap k(x)$. Then

$$R'[y]/\mathfrak{p}R'[y] = \mathfrak{k}(R')[Y]/(Y^m + \xi^m - 1),$$

where ξ denotes the residue of x in $\mathfrak{k}(R')$. Since the characteristic of $\mathfrak{k}(R')$ does not divide m, the polynomial $Y^m + \xi^m - 1$ is separable over $\mathfrak{k}(R')$, hence $R'[y]/\mathfrak{p}R'[y]$ is a direct product of separable extension fields of $\mathfrak{k}(R')$. If $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ are the maximal ideals of $R'[y]$ corresponding to the factors of $R'[y]$, then the $R'[y]_{\mathfrak{m}_i}$ are elements of V_s, and R is one of these rings. Moreover, since $\mathfrak{k}(R)/\mathfrak{k}(R')$ is separable algebraic and y a unit of R, we have

$$\Omega^1_{R/A} = R \otimes_{R'} \Omega^1_{R'/A} = R\frac{dx}{\pi^t} = R\frac{\omega}{\pi^t},$$

where t is the length of the quadratic sequence connecting $A[x]$ with R'.

It remains to consider the $R \in V_s(p)$, where p is a prime number with $p|m$. Again $\mathfrak{m}_R \cap A =: \mathfrak{p}$ is a maximal ideal of A. We have $p = \epsilon\pi^e$ with a prime element π, a unit ϵ of $A_\mathfrak{p}$ and the ramification index e of $A_\mathfrak{p}$ over $\mathbb{Z}_{(p)}$. Assume that $x \in R$, write $m = p^\nu m'$ with $p \nmid m'$ and set $z := x^{m'} + y^{m'} - 1$. By the binomial theorem, the Fermat equation $x^m + y^m = 1$ can be written

$$z^{p^\nu} + \sum_{i=1}^{p^\nu - 1} \binom{p^\nu}{i} z^{p^\nu - i}(1 - x^{m'})^i + ph_\nu(x) = 0, \tag{1}$$

where

$$h_\nu(x) := \frac{1}{p}((x^{m'})^{p^\nu} + (1 - x^{m'})^{p^\nu} - 1). \tag{2}$$

Again by the binomial theorem

$$h_\nu(x) = \begin{cases} \frac{1}{p}\sum_{i=1}^{p^\nu - 1} \binom{p^\nu}{i}(-x^{m'})^i & \text{if } p \neq 2, \\ (x^{m'})^{2^\nu} + \frac{1}{2}\sum_{i=1}^{2^\nu - 1}\binom{2^\nu}{i}(-x^{m'})^i & \text{if } p = 2. \end{cases} \tag{3}$$

Proposition 2.2. *We always have $v_R(z) > 0$. Moreover, $v_R(h_\nu(x)) = 0$ if and only if $p^\nu v_R(z) = e$.*

Proof. In equation (1) all terms other than z^{p^ν} have positive value, hence also $v_R(z) > 0$. The terms $\binom{p^\nu}{i} z^{p^\nu - i}(1 - x^{m'})^i$ $(i = 1, \dots, p^\nu - 1)$ have value

$$(p^\nu - i)v_R(z) + (\nu - v_p(i))e + iv_R(1 - x^{m'}) \geq e + (p^\nu - i)v_R(z).$$

If $v_R(h_\nu(x)) = 0$, then e is the unique smallest value of the terms of (1) other than z^{p^ν}, hence $p^\nu v_R(z) = e$. Conversely, if this equation holds, then e is the unique smallest value of the terms other than $ph_\nu(x)$, and it follows that $v_R(h_\nu(x)) = 0$. □

Corollary 2.3. *If p^ν does not divide e, then each $R \in V_s(p)$ dominates one of the rings $R' = A[x]_{(\mathfrak{p},f)}$ with $\mathfrak{p} \in MaxA, p \in \mathfrak{p}$ and $f \in A[x]$, where the reduction $\bar{f} \in A/\mathfrak{p}[x]$ of f is one of the irreducible factors of the reduction $\bar{h}_\nu(x)$ of $h_\nu(x)$.*

The assumption of the corollary is trivially satisfied if the primes $p|m$ are unramified in A, in particular if $k = \mathbb{Q}$. On the other hand, let k be the m-th cyclotomic number field. The decomposition law for such fields implies that

$$e = p^{\nu-1}(p-1),$$

hence the corollary can be applied in this case too.

Now the question arises whether the $R' \in V'_s$ which dominate an $A[x]_{(\mathfrak{p},f)}$ as in the corollary are dominated by some $R \in V_s(p)$.

Among the divisors of $h_\nu(x)$ are $x^{m'}$ and $1 - x^{m'}$. Writing the Fermat equation in the form

$$(y^{m'})^{p^\nu} + \sum_{i=1}^{p^\nu} \binom{p^\nu}{i} (x^{m'} - 1)^i = 0 \tag{4}$$

we see

Lemma 2.4. *For $R \in V_s(p)$ we have $v_R(x^{m'} - 1) > 0$ if and only if $v_R(y) > 0$. There exists $R \in V_s(p)$ with $v_R(x^{m'} - 1) > 0$ if and only if there exists $R^* \in V_s(p)$ with $v_{R^*}(x) > 0$.*

We get R^* from R by applying the k-automorphism of K_m which exchanges y and x.

Assumptions 2.5. Under the Assumptions 2.1 let a prime number $p|m$ be given such that $p^2 \nmid m$. Write $m = p \cdot m'$ $(p \nmid m')$. Consider $\mathfrak{p} \in \mathrm{Max}A$ with $p \in \mathfrak{p}$ and suppose the ramification index e of $A_\mathfrak{p}$ over $\mathbb{Z}_{(p)}$ is $p - 1$. Let π be a prime element of $A_\mathfrak{p}$.

For example, if m is squarefree and k the m-th cyclotomic number field, then these assumptions are satisfied for every $p|m$ and $\mathfrak{p} \in \mathrm{Max}A$ with $p \in \mathfrak{p}$ by the decomposition law for such fields.

THEOREM 2.6. *Under the Assumptions 2.5 consider* $R' \in V_s'$ *which dominates* $A_\mathfrak{p}$. *Assume further that* $v_{R'}(x) \geq 0, v_{R'}(x^{m'} - 1) = 0, v_{R'}(h_1(x)) > 0$.
a) The rings $R \in V_s$ *which dominate* R' *are the localizations of* $R'[w, y]$ *at its maximal ideals, where* $w := \frac{z}{\pi} = \frac{x^{m'} + y^{m'} - 1}{\pi}$. *Further*

$$\Omega^1_{R'[w,y]/A} = R'[w, y] \otimes_{R'} \Omega^1_{R'/A} = R'[w, y] \frac{\omega}{\pi^t},$$

where t *is the length of the quadratic sequence connecting* $A[x]$ *with* R'.
b) Let $f \in A[x]$ *be normed, modulo* $\mathfrak{p}$ *irreducible, and let its reduction* $\bar{f}$ *be a factor of the reduction* $\bar{h}_1$ *of* h_1. *Further let* $m' = 1$. *Then* $R' = A_\mathfrak{p}[x][\frac{f}{\pi}]_{(\pi)} \in V_s'$, *and the rings* $R \in V_s$ *which dominate* R' *are the localizations of* $R = R'[w]$ *at its maximal ideals where* $w := \frac{x+y-1}{\pi}$. *Further*

$$\Omega^1_{R'[w]/A} = R'[w] \frac{\omega}{\pi}$$

If in addition $\bar{f}$ *is a simple factor of* $\bar{h}_1$, *then* $R = R'[w] \in V_s(p)$.

PROOF. a) We have $p = \epsilon \pi^{p-1}$ with a unit ϵ of $A_\mathfrak{p}$. Dividing the equation (1) for $\nu = 1$

$$z^p + \sum_{i=1}^{p-1} \binom{p}{i} z^{p-i} (1 - x^{m'})^i + p h_1(x) = 0$$

by π^p, we obtain

$$w^p + \sum_{i=1}^{p-1} \frac{1}{\pi^i} \binom{p}{i} w^{p-i} (1 - x^{m'})^i + \epsilon \frac{h_1(x)}{\pi} = 0. \tag{5}$$

We have $\frac{1}{\pi^i}\binom{p}{i} = \eta_i \pi^{p-1-i}$ $(i = 1, \ldots, p-1)$ with units $\eta_i \in A_\mathfrak{p}$, and by assumption $\frac{h_1(x)}{\pi} \in R'$. Therefore, (5) is an equation of integral dependence for w over R' and hence $w \in R$ for each $R \in V$ which dominates R'.

