pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*,
Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

CRITERIA FOR COMPLETE INTERSECTIONS

Bart de Smit, Karl Rubin, René Schoof

Introduction

In this paper we discuss two results in commutative algebra that are used in A. Wiles's proof that all semi-stable elliptic curves over $\mathbf{Q}$ are modular [11].

We first fix some notation that is used throughout this paper. Let $\mathcal{O}$ be a complete Noetherian local ring with maximal ideal $\mathfrak{m}_{\mathcal{O}}$ and residue field $k = \mathcal{O}/\mathfrak{m}_{\mathcal{O}}$. Suppose that we have a commutative triangle of surjective homomorphisms of complete Noetherian local $\mathcal{O}$-algebras:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & T \\ & {\scriptstyle \pi_R}\searrow \quad \swarrow{\scriptstyle \pi_T} & \\ & \mathcal{O}. & \end{array}$$

Assume that T is a finite flat $\mathcal{O}$-algebra, i.e., that T is finitely generated and free as an $\mathcal{O}$-module. In the applications in Wiles's proof $\mathcal{O}$ is a discrete valuation ring, R is a deformation ring, T is a Hecke algebra and π_T is the homomorphism associated to a certain eigenform.

We show two distinct criteria, formulated as Criterion I and Criterion II below, which give sufficient conditions to conclude that φ is an isomorphism and that R and T are complete intersections. We say that a local $\mathcal{O}$-algebra that is finitely generated as an $\mathcal{O}$-module is a *complete intersection* over $\mathcal{O}$ if it is of the form

$$\mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n), \qquad \text{with } f_1, \ldots, f_n \in \mathcal{O}[[X_1, \ldots, X_n]].$$

We first state Criterion I. We put $I_R = \ker \pi_R$ and $I_T = \ker \pi_T$. The *congruence ideal* of T is defined to be the $\mathcal{O}$-ideal $\eta_T = \pi_T \operatorname{Ann}_T(I_T)$.

Criterion I. *Suppose that $\mathcal{O}$ is a complete discrete valuation ring and that $\eta_T \neq 0$. Then*

$$\operatorname{length}_{\mathcal{O}}(I_R/I_R^2) \;\geq\; \operatorname{length}_{\mathcal{O}}(\mathcal{O}/\eta_T).$$

Moreover, equality holds if and only if φ is an isomorphism between complete intersections over $\mathcal{O}$.

Wiles used a slightly weaker form of this criterion, where T is assumed to be Gorenstein, to show that certain "non-minimal" deformation rings are isomorphic to Hecke algebras [7]. The present version, without the Gorenstein condition, is due to H.W. Lenstra [5]. In Section 3 we give an alternative argument for Criterion I that was found by the first and the third author. Criterion I is an easy consequence of the following result, which holds without any conditions on $\mathcal{O}$ or η_T.

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

Theorem. *The map φ is an isomorphism between complete intersections over $\mathcal{O}$ if and only if $\varphi\,\mathrm{Fit}_R(I_R) \not\subset \mathfrak{m}_{\mathcal{O}}T$.*

Here $\mathrm{Fit}_R(I_R)$ denotes the R-Fitting ideal of I_R. Fitting ideals are instrumental in the proof of Criterion I. We recall their definition and basic properties in Section 1.

A crucial special case of the theorem can already be found in a 1969 paper of H. Wiebe [10]; see also [1, Thm.2.3.16]. More precisely, Wiebe's result covers the case that $\mathcal{O} = k$ is a field, and φ is the identity on $R = T$. The statement is then that T is a complete intersection over k if and only if the Fitting ideal of its maximal ideal is non-zero.

For the proof of Criterion 1 we need some properties of complete intersections that go back to J.T. Tate [8]. In Section 2 we formulate Tate's result and prove it using Koszul complexes. These are discussed in Section 1. As a consequence we find that complete intersections have the Gorenstein property. The Gorenstein property does not occur in our proof of Criterion I, but we briefly discuss its significance in our context at the end of Section 2.