Further

$$R'[w]/\pi R'[w] = \mathfrak{k}(R')[W]/(W^p + \eta W + \theta)$$

with $\eta \in \mathfrak{k}(R') \setminus \{0\}$, $\theta \in \mathfrak{k}(R')$. It follows that $R'[w]/\pi R'[w]$ is a direct product of separable extension fields of $\mathfrak{k}(R')$. The localizations of $R'[w]$ at its maximal ideals are therefore discrete valuation rings with quotient field $k(x, y^{m'})$ which are smooth over A, and each ring R_0 of this kind which dominates R' is such a localization. Moreover, $R_0[y]/\pi R_0[y] = \mathfrak{k}(R_0)[Y]/(Y^{m'} - \beta)$ with the residue β of $y^{m'}$ in $\mathfrak{k}(R_0)$. Since $v_{R_0}(z) > 0$ and $v_{R_0}(x^{m'} - 1) = 0$, we have $v_{R_0}(y^{m'}) = 0$, hence $\beta \neq 0$. It follows that once again $R_0[y]/\pi R_0[y]$ is a direct product of separable extension fields of $\mathfrak{k}(R_0)$. Therefore, the localizations of $R_0[y]$ at its maximal ideals are elements of V_s, and each $R \in V_s$ is such a localization for a suitable R_0.

In order to verify the assertion about differential modules observe that the localizations of $R'[w,y]$ at its maximal ideals have a residue field which is separable algebraic over $\mathfrak{k}(R')$ which implies the first equation of 2.6a). Further $\Omega^1_{R'/A} = R'\frac{dx}{\pi^t}$. In $R'[w,y]$ the element y is a unit since this is true for each localization of $R'[w,y]$ as $v_{R'}(x^{m'}-1) = 0$. It follows that $R'[w,y]dx = R'[w,y]\omega$.

b) Only the last assertion of b) has to be proved. The residue $\bar{v}$ of $v := \frac{f}{\pi}$ in $\mathfrak{k}(R')$ is transcendental over $\mathfrak{k}(A_{\mathfrak{p}})[\xi]$ where ξ denotes the residue of x. Write

$$h_1(x) = q(x) \cdot f(x) + r(x) \text{ with } q(x), r(x) \in A[x],\ \deg(r) < \deg(f).$$

Then the coefficients of $r(x)$ are divisible in $A_{\mathfrak{p}}$ by π. The residue of $\frac{h_1(x)}{\pi}$ is of the form $\bar{q}(\xi)\bar{v} + \rho(\xi)$ with $\rho(x) \in \mathfrak{k}(A_{\mathfrak{p}})[x]$, and $\bar{q}(\xi) \neq 0$ since $\bar{f}$ is a simple factor of $\bar{h}_1$. In the polynomial $W^p + \eta W + \theta$ we have $\eta \in \mathfrak{k}(A_{\mathfrak{p}})[\xi]$, and θ is a linear polynomial in $\bar{v}$ over this ring. It follows that $W^p + \eta W + \theta$ is irreducible over $\mathfrak{k}(R')$, and $R'[w]$ is the only element of $V_s(p)$ that dominates R'. This completes the proof of b). $\square$

For $R \in V_s(p)$ with $v_R(x^{m'}-1) > 0$ we have $v_R(y) > 0$ by 2.4. Such R are given as in 2.6 where we have to replace x by y and where it suffices to consider $f = y$. It remains to consider the $R' \in V'_s$ which dominate $A_{\mathfrak{p}}$ and for which $v_{R'}(\tilde{x}) > 0$. With $\tilde{z} := \tilde{x}^{m'} - \tilde{y}^{m'} - 1$ the Fermat equation can be written as follows

$$\tilde{z}^p + \sum_{i=1}^{p-1} \binom{p}{i} \tilde{z}^{p-i}(1-\tilde{x}^{m'})^i + ph_1(\tilde{x}) = 0.$$

Analogous to 2.6 is

Theorem 2.7. *Let $v_{R'}(\tilde{x}) > 0$.*

a) The localizations of $R'[\tilde{w},\tilde{y}]$ with $\tilde{w} := \frac{\tilde{z}}{\pi}$ at its maximal ideals are the rings $R \in V_s$ which dominate R'. We have

$$\Omega^1_{R'[\tilde{w},\tilde{x}]/A} = R'[\tilde{w},\tilde{y}]\frac{\tilde{\omega}}{\pi^t}$$

with t as in 2.6.

b) If $m' = 1$ and $\tilde{R}' = A_{\mathfrak{p}}[\frac{\tilde{x}}{\pi}]_{(\pi)}$, then there exists exactly one $\tilde{R} \in V_s(p)$ which dominates $\tilde{R}'$, namely $\tilde{R} = \tilde{R}'[\tilde{w}]$ with $\tilde{w} := \frac{\tilde{x}-\tilde{y}-1}{\pi}$.

Assumptions 2.8. Under the Assumptions 2.5 let $m' = 1$ and suppose that k contains a primitive p-th root of unity ζ and $\pi := \zeta - 1$ is a prime element of $A_{\mathfrak{p}}$.

These assumptions are satisfied for example if k is the p-th cyclotomic number field and $m = p$.

THEOREM 2.9. *Let $R \in V_s(p)$ be the ring which dominates $R' := A_{\mathfrak{p}}[\frac{y}{\pi}]_{(\pi)}$, that is $R = R'[w]$ with $w := \frac{x+y-1}{\pi}$. Then we also have*

$$R = A_{\mathfrak{p}}[\frac{x-1}{\pi}]_{(\pi)}[w]$$

and R is the only element of $V_s(p)$ which dominates $A_{\mathfrak{p}}[\frac{x-1}{\pi}]_{(\pi)}$.

PROOF. Clearly $A_{\mathfrak{p}}[\frac{x-1}{\pi}]_{(\pi)} \subset R$. We show at first that the residue $\bar{v}$ of $v := \frac{x-1}{\pi}$ in $\mathfrak{k}(R)$ is transcendental over $\mathbb{F}_p$. Since

$$y^p + \prod_{j=0}^{p-1}(x - \zeta^j) = 0$$

and $v_R(y) = 1$, we have $v_R(\prod_{j=0}^{p-1}(x - \zeta^j)) = p$, hence $v_R(x - \zeta^j) > 0$ for at least one $j \in \{0, \ldots, p-1\}$. However,

$$(x - \zeta^j) - (x - \zeta^k) = \zeta^k - \zeta^j = (\zeta - 1)\varphi_{jk}(\zeta),$$

where $\varphi_{jk}(\zeta)$ is a unit of $A_{\mathfrak{p}}$. Since $\zeta - 1$ is a prime element of $A_{\mathfrak{p}}$ it follows that $v_R(x - \zeta^j) = 1$ for all $j = 0, \ldots, p-1$. The equation

$$(\frac{y}{\pi})^p + \prod_{j=0}^{p-1}\frac{x - \zeta^j}{\pi} = 0$$

shows that the residue in $\mathfrak{k}(R)$ of least one of the $\frac{x-\zeta^j}{\pi}$ must be transcendental over $\mathfrak{k}(A_{\mathfrak{p}})$. But

$$\frac{x - \zeta^j}{\pi} - \frac{x - \zeta^k}{\pi} = \varphi_{jk}(\zeta)$$

implies that all these residues are transcendental over $\mathfrak{k}(A_{\mathfrak{p}})$, in particular, so is $\bar{v}$.

It follows that $A_{\mathfrak{p}}[\frac{x-1}{\pi}]_{(\pi)}[w] \subset R$. Set $R'' := A_{\mathfrak{p}}[\frac{x-1}{\pi}]_{(\pi)}$. Equation (5) shows that the minimal polynomial of the residue of w in $\mathfrak{k}(R'')$ has the form $W^p + \theta$, where θ is transcendental over $\mathfrak{k}(A_{\mathfrak{p}})$, since $x - 1$ is a simple factor of $\bar{h}_1(x)$ as $\bar{h}_1'(1) \neq 0$. Therefore, R is the only element of $V_s(p)$ which dominates R'', that is $R = R''[w]$. □

Under the Assumptions 2.8 all $R \in V_s(p)$ are described now as extensions of rings $R' \subset k(x)$ so that it is not necessary to pass from x to y.

3. Normalization of the Fermat scheme. Under the Assumptions 2.1 let

$$X_m := \mathrm{Proj} A[X_0, X_1, X_2]/(X_1^m + X_2^m - X_0^m)$$

be the m-th Fermat scheme over A. We have

$$X_m = \mathrm{Spec} S \cup \mathrm{Spec} \tilde{S}$$

with $S := A[x, y], \tilde{S} := A[\tilde{x}, \tilde{y}]$. Let $M := \{1, m, m^2, \dots\}$.

LEMMA 3.1. $(X_m)_M := A_M \otimes_A X_m$ *is smooth over* A_M *and*

$$\bigcap_{R \in V_s, m \notin \mathfrak{m}_R} \Omega^1_{R/A} = \Omega^1_{S_M/A} \cap \Omega^1_{\tilde{S}_M/A} = (\bigoplus_{i+k \leq m-3} A_M x^i y^k)\omega.$$

PROOF. We have $\Omega^1_{S_M/A} = S_M dX \oplus S_M dY / \langle m x^{m-1} dX + m y^{m-1} dY \rangle$. Here m is a unit of S_M and locally so is x or y. It follows that $\Omega^1_{S_M/A} = S_M \omega$. Similarly $\Omega^1_{\tilde{S}_M/A} = \tilde{S}_M \tilde{\omega}$ with $\tilde{\omega} = \frac{d\tilde{x}}{\tilde{y}^{m-1}} = \frac{d\tilde{y}}{\tilde{x}^{m-1}}$, hence $(X_m)_M$ is smooth over A_M. Since $\tilde{\omega} = -x^{m-3}\omega$, we obtain

$$\Omega^1_{S_M} \cap \Omega^1_{\tilde{S}_M} = (S_M \cap x^{m-3}\tilde{S}_M)\omega = (\bigoplus_{i+k \leq m-3} A_M x^i y^k)\omega$$

as an easy computation shows. Since $(X_m)_M$ is smooth over A_M, we have

$$\bigcap_{R \in V_s, m \notin \mathfrak{m}_R} \Omega^1_{R/A} \subset \Omega^1_{S_M/A} \cap \Omega^1_{\tilde{S}_M/A}.$$

On the other hand, $x^i y^k \omega \in \Omega^1_{R/A}$ $(i + k \leq p - 3)$, if $R \in V_s$ and $m \notin \mathfrak{m}_R$, as we have seen at the beginning of Section 2. $\square$

LEMMA 3.2. *For a prime number* $p|m$ *let* $m = p^\nu \cdot m'$ *with* $p \nmid m'$. *Let* $\mathfrak{P} \in \mathit{Spec} S$ *with* $h(\mathfrak{P}) = 1$ *and* $p \in \mathfrak{P}$ *be given, and set* $z := x^{m'} + y^{m'} - 1, \mathfrak{p} := \mathfrak{P} \cap A$. *Then*

$$\mathfrak{P} = (\mathfrak{p}, z)S.$$

$S_{\mathfrak{P}}$ *is regular if and only if* p *is unramified in* A.

PROOF. Since $p \in \mathfrak{P}$ equation (1) shows that $z \in \mathfrak{P}$. Further $S/\mathfrak{p}S = \mathfrak{k}(A_{\mathfrak{p}})[x, y]/(z^{p^\nu})$ and $S/(\mathfrak{p}, z)S = \mathfrak{k}(A_{\mathfrak{p}})[x, y]/(z)$ is a domain. Hence $(\mathfrak{p}, z)S \in \mathrm{Spec} S$, and since $h(\mathfrak{P}) = 1$, we have $(\mathfrak{p}, z)S = \mathfrak{P}$.

When p is unramified in A, then $\mathfrak{P}S_{\mathfrak{P}} = (p, z)S_{\mathfrak{P}}$. We have $\mathfrak{P} \cap A[x] = \mathfrak{p}A[x]$, and therefore the polynomial $h_\nu(x)$ of equation (1) is a unit of $A[x]_{\mathfrak{p}} \subset S_{\mathfrak{P}}$. Equation (1) shows that $p \in zS_{\mathfrak{P}}$ hence $\mathfrak{P}S_{\mathfrak{P}} = zS_{\mathfrak{P}}$, and $S_{\mathfrak{P}}$ is regular.

Assume now that $p = \epsilon\pi^e$ with a prime element π, a unit ϵ of $A_{\mathfrak{p}}$ and $e > 1$. If $\mathfrak{P}S_{\mathfrak{P}} = (\pi, z)S_{\mathfrak{p}}$ would be a principal ideal, then π or z would generate it. Let $\mathfrak{Q}$ be the preimage of $\mathfrak{P}$ in the polynomial ring $A[x, y]$ and $\bar{\mathfrak{Q}}$ its image in $\mathfrak{k}(A_{\mathfrak{p}})[x, y]$. As neither $S_{\mathfrak{P}}/\pi S_{\mathfrak{P}} = \mathfrak{k}(A_{\mathfrak{p}})[x, y]_{\bar{\mathfrak{Q}}}/(z^{p^\nu})$ nor

$S_{\mathfrak{P}}/zS_{\mathfrak{P}} = A[x,y]_{\mathfrak{Q}}/(ph_\nu(x),z) = A[x,y]_{\mathfrak{Q}}/(\pi^e,z)$ is a field the ring $S_{\mathfrak{P}}$ is certainly singular. □

THEOREM 3.3. *X_m is normal if and only if all prime numbers $p|m$ are unramified in A.*

PROOF. To show normality of X_m it suffices to verify that all local rings $S_{\mathfrak{P}}$ with $\mathfrak{P} \in \mathrm{Spec} S, h(\mathfrak{P}) = 1$ are regular. By symmetry, this is then also true for $\tilde{S}$. If the condition on the prime divisors of m is hurt, then 3.2 shows that X_m is not normal.

If, however, the condition is fulfilled for the $S_{\mathfrak{P}}$ with $h(\mathfrak{P}) = 1$ and $m \in \mathfrak{P}$, then these rings are regular. By 3.1 this is also true for the $S_{\mathfrak{P}}$ with $m \notin \mathfrak{P}$. □

It is clear that X_m is normal for $k = \mathbb{Q}$. If k is the m-th cyclotomic number field, then X_m is not normal. In fact: If m has a prime divisor $p \neq 2$, then p has ramification index $e = p^{\nu-1}(p-1) > 1$. The same is true for $p = 2$ if $m = 2^\nu$ with $\nu > 1$.

ASSUMPTIONS 3.4. Let k be the m-th cyclotomic number field, where m is squarefree. Let $\bar{X}_m$ be the normalisation of X_m.

LEMMA 3.5. *Under the Assumptions 3.4 the 1-dimensional singular local rings of X_m are the $S_{\mathfrak{P}}$ with $\mathfrak{P} \in \mathrm{Spec} S, h(\mathfrak{P}) = 1$ which contain a prime $p \neq 2$ that divides m. With $\mathfrak{p} := \mathfrak{P} \cap A$ we have $\mathfrak{P}S_{\mathfrak{P}} = (\pi, z)S_{\mathfrak{P}}$, where $\mathfrak{p}A_{\mathfrak{p}} = \pi A_{\mathfrak{p}}$, and $\mathfrak{k}(S_{\mathfrak{P}}) = \mathfrak{k}(A_{\mathfrak{p}})(\xi,\eta)$ with $\xi^{m'} + \eta^{m'} = 1$ is the m'-th Fermat field over $\mathfrak{k}(A_{\mathfrak{p}})$.*

PROOF. Since the primes $p \neq 2$ which divide m are ramified in A the local rings mentioned in the lemma are singular by 3.2. The assertion about their maximal ideal and their residue field is clear. Moreover, we have $\mathfrak{P} \cap A[x] = \mathfrak{p}A[x]$, hence x is a unit in $S_{\mathfrak{P}}$, and it follows that $A[\tilde{x}]_{\mathfrak{p}A[\tilde{x}]} \subset S_{\mathfrak{P}}$ and $\tilde{z} := \tilde{x}^{m'} - \tilde{y}^{m'} - 1 \in \mathfrak{P}S_{\mathfrak{P}}$. Therefore, $S_{\mathfrak{P}} = \tilde{S}_{\tilde{\mathfrak{P}}}$ with $\tilde{\mathfrak{P}} := (\mathfrak{p}, \tilde{z})\tilde{S}$, and hence there are no other 1-dimensional singular local rings of X_m but the $S_{\mathfrak{P}}$. □

We want to describe now the normalizations of these rings and their modules of regular differentials over $A_{\mathfrak{p}}$.