In order to formulate Criterion II, assume that $\mathrm{char}(k) = p > 0$, and let $n \geq 1$. The ring $\mathcal{O}[[S_1, \ldots, S_n]]$ is filtered by the ideals J_m with $m \geq 0$ given by $J_m = (\omega_m(S_1), \ldots, \omega_m(S_n))$, where $\omega_m(S)$ denotes the polynomial $(1+S)^{p^m} - 1$. Note that $J_0 = (S_1, \ldots, S_n)$.

Criterion II. *Suppose that for every $m > 0$ there is a commutative diagram of $\mathcal{O}$-algebras*

$$\begin{array}{ccccc} \mathcal{O}[[S_1,\ldots,S_n]] & \longrightarrow & R_m & \xrightarrow{\varphi_m} & T_m \\ & & \downarrow & & \downarrow \\ & & R & \xrightarrow{\varphi} & T \end{array}$$

with the properties:

(i) there is a surjection of $\mathcal{O}$-algebras $\mathcal{O}[[X_1, \ldots, X_n]] \longrightarrow R_m$;

(ii) the map φ_m: $R_m \longrightarrow T_m$ is surjective;

(iii) the vertical arrows induce isomorphisms

$$R_m/J_0R_m \xrightarrow{\sim} R \qquad \text{and} \qquad T_m/J_0T_m \xrightarrow{\sim} T.$$

(iv) the quotient ring T_m/J_mT_m is finite flat over $\mathcal{O}[[S_1, \ldots, S_n]]/J_m$;

Then φ: $R \longrightarrow T$ is an isomorphism between complete intersections over $\mathcal{O}$.

Criterion II, with the additional condition that k be a finite field, first appeared in the paper by R. Taylor and A. Wiles [9] with an improvement due to G. Faltings. It is used by Wiles for the "minimal" deformation problem [2]. In section 4 we present a proof due to the second author. It does not depend on the previous sections of the paper. Our approach avoids the original non-canonical limiting process and works for arbitrary complete Noetherian local rings $\mathcal{O}$.

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

1. Preliminaries.

In this section we first recall the definition and basic properties of Fitting ideals. Then we do the same for Koszul complexes following [3]. For more details see [4, Sections XIX.2, XXI.4].

Fitting ideals. Let A be a ring and let M be a finitely generated A-module with generators $m_1, \dots, m_n$. Let $f\colon A^n \longrightarrow\!\!\!\!\!\rightarrow M$ be the surjective A-homomorphism defined by $f(e_i) = m_i$ for $i = 1, \dots, n$. Here e_i denotes the ith standard basis vector of A^n. The *Fitting ideal* $\mathrm{Fit}_A(M)$ of M is the ideal generated by $\det(v_1, \dots, v_n)$ with $v_1, \dots, v_n \in \ker f$. Clearly, $\mathrm{Fit}_A(M)$ is already generated by the elements $\det(v_1, \dots, v_n)$ where the vectors $v_1, \dots, v_n$ range over a fixed set of A-module generators for $\ker f$.

The Fitting ideal does not depend on the choice of the generators m_i. To see this, let $m_{n+1} = \sum_{i=n}^{d} \alpha_i m_i$ with $\alpha_i \in A$ be an additional generator of M. The kernel of the surjective homomorphism $\psi\colon A^{n+1} \longrightarrow\!\!\!\!\!\rightarrow M$ given by $\psi(e_i) = m_i$ for $i = 1, \dots, m, m+1$, is generated by the vector $(\alpha_1, \dots, \alpha_d, -1)$ and vectors $(v_i, 0)$ where the v_i range over a set of generators for $\ker f$. It follows at once that the Fitting ideal does not change when we replace the generators $m_1, \dots, m_n$ by $m_1, \dots, m_n, m_{n+1}$. Inductively, this implies that any two generating sets $m_1, \dots, m_n$ and $m'_1, \dots, m'_{n'}$ give rise to the same Fitting ideal as their union $m_1, \dots, m_n, m'_1, \dots, m'_{n'}$.