THEOREM 3.6. *For $S_{\mathfrak{P}}$ as in 3.5 the blowing up $R := S_{\mathfrak{P}}[u]$ with $u := \frac{\pi}{z}$ is the normalization of $S_{\mathfrak{P}}$. It is a discrete valuation ring with the prime element u, and $\mathfrak{k}(R) = \mathfrak{k}(S_{\mathfrak{P}})$. We have $v_R(z) = p-1,\ v_R(\pi) = p$ and for the Kähler different of $R/A_{\mathfrak{p}}$*

$$\mathfrak{d}_1(R/A_{\mathfrak{p}}) = \pi R.$$

Further for the image $[R, dR]$ of $\Omega^1_{R/A_{\mathfrak{p}}}$ in $\Omega^1_{K_m/k}$ we have

$$[R, dR] = R\frac{\pi}{z^2}\omega$$

and the module of regular differentials of $R/A_{\mathfrak{p}}$ is

$$\omega^1_{R/A_{\mathfrak{p}}} = \mathfrak{d}_1(R/A_{\mathfrak{p}})^{-1}[R, dR] = R\frac{\omega}{z^2}.$$

PROOF. Write $p = \epsilon\pi^{p-1}$ with a unit $\epsilon \in A_{\mathfrak{p}}$. Dividing (1) (with $\nu = 1$) by z^{p-1}, we obtain

$$z + \sum_{i=1}^{p-1} \epsilon_i \pi^{p-i}(1 - x^{m'})^i u^{i-1} + \epsilon h_1(x) u^{p-1} = 0 \tag{6}$$

with units $\epsilon_i \in A_{\mathfrak{p}}$. Since $\mathfrak{P} \cap A[x] = \mathfrak{p}A[x]$, the polynomial $h_1(x)$ is a unit of $S_{\mathfrak{P}}$. Therefore, u is integral over $S_{\mathfrak{P}}$, hence u is contained in each discrete valuation ring of K_m which dominates $S_{\mathfrak{P}}$.

As $\pi = zu \in uS_{\mathfrak{P}}[u]$ we see from (6) that $z \in uS_{\mathfrak{P}}[u]$ and hence

$$S_{\mathfrak{P}}[u]/uS_{\mathfrak{P}}[u] = S_{\mathfrak{P}}/(\pi, z)S_{\mathfrak{P}} = \mathfrak{k}(S_{\mathfrak{p}}).$$

Thus we have shown that $uS_{\mathfrak{P}}[u]$ is a maximal ideal of $S_{\mathfrak{P}}[u]$.

Any maximal ideal of $S_{\mathfrak{P}}[u]$ contains by (6) with π and z also u and is therefore $uS_{\mathfrak{P}}[u]$. It follows that $R := S_{\mathfrak{P}}[u]$ is the normalization of $S_{\mathfrak{P}}$ and a discrete valuation ring with $v_R(u) = 1$ and $\mathfrak{k}(R) = \mathfrak{k}(S_{\mathfrak{P}})$. Using (6), we find $v_R(z) = p - 1$ and $v_R(\pi) = p$.

In order to compute $\Omega^1_{R/A_{\mathfrak{p}}}$ we consider the kernel I of the canonical $S_{\mathfrak{P}}$-epimorphism $S_{\mathfrak{P}}[U] \to S_{\mathfrak{P}}[u]$ $(U \mapsto u)$. We show that

$$I = (zU - \pi, z + g(x, U)),$$

where

$$g(x, U) := \sum_{i=1}^{p-1} \epsilon_i \pi^{p-i}(1 - x^{m'})^i U^{i-1} + \epsilon h_1(x) U^{p-1}.$$

Certainly, $zU - \pi$ and $z + g(x, U)$ are in I. Further

$$S_{\mathfrak{P}}[U]/(U, zU - \pi, z + g(x, U)) = S_{\mathfrak{P}}/(\pi, z) = \mathfrak{k}(S_{\mathfrak{P}}).$$

The residue class $\bar{u}$ of U in $B := S_{\mathfrak{P}}[U]/(zU - \pi, z + g(x, U))$ generates a maximal ideal of B and it is intergral over $S_{\mathfrak{P}}$. As above we see that $\bar{u}B$ is the only maximal ideal of B lying over $\mathfrak{P}S_{\mathfrak{P}}$. It follows that $B = R$ and $I = (zU - \pi, z + g(x, U))$.

We have

$$\Omega^1_{S_{\mathfrak{P}}/A_{\mathfrak{p}}} = S_{\mathfrak{P}}dX \oplus S_{\mathfrak{P}}dY / \langle pm'(x^{m-1}dX + y^{m-1}dY)\rangle.$$

It follows that $\Omega^1_{R/A_{\mathfrak{p}}}$ with respect to the system of generators $\{dx, dy, du\}$ has the relation matrix

$$\begin{bmatrix} pm'x^{m-1} & pm'y^{m-1} & 0 \\ m'x^{m'-1}u & m'y^{m'-1}u & z \\ m'x^{m'-1} + \frac{\partial g}{\partial x}(x,u) & m'y^{m'-1} & \frac{\partial g}{\partial U}(x,u) \end{bmatrix}.$$

Here

$$\frac{\partial g}{\partial x}(x,u) = \sum_{i=1}^{p-1} \epsilon_i \pi^{p-i}(-im')x^{m'-1}(1-x^{m'})^{i-1}u^{i-1} + \epsilon h_1'(x)u^{p-1}$$

and $h_1'(x) = x^{p-1} - (1-x)^{p-1} \notin \mathfrak{p}A[x]$. Hence $h_1'(x)$ is a unit of R and it follows that $v_R(\frac{\partial g}{\partial x}(x,u)) = p-1$. As R has ramification index $p = v_R(\pi)$ over $A_{\mathfrak{p}}$ we have $v_R(\mathfrak{d}_1(R/A_{\mathfrak{p}})) \geq p$. But the minor

$$det \begin{bmatrix} m'x^{m'-1}u & m'y^{m'-1}u \\ m'x^{m'-1} + \frac{\partial g}{\partial x}(x,u) & m'y^{m'-1} \end{bmatrix}$$

of the relation matrix has value $v_R(u\frac{\partial g}{\partial x}(x,u)) = p$. Therefore, $\mathfrak{d}_1(R/A_{\mathfrak{p}}) = \pi R$.

In $[R, dR]$ we have $x^{m-1}dx + y^{m-1}dy = 0$. As $x^{m'} - 1$ is a unit in R so is y and therefore $\frac{x}{y} \in R$. It follows that $dy \in Rdx$. Further

$$[m'x^{m'-1} - m'y^{m'-1}(\frac{x}{y})^{m-1} + \frac{\partial g}{\partial x}(x,u)]dx \in Rdu.$$

The expression in brackets is a unit in R. Therefore,

$$[R, dR] = Rdu = R\frac{\pi}{z^2}dz = R\frac{\pi}{z^2}(x^{m'-1}dx + y^{m'-1}dy) = R\frac{\pi}{z^2}dx = R\frac{\pi}{z^2}\omega$$

and

$$\omega^1_{R/A_{\mathfrak{p}}} = \mathfrak{d}_1(R/A_{\mathfrak{p}})^{-1}[R, dR] = R\frac{\omega}{z^2}.$$

□

ASSUMPTIONS 3.7. Let $m = p$ be an odd prime number, $k = \mathbb{Q}[\zeta]$ the p-th cyclotomic number field, where ζ is a primitive p-th root of unity. Set $\pi := \zeta - 1$, $z := x + y - 1$ and $M := \{1, \pi, \pi^2, \dots\}$.