The following proposition contains the properties of the Fitting ideal that we will use.

Proposition 1.1. *Let A be a ring and let M be a finitely generated A-module. Then*

(i) we have $\mathrm{Fit}_A(M) \subset \mathrm{Ann}_A(M)$;
(ii) for any A-algebra B we have $\mathrm{Fit}_B(M \otimes_A B) = \mathrm{Fit}_A(M) \cdot B$;
(iii) for any ideal $\mathfrak{a} \subset A$ we have $\mathrm{Fit}_A(A/\mathfrak{a}) = \mathfrak{a}$;
(iv) for every A-module N we have $\mathrm{Fit}_A(M \times N) = \mathrm{Fit}_A(M)\mathrm{Fit}_A(N)$.

Proof. We sketch the proof. If $v_1, \dots, v_n$ are in the kernel of $A^n \xrightarrow{f} M$, then the matrix σ with columns $v_1, \dots, v_n$ has the property that the composite map $A^n \xrightarrow{\sigma} A^n \xrightarrow{f} M$ is equal to zero. By multiplying first with the adjoint matrix of σ, we see that $\det(\sigma) \cdot A^n \subset \ker f$. Since f is surjective, this implies that $\det(\sigma) \in \mathrm{Ann}_A(M)$, and *(i)* follows. Part *(ii)* follows from the fact that taking the tensor product with B is right exact. Part *(iii)* is immediate from the definition if we take $n = 1$. We leave part *(iv)* to the reader.

If A is a principal ideal domain, then, by the theory of elementary divisors, every finitely generated A-module M is of the form $M \cong A/\mathfrak{a}_1 \times \ldots \times A/\mathfrak{a}_s$ for certain ideals $\mathfrak{a}_i \subset A$. By *(iii)* and *(iv)*, we see that $\mathrm{Fit}_A(M) = \mathfrak{a}_1 \cdots \mathfrak{a}_s$. If A is a discrete valuation ring with maximal ideal $\mathfrak{m}_A$, then we see that

$$\mathrm{Fit}_A(M) = \mathfrak{m}_A^{\mathrm{length}_A(M)},$$

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

with the convention that $\mathfrak{m}_A^\infty = 0$.

Example. Let $A = \mathcal{O}[[X_1, \ldots, X_n]]/J$ with $J = (f_1, \ldots, f_r)$ an ideal contained in $I = (X_1, \ldots, X_n)$, and put $I_A = I/J$. Suppose that $g_{ij} \in \mathcal{O}[[X_1, \ldots, X_n]]$ satisfy

$$f_i = \sum_{j=1}^{n} g_{ij} X_j \qquad \text{for } i = 1, \ldots, r.$$

Then the Fitting ideal $\mathrm{Fit}_A(I_A)$ contains the determinants of the $n \times n$ submatrices of the matrix (g_{ij}) modulo J. Actually, one can show that these determinants generate $\mathrm{Fit}_A(I_A)$ by applying Proposition 1.3 to the sequence $X_1, \ldots, X_n$ in $\mathcal{O}[[X_1, \ldots, X_n]]$. This will not be used in the sequel.

Koszul complexes. Let A be a ring, let $V = A^n$ and let $f = (f_1, \ldots, f_n) \in V$. For any A-module M we set

$$K_m(f, M) = \mathrm{Hom}_A(\textstyle\bigwedge_A^m V, M), \qquad \text{for } m \geq 0;$$

and for $\varphi \in K_m(f, M)$ we define $d\varphi \in K_{m-1}(f, M)$ by $d\varphi(x) = \varphi(f \wedge x)$. Since $d^2 = 0$, we obtain a complex $K_\bullet(f, M)$, which we call the *Koszul complex* of f on M:

$K_\bullet(f, M)$:

$$0 \longrightarrow K_n(f, M) \xrightarrow{d} \ldots \xrightarrow{d} K_1(f, M) \xrightarrow{d} K_0(f, M) \longrightarrow 0.$$

Note that $K_\bullet(f, M) = K_\bullet(f, A) \otimes_A M$ and that $K_m(f, A)$ is a free A-module of rank $\binom{n}{m}$. The m-th homology group of $K_\bullet(f, M)$ is denoted by $H_m(f, M)$.