In this situation $S_{\mathfrak{P}}$ with $\mathfrak{P} = (\pi, z)$ is, by 3.5, the only singular 1-dimensional local ring of X_p. Let $\bar{S}$ denote the integral closure of S in K_p. Then

$$\bar{S} = \bigcap_{\bar{\mathfrak{Q}} \in \mathrm{Spec}\bar{S}, h(\bar{\mathfrak{Q}})=1} \bar{S}_{\bar{\mathfrak{Q}}}.$$

If $\bar{\mathfrak{Q}} \in \mathrm{Spec}\bar{S}$ has height 1, so has $\mathfrak{Q} := \bar{\mathfrak{Q}} \cap S$. There is only one $\mathfrak{Q} \in \mathrm{Spec}S$ with $p \in \mathfrak{Q}$, namely $\mathfrak{Q} = \mathfrak{P}$, and, by 3.6, $S_{\mathfrak{P}}[u]$ with $u := \frac{\pi}{z}$ is the normalization of $S_{\mathfrak{P}}$. Consequently, there is only one $\bar{\mathfrak{P}} \in \mathrm{Spec}\bar{S}$ lying over $\mathfrak{P}$ and $\bar{S}_{\bar{\mathfrak{P}}} = S_{\mathfrak{P}}[u]$. Further $\bar{\mathfrak{P}}$ is uniquely determined by the condition $p \in \bar{\mathfrak{P}}$.

The local rings $\bar{S}_{\bar{\mathfrak{Q}}}$ with $p \notin \bar{\mathfrak{Q}}$ are localizations of S_M which, by 3.1, is smooth over A, and each localization of S_M at a prime of height 1 is such an $\bar{S}_{\bar{\mathfrak{Q}}}$. It follows that

$$\bar{S} = S_M \cap S_{\mathfrak{P}}[u].$$

Analogously for the normalization $\bar{\tilde{S}}$ of $\tilde{S}$

$$\bar{\tilde{S}} = \tilde{S}_M \cap S_{\mathfrak{P}}[u].$$

Up to $S_{\mathfrak{P}}$ resp. $R := S_{\mathfrak{P}}[u]$ the schemes X_p and $\bar{X}_p$ have the same 1-dimensional local rings.

Proposition 3.8. $\bar{S} = A[x] \oplus A[x]z \oplus A[x]\frac{z^2}{\pi} \oplus \cdots \oplus A[x]\frac{z^{p-1}}{\pi^{p-2}}$.

Proof. We have $\bar{S} = \{s \in S_M | v_R(s) \geq 0\}$ by the above. By 3.5,

$$v_R(z) = p-1,\ v_R(\pi) = p,\ v_R(u) = 1.$$

Therefore,

$$v_R(\frac{z^k}{\pi^{k-1}}) = (p-1)k - p(k-1) = p-k \qquad (k = 1, \ldots, p-1)$$

and the above direct sum is contained in $\bar{S}$. Any $s \in S_M = A_M[x,z]$ can be written as

$$s = \varphi_0 + \varphi_1 z + \varphi_2 \frac{z^2}{\pi} + \cdots + \varphi_{p-1}\frac{z^{p-1}}{\pi^{p-2}}$$

with $\varphi_k = \sum_i b_{ik}x^i \in A_M[x], b_{ik} \in A_M$. The $v_R(\frac{z^k}{\pi^{k-1}})$ are the numbers of $\{0, \ldots, p-1\}$ while the $v_R(\varphi_k)$ are divisible by p. Therefore, if $v_R(s) \geq 0$, then $v_R(\varphi_k) \geq 0$ for $k = 0, \ldots, p-1$. But $\mathfrak{k}(R) = \mathfrak{k}(A_{\mathfrak{p}})(x)$ with $\mathfrak{p} := \mathfrak{P} \cap A$, where x is transcendental over $\mathfrak{k}(A_{\mathfrak{p}})$. It follows that $b_{ik} \in A_{\mathfrak{p}} \cap A_M = A$ for all i, k which proves 3.8. $\square$

Theorem 3.9. *Under the assumptions 3.7 let $\omega^1_{\bar{X}_p/A}$ be the sheaf of regular differentials of $\bar{X}_p$ over A. Then*

$$H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A}) = (\bigoplus_{i+k \leq p-3} Ax^i w^k)\frac{\omega}{\pi},$$

where $w := \frac{z}{\pi}$.

Proof. The sheaf $\omega^1_{\bar{X}_p/A}$ is reflexive: We have $\omega^1_{\bar{S}/A} \cong \mathrm{Hom}_{A[x]}(\bar{S}, A[x])$, and this is a reflexive $\bar{S}$-module, similarly for $\bar{\tilde{S}}$. Therefore, for the global sections

$$H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A}) = \bigcap_{P \in \bar{X}_p, \dim \mathcal{O}_P = 1} \omega^1_{\mathcal{O}_P/A}.$$

The $\mathcal{O}_P$ with $\dim\mathcal{O}_P = 1$ and $p \notin \mathfrak{m}_P$ are the 1-dimensional local rings of $(X_p)_M$. From 3.1 and 3.6 we obtain with $R := S_{\mathfrak{P}}[u]$

$$H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A}) = (\bigoplus_{i+k\le p-3} A_M x^i y^k)\omega \cap \omega^1_{R/A} = (\bigoplus_{i+k\le p-3} A_M x^i z^k)\omega \cap R\frac{\omega}{z^2}$$
$$= (\bigoplus_{i+k\le p-3} A_M x^i z^k \cap R\frac{\pi}{z^2})\frac{\omega}{\pi}.$$

An element $\sum_{i+k\le p-3} b_{ik}x^i z^k$ with $b_{ik} \in A_M$ is in $R\frac{\pi}{z^2}$ if and only if

$$v_R(\frac{z^2}{\pi}\sum_{i+k\le p-3} b_{ik}x^i z^k) = v_R(\sum_{k=0}^{p-3}(\sum_{i=0}^{p-3-k}\pi^k b_{ik}x^i)\frac{z^{k+2}}{\pi^{k+1}}) \ge 0.$$

With a similar argument as in the Proof of 3.8 this is the case if and only if $\pi^k b_{ik} \in A$ for all i,k with $i+k \le p-3$, and it follows that

$$H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A}) = (\bigoplus_{i+k\le p-3} Ax^i w^k)\frac{\omega}{\pi}.$$

□

4. Base change. Under the Assumptions of 2.1 let l be a finite extension field of k with ring of integers B and let $L_m := l(x,y)$ $(x^m + y^m = 1)$ be the Fermat field over l. The set $V_s(l)$ is defined analogously as $V_s(k)$. We want to compare $D^1_s(\frac{K_m}{A}) := \bigcap_{R\in V_s(k)} \Omega^1_{R/A}$ with $D^1_s(\frac{L_m}{B}) := \bigcap_{T\in V_s(l)} \Omega^1_{T/B}$.

LEMMA 4.1. *For $R \in V_s(k)$ let $\mathfrak{M}$ be a maximal ideal of $B\otimes_A R$. Then*

$$T := (B\otimes_A R)_{\mathfrak{M}} \in V_s(l) \text{ and } \Omega^1_{T/A} = B\otimes_R \Omega^1_{R/A}.$$

PROOF. The assertion about differential modules is clear. Therefore, $\Omega^1_{T/B}$ is a free T-module of rank 1, and T is smooth over B. □

If $T \in V_s(l)$ is of the form $(B\otimes_A R)_{\mathfrak{M}}$ with $R \in V_s(k), \mathfrak{M} \in \mathrm{Max}(B\otimes_A R)$ we say that T arises from R by base change. In general, this need not be the case. However, we have

LEMMA 4.2. *For $T \in V_s(l)$ let $\mathfrak{P} := \mathfrak{m}_T \cap B \in MaxB$ and $\mathfrak{p} := \mathfrak{P}\cap A$. If $B_{\mathfrak{P}}$ is unramified over $A_{\mathfrak{p}}$, then $R := T\cap k(x,y) \in V_s(k)$, and T arises from R by base change.*

PROOF. Since $B_{\mathfrak{p}}$ is unramified over $A_{\mathfrak{p}}$, it follows that T is smooth over A. Then $R' := T\cap k(x)$ is essentially of finite type over $A_{\mathfrak{p}}$ ([**4**], 2.1). Therefore, R is essentially of finite type over $A_{\mathfrak{p}}$. From $\mathfrak{m}_T = \mathfrak{p}T \subset \mathfrak{m}_R T \subset \mathfrak{m}_T$ we obtain $\mathfrak{p}R = \mathfrak{m}_R$, hence the smoothness of R over A. We have $B\otimes_A R \subset T, \mathfrak{m}_T \cap B\otimes_A R =: \mathfrak{M} \in \mathrm{Max}(B\otimes_A R)$, and it follows that $T = (B\otimes_A R)_{\mathfrak{M}}$. □

Proposition 4.3. *Suppose the Fermat scheme X_m over A is normal. Then all $T \in V_s(p)$ with $p|m$ arise from rings $R \in V_s(\mathbb{Q})$ by base change.*

Proof. By 3.3 all prime numbers p with $p|m$ are unramified in A, therefore 4.2 can be applied. $\square$

The rings $R \in V_s(\mathbb{Q})$ and their modules of differentials have been described in [**4**], 3.8–3.11, so that the $T \in V_s(k)$ are also known by the above, if X_m is normal. Alternately it is possible to repeat the arguments of [**4**] to give an analogous description of the $T \in V_s(k)$ in case X_m is normal.

Proposition 4.4. *a) We always have*

$$D_s^1(\frac{L_m}{B}) \subset B \otimes_A D_s^1(\frac{K_m}{A}).$$

b) If all $B_{\mathfrak{P}}$ with $\mathfrak{P} \in MaxB$ and $m \in \mathfrak{P}$ are unramified over $A_{\mathfrak{p}}$, where $\mathfrak{p} = \mathfrak{P} \cap A$, then we have equality in a).

Proof. a) By 3.1, we have

$$D_s^1(\frac{K_m}{A}) = (\bigoplus_{i+k \leq m-3} A_M x^i y^k)\omega \cap \bigcap_{R \in V_s(k), m \in \mathfrak{m}_R} \Omega^1_{R/A}$$

and there is an analogous formula for $D_s^1(\frac{L_m}{B})$. We write $T \downarrow R$ if $T \in V_s(l)$ arises from $R \in V_s(k)$ by base change. Then $\bigcap_{T \downarrow R} \Omega^1_{T/B} = B \otimes_A \Omega^1_{R/A}$ and hence

$$D_s^1(\frac{L_m}{B}) \subset B \otimes_A (\bigoplus_{i+k \leq m-3} A_M x^i y^k)\omega \cap \bigcap_{R \in V_s(k), m \in \mathfrak{m}_R} B \otimes_A \Omega^1_{R/A}$$

$$= B \otimes_A [(\bigoplus_{i+k \leq m-3} A_M x^i y^k)\omega \cap \bigcap_{R \in V_s(k), m \in \mathfrak{m}_R} \Omega^1_{R/A}] = B \otimes_A D_s^1(\frac{K_m}{A}).$$

b) If the condition of unramifiedness is satisfied, then, by 4.2, all $T \in V_s(l)$ with $v_T(m) > 0$ arise from rings $R \in V_s(k)$ by base change, and the above inclusion becomes an equality. $\square$

Corollary 4.5. *In the situation of 4.4b) differentials $\eta_1, \ldots, \eta_s \in \Omega^1_{K_m/k}$ form a system of generators (a basis) of the A-module $D_s^1(\frac{K_m}{A})$ if and only if they form a system of generators (a basis) of the B-module $D_s^1(\frac{L_m}{B})$.*

This is clear since B is faithfully flat over A.

Corollary 4.6. *Let $K_m^0 := \mathbb{Q}(x, y)$ $(x^m + y^m = 1)$ be the m-th Fermat field over $\mathbb{Q}$. If the Fermat scheme X_m is normal, then*

$$D_s^1(\frac{K_m}{A}) = A \otimes_{\mathbb{Z}} D_s^1(\frac{K_m^0}{\mathbb{Z}}).$$

Lemma 4.7. *Let p be an odd prime number, $k = \mathbb{Q}[\zeta]$ the p-th cyclotomic number field with a primitive p-th root ζ of unity and $\pi := \zeta - 1$. Then*

$$\frac{\omega}{\pi} \in D_s^1(\frac{K_p}{A}) \text{ and } \frac{\tilde{\omega}}{\pi} \in D_s^1(\frac{K_p}{A}).$$

Proof. Let $R \in V_s$ be given. If $p \notin \mathfrak{m}_R$, then clearly $\frac{\omega}{\pi} \in \Omega^1_{R/A}$ and $\frac{\tilde{\omega}}{\pi} \in \Omega^1_{R/A}$ by what was said about $\Omega^1_{R/A}$ at the beginning of Section 2. If $R \in V_s(p)$ and $x \in R$, then $\frac{\omega}{\pi} \in \Omega^1_{R/A}$ by 2.6a). Since $\tilde{\omega} = -x^{p-3}\omega$, we also have $\frac{\tilde{\omega}}{\pi} \in \Omega^1_{R/A}$. In case $R \in V_s(p)$ and $x \notin R$ we use 2.7a) to conclude that $\frac{\tilde{\omega}}{\pi} \in \Omega^1_{R/A}$ and $\omega = -\tilde{x}^{p-3}\tilde{\omega}$ to conclude that $\frac{\omega}{\pi} \in \Omega^1_{R/A}$. □

Example 4.8. *Let p be an odd prime number, k the p-th cyclotomic number field and K_p^0 the p-th Fermat field over $\mathbb{Q}$. Then*

$$D_s^1(\frac{K_p}{A}) \neq A \otimes_{\mathbb{Z}} D_s^1(\frac{K_p^0}{\mathbb{Z}}).$$

In fact, by 4.7, $\frac{\omega}{p} \in D_s^1(\frac{K_p^0}{\mathbb{Z}})$. By 2.6, there are rings $T \in V_s(k)$ with $\Omega^1_{T/A} = T\frac{\omega}{\pi}$, hence $\frac{\omega}{p} \notin D_s^1(\frac{K_p}{A})$ since p has ramification index $p-1$ in A.

5. Connection to Fermat congruences.

Assumptions 5.1. Under the Assumptions 3.7 let $\bar{X}_p$ denote the normalization of the Fermat scheme X_p and set $w := \frac{z}{\pi}$. Let $S(p)$ be the set of solutions (x, y) of the Fermat congruence

$$x^p + y^p \equiv 1 \bmod p^2 \text{ with } 1 \leq x, y \leq p-1$$

and $N(p)$ the cardinality of $S(p)$.

It is easy to see that $D_s^1(\frac{K_3}{A}) = A\frac{\omega}{\pi}$ and $N(3) = 0$. In this section we want to prove

Theorem 5.2. *If $p > 3$, then*
a) $H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A}) = (\bigoplus_{i+k \leq p-3} Ax^i w^k)\frac{\omega}{\pi} \subset D_s^1(\frac{K_p}{A})$.
b) We have equality in a) if and only if $N(p) \leq 2$.
c) In the general case the quotient $D_s^1(\frac{K_p}{A})/H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A})$ is an A-module of finite length $\geq N(p) - 2$.

For the proof of a) notice that $\frac{\omega}{\pi}, \frac{\tilde{\omega}}{\pi} \in D_s^1(\frac{K_p}{A})$ by 4.7. For each $R \in V_s(p)$ with $v_R(x) \geq 0$ we have $w \in R$ by 2.6a) and 2.9, hence $x^i w^k \frac{\omega}{\pi} \in \Omega^1_{R/A}$ for these R and all i, k with $i + k \leq p-3$. For $R \in V_s(p)$ with $v_R(\tilde{x}) > 0$ this is also true by 2.7a), since $w = -x\tilde{w}, \omega = -\tilde{x}^{p-3}\tilde{\omega}$ imply $x^i w^k \frac{\omega}{\pi} = (-1)^{k+1}\tilde{x}^{p-3-i-k}\tilde{w}^k\frac{\tilde{\omega}}{\pi}$

for $i+k \leq p-3$. The $R \in V_s \setminus V_s(p)$ also present no problem since π is a unit in such R, and a) follows.

The relation to Fermat congruences comes from the following fact (Ribenboim [**5**], p. 172):

LEMMA 5.3. *Let $\bar{h}_1(x) \in \mathbb{F}_p[x]$ be the reduction of $h_1(x)$ modulo p. Then $N(p)$ is the number of zeros of $\bar{h}_1(x)$ in $\mathbb{F}_p \setminus \{0,1\}$. These zeros are double roots of $\bar{h}_1(x)$ in the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$. All other roots of $\bar{h}_1(x)$ are simple.*

PROOF. The last two assertions are clear since

$$(1-x)h_1'(x) = (1-x)(x^{p-1}-(1-x)^{p-1}) = x^{p-1}-x^p-(1-x)^p \equiv x^{p-1}-1 \bmod p.$$

Let $\tilde{S}(p)$ denote the set of zeros of $\bar{h}_1(x)$ in $\mathbb{F}_p \setminus \{0,1\}$. If $a \in \{2,\dots,p-1\} \subset \mathbb{N}$ is a representative of $\alpha \in \tilde{S}(p)$, then

$$a^p + (p+1-a)^p \equiv a^p + (1-a)^p \equiv 1 \bmod p^2,$$

i.e. $(a, p+1-a) \in S(p)$. Conversely if $(x,y) \in S(p)$, then necessarily $2 \leq x, y \leq p-1$ and $x^p + y^p \equiv 1 \bmod p$. By Fermat's little theorem, we have $x^p + y^p \equiv x + y \bmod p$, hence $x + y \equiv 1 \bmod p$ and $4 \leq x+y \leq 2p-2$. It follows that $y = p+1-x$ and $x^p + (1-x)^p \equiv 1 \bmod p^2$. Thus $(x,y) \mapsto x$ defines a bijection $S(p) \to \tilde{S}(p)$. □

Roughly the smaller $N(p)$ is, the more roots has $\bar{h}_1(x)$, the more $R \in V_s(p)$ exist and the smaller is the intersection of their modules of differentials.

The detailed proof of 5.2b) and c) requires some preparations. Let l be a finite extension field of k with the following property: In the ring B of integers of l there exists a maximal ideal $\mathfrak{P}$ with $\mathfrak{P} \cap A = \mathfrak{p} = (\pi)$ such that $B_{\mathfrak{P}}$ is unramified over $A_{\mathfrak{p}}$ and $\mathfrak{k}(B_{\mathfrak{P}})$ is a splitting field of $\bar{h}_1(x)$ over $\mathfrak{k}(A_{\mathfrak{p}})$. One gains such an l by taking a primitive element τ of a splitting field of $\bar{h}_1(x)$, choosing a normed polynomial $f(x) \in A[x]$ which represents the minimal polynomial of τ over $\mathfrak{k}(A_{\mathfrak{p}})$ and setting $l := k[x]/(f(x))$. Then there is only one maximal ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$, and π is a prime element of $B_{\mathfrak{P}}$.

For the Fermat field $L_p := l(x,y)$ the Assumptions 2.5 are satisfied and hence the Assertions 2.6, 2.7 and 2.9 are applicable, further 4.4b) and 4.5. To prove 5.2b) it suffices therefore to show that $\{x^i w^k \frac{\omega}{\pi}\}_{i+k \leq p-3}$ is a basis of the B-module $D_s^1(\frac{L_p}{B})$ if and only if $N(p) \leq 2$.

LEMMA 5.4. *Let $\beta \in B_{\mathfrak{P}}$ be a representative of a zero $\bar{\beta}$ of $\bar{h}_1(x)$ in $\mathfrak{k}(B_{\mathfrak{P}})$ and $R := R'[w]$ with $R' := B_{\mathfrak{P}}[\frac{x-\beta}{\pi}]_{(\pi)}$. Then if $M = \{1, \pi, \pi^2, \dots\}$*

$$\Big(\bigoplus_{i+k \leq p-3} B_M x^i y^k\Big)\frac{\omega}{\pi} \cap \Omega^1_{R/B} \subset \Omega^1_{R^*/B}$$

for all $R^* \in V_s(l)$ *with* $v_{R^*}(p) > 0$ *and* $v_{R^*}(x-\beta) > 0$. *An analogous assertion is also true for the ring* $\tilde{R} := \tilde{R}'[\tilde{w}]$ *with* $\tilde{w} := \frac{\tilde{x}-\tilde{y}-1}{\pi}$ *lying over* $\tilde{R}' := B_{\mathfrak{P}}[\frac{\tilde{x}}{\pi}]_{(\pi)}$ *and all* $\tilde{R}^* \in V_s(l)$ *with* $v_{\tilde{R}^*}(p) > 0$ *and* $v_{\tilde{R}^*}(\tilde{x}) > 0$.

Proof. By 2.6b) and 2.9, the only rings in $V_s(l)$ which dominate R' are the localizations of R at its maximal ideals, and the same holds true for $\tilde{R}$ and $\tilde{R}'$. Further $\Omega^1_{R/B} = R\frac{\omega}{\pi}$ and $\Omega^1_{\tilde{R}/B} = \tilde{R}\frac{\tilde{\omega}}{\pi}$.

Any $\sigma \in \bigoplus_{i+k\le p-3} B_M x^i y^k$ can be written as $\sigma = \sum_{k=0}^{p-3} \sigma_k w^k$, where

$$\sigma_k = \sum_{i=0}^{p-3-k} b_{ik} x^i \ (b_{ik} \in B_M).$$

Since $\{1, w, \ldots, w^{p-3}\}$ is part of a basis of R over R', we have $\sigma\frac{\omega}{\pi} \in \Omega^1_{R/B}$ if and only if $\sigma_k \in R'$ for $k = 0, \ldots, p-3$. Write

$$\begin{aligned}\sigma_k = \sum_{i=0}^{p-3-k} b_{ik}(x-\beta+\beta)^i &= \sum_{i=0}^{p-3-k} b_{ik} \sum_{j=0}^{i} \binom{i}{j} \beta^{i-j}(x-\beta)^j \\ &= \sum_{j=0}^{p-3-k} \pi^j \Big(\sum_{i\ge j} \binom{i}{j} \beta^{i-j} b_{ik}\Big)\Big(\frac{x-\beta}{\pi}\Big)^j.\end{aligned}$$

The residue class of $\frac{x-\beta}{\pi}$ in $\mathfrak{k}(R')$ is transcendental over $\mathfrak{k}(B_{\mathfrak{P}})$. Therefore, $\sigma_k \in R'$ if and only if for all j, k the following conditions are satisfied

$$G_{jk}(\beta) \qquad v_{\mathfrak{P}}\Big(\sum_{i\ge j} \binom{i}{j} \beta^{i-j} b_{ik}\Big) \ge -j.$$

Now if R^* is given as in the lemma, then R^* is a localization of $R''[w]$ with some $R'' \in V'_s(l)$, where $v_{R''}(x-\beta) > 0$, and we have $\Omega^1_{R^*/B} = R^*\frac{\omega}{\pi^t}$ with some $t \ge 1$. If $G_{jk}(\beta)$ holds for all j, k, then $\sigma_k \in R''$ $(k = 0, \ldots, p-3)$, and it follows that $\sigma\frac{\omega}{\pi} \in \Omega^1_{R^*/B}$.

The proof for $\tilde{R}$ and $\tilde{R}'$ is analogous: As $w = -\tilde{x}^{-1}\tilde{w}$ and $\omega = -\tilde{x}^{p-3}\tilde{\omega}$ we have

$$\sigma\frac{\omega}{\pi} = \Big(\sum_{i+k\le p-3} b_{ik}\pi^{p-3-i-k}\Big(\frac{\tilde{x}}{\pi}\Big)^{p-3-i-k}\tilde{w}^k\Big)\frac{\tilde{\omega}}{\pi}.$$

Since $\{1, \tilde{w}, \ldots, \tilde{w}^{p-3}\}$ is part of a basis of $\tilde{R}$ over $\tilde{R}'$ and the residue class of $\frac{\tilde{x}}{\pi}$ in $\mathfrak{k}(\tilde{R}')$ is transcendental over $\mathfrak{k}(B_{\mathfrak{P}})$, we conclude that $\sigma\frac{\omega}{\pi} \in \Omega^1_{\tilde{R}/B} = \tilde{R}\frac{\tilde{\omega}}{\pi}$ if and only if $b_{ik}\pi^{p-3-i-k} \in B_{\mathfrak{P}}$ that is if and only if the following conditions

$$\tilde{G}_{ik} \qquad v_{\mathfrak{P}}(b_{ik}) \ge -(p-3-i-k) \qquad (i+k \le p-3)$$

are satisfied. Now let $\tilde{R}^* \in V_s(l)$ be such that $v_{\tilde{R}^*}(p) > 0$ and $v_{\tilde{R}^*}(\tilde{x}) > 0$. If the conditions $\tilde{G}_{ik}$ are satisfied, then $v_{\tilde{R}^*}(b_{ik}\tilde{x}^{p-3-i-k}) \ge 0$ for $i+k \le p-3$, hence $\sigma\frac{\omega}{\pi} \in \tilde{R}^*\frac{\tilde{\omega}}{\pi} \subset \Omega^1_{\tilde{R}^*/B}$, and this concludes the proof of Lemma 5.4. □

Assume that $\bar\beta_1, \dots, \bar\beta_r$ are the pairwise different zeros of $\bar h_1(x)$ in $\mathfrak{k}(B_{\mathfrak{P}})$, hence $p-1-r = N(p)$ by Lemma 5.3. With representatives $\beta_i \in B$ of the $\bar\beta_i$ set $R_i' := B_{\mathfrak{P}}[\frac{x-\beta_i}{\pi}]_{(\pi)}$ and $R_i := R_i'[w]$ $(i=1,\dots,r)$. By 3.1, we have

$$\bigcap_{R\in V_s, p\notin \mathfrak{m}_R} \Omega^1_{R/B} = \Big(\bigoplus_{i+k\le p-3} B_M x^i w^k\Big)\frac{\omega}{\pi}.$$

The definition of $D^1_s(\frac{L_p}{B})$, Lemma 5.4 and its proof imply

Lemma 5.5. *a)* $D^1_s(\frac{L_p}{B}) = \big(\bigoplus_{i+k\le p-3} B_M x^i w^k\big)\frac{\omega}{\pi}\big) \cap \bigcap_{s=1}^r \Omega^1_{R_s/B} \cap \Omega^1_{\tilde R/B}$.

b) Let $\sigma = \sum_{i+k\le p-3} b_{ik} x^i w^k$ *with* $b_{ik} \in B_M$ *be given. Then* $\sigma\frac{\omega}{\pi} \in D^1_s(\frac{L_p}{B})$ *if and only if the conditions* $G_{i,k}(\beta_s)$ *and* $\tilde G_{ik}$ *are satisfied* $(i+k \le p-3, s = 1,\dots,r)$.

c) $D^1_s(\frac{L_p}{B})/(\bigoplus_{i+k\le p-3} Bx^i w^k)\frac{\omega}{\pi}$ *is a B-module of finite length.*

Proof of 5.2b) and c). For $1 \le t \le r$ we denote by M_t the van der Monde matrix $(\beta_j^i)_{s=1,\dots,t,\ i=0,\dots,t-1}$. We have $M_t \in Gl_t(B_{\mathfrak{P}})$ as $\bar\beta_1,\dots,\bar\beta_r$ are pairwise different. Let σ be given as in 5.5b).

Assume at first that $N(p) \le 2$. Then by 5.3, the polynomial $\bar h_1(x)$ has at least $p-3$ different roots $\bar\beta_1,\dots,\bar\beta_{p-3}$. If $\sigma\frac{\omega}{\pi} \in D^1_s(\frac{L_p}{B})$, then by 5.5b), in particular the conditions

$$\tilde G_{p-3-k,k} \qquad\qquad b_{p-3-k,k} \in B_{\mathfrak{P}} \qquad (k=0,\dots,p-3)$$

are satisfied. Together with the conditions $G_{0,k}(\beta_s)$ they furnish for each $k = 0,\dots,p-3$ a linear system of equations

$$\sum_{i=0}^{p-3-k-1} \beta_s^i b_{ik} = B_{ks} \qquad (s=1,\dots,p-3-k)$$

with $B_{ks} \in B_{\mathfrak{P}}$ and matrix of coefficients $M_{p-3-k} \in Gl_{p-3-k}(B_{\mathfrak{P}})$. Hence by Cramer's rule, all $b_{ik} \in B_{\mathfrak{P}} \cap B_M = B$, and we have shown that $\{x^i w^k \frac{\omega}{\pi}\}$ is a basis of the B-module $D^1_s(\frac{L_p}{B})$.

Conversely assume now that $N(p) \ge 3$, that is $r < p-3$. By a suitable choice of the $b_{ik} \in B_M$, we shall construct differentials $\omega_t = \sigma_t\frac{\omega}{\pi} \in D^1_s(\frac{L_p}{B})$, $(t = r,\dots,p-4)$ which are not contained in the B-submodule generated by $\{x^i w^k \frac{\omega}{\pi}\}_{i+k\le p-3}$.

Clearly, the conditions $G_{00}(\beta_1),\dots,G_{00}(\beta_r)$ are satisfied by each solution in B_M of the system of linear equations

$$\sum_{i=0}^{p-3} \beta_s^i b_{i0} = 0 \qquad (s=1,\dots,r). \tag{7}$$

Multiplying its coefficient matrix from the left by M_r^{-1} yields an equivalent system

$$b_{j0} + \sum_{i=r}^{p-3} c_{j+1,i} b_{i0} = 0 \qquad (j = 0, \dots, r-1) \tag{8}$$

with coefficients $c_{s,i} \in B_{\mathfrak{P}}$. Choose in $B \setminus \mathfrak{P}$ a common denominator n for the $c_{s,i}$. For each $t \in \{r, \dots, p-4\}$ we obtain a solution of (8) by setting $b_{t0} = n\pi^{-1}, b_{i0} = 0$ for $i \geq r, i \neq t$ and $b_{j0} = -c_{j+1,t} n\pi^{-1}$ for $j = 0, \dots, r-1$. Then the corresponding differentials

$$\omega_t := (x^t - \sum_{j=0}^{r-1} c_{j+1,t} x^j) \frac{n\omega}{\pi^2} \qquad (t = r, \dots, p-4)$$

are contained in $(\bigoplus_{i+k \leq p-3} B_M x^i w^k) \frac{\omega}{\pi}$ and satisfy all conditions $\tilde{G}_{ik}$ and $G_{jk}(\beta_s)$ for $s = 1, \dots, r$. Hence

$$\omega_t \in D_s^1(\frac{L_p}{B}) \setminus (\bigoplus_{i+k \leq p-3} B x^i w^k) \frac{\omega}{\pi}$$

as $\frac{n}{\pi} \notin B$. This shows that the length of the A-module $D_s^1(\frac{K_p}{A}) / H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A})$ is at least $p - 3 - r = N(p) - 2$ and finishes the proof of 5.2b) and c). $\square$

Corollary 5.6. *If $N(p) \leq 2$, then $H^0(\bar{X}_p, \omega^1_{\bar{X}_p/A})$ is a birational invariant of the Fermat curve $k \otimes_A X_p$.*

References

1. Abhyankar S., *On the valuations centered in a local domain*, Amer. J. Math., **78** (1956), 321–348.
2. Bost J.-B., *A neglected aspect of Kähler's work on arithmetic geometry: Birational invariants of algebraic varieties over number fields*, in: R. Berndt and O. Riemenschneider (eds.), *Erich Kähler. Mathematische Werke/Mathematical Works*, de Gruyter, Berlin, 2003, 854–869.
3. Klösgen W., *Untersuchungen über Fermatsche Kongruenzen*, Gesellschaft Math. Datenverarbeitung, Bonn, **36** (1970).
4. Kunz E., Waldi R., *On certain birational invariants of the Fermat curves*, J. Pure Appl. Algebra, **210** (2007), 63–80.
5. Ribenboim P., *Fermat's last theorem for amateurs*, Springer, New York, 1999.

Received January 15, 2007

NWF I – Mathematik
Universitt Regensburg
D-93040 Regensburg, Germany
e-mail:
`ernst.kunz@mathematik.uni-regensburg.de`
e-mail:
`Rolf.Waldi@mathematik.uni-regensburg.de`