We have $H_0(f, M) = M/IM$, where I is the A-ideal generated by the f_i.

Lemma 1.2. *The homology groups $H_m(f, M)$ are annihilated by I.*

Proof. Let $\varphi \in K_m(f, M)$ with $d\varphi = 0$. For each generator f_i of I we must show that there is $\psi \in K_{m+1}(f, M)$ with $d\psi = f_i\varphi$. To see this, write $V = Ae_i \times V'$ where e_i is the ith standard basis vector of V over A, and V' is generated by the other standard basis vectors. Then every $x \in \bigwedge^{m+1} V$ can be written as $x = e_i \wedge x' + x''$ for unique $x' \in \bigwedge^m V'$ and $x'' \in \bigwedge^{m+1} V'$. Now define $\psi \in K_{m+1}(f, M)$ by $\psi(x) = \varphi(x')$. From $d\varphi = 0$ one deduces that $d\psi = f_i\varphi$, as required.

We say that a sequence of elements $p_1, \ldots, p_n$ in A is *M-regular*, if for $i = 1, \ldots, n$ the multiplication by p_i on $M/(p_1, \ldots, p_{i-1})M$ is an injective map. The following proposition can also be found in [1, Thm.1.6.16].

Proposition 1.3. *Let $f = (f_1, \ldots, f_n) \in A^n$ and let M be an A-module. If the A-ideal I generated by $f_1, \ldots, f_n$ contains an M-regular sequence of length n, then $H_i(f, M) = 0$ for $i \geq 1$.*

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

Proof. Let $p_1, \dots, p_n \in A$ be an M-regular sequence in I. For any integer j with $0 \le j \le n$ we prove inductively that $H_i(f, M/(p_1, \dots, p_j)M) = 0$ for all $i \ge j+1$. For $j = n$ this is trivial, and for $j = 0$ this is the content of the proposition.

Assume that this statement is true for some $j > 0$, and let $M' = M/(p_1, \dots, p_{j-1})M$. Since the sequence $p_1, \dots, p_n$ is M-regular, there is an exact sequence

$$0 \longrightarrow M' \xrightarrow{p_j} M' \longrightarrow M'/p_jM' \longrightarrow 0.$$

For each m we apply the exact functor $\mathrm{Hom}_A(\bigwedge^m V, -)$. This gives us a short exact sequence of complexes

$$0 \longrightarrow K_\bullet(f, M') \xrightarrow{p_j} K_\bullet(f, M') \longrightarrow K_\bullet(f, M'/p_jM') \longrightarrow 0.$$

By Lemma 1.2 the homology groups of $K_\bullet(f, M')$ are annihilated by I and therefore by p_i. This implies that the long exact homology sequence breaks up into short exact sequences. For every $i = 1, \dots, n$ we obtain an exact sequence

$$0 \longrightarrow H_i(f, M') \longrightarrow H_i(f, M'/p_jM') \longrightarrow H_{i-1}(f, M') \longrightarrow 0.$$

The induction hypothesis implies that the middle group is zero for $i \ge j+1$. This implies that $H_i(f, M') = 0$ for $i \ge j$, which is the statement for $j - 1$.

2. Complete intersections.

This section is devoted to the proof of the following result, which goes back to Tate [8].

Proposition 2.1. *Let $\mathcal{O}$ be a complete Noetherian local ring. Let A be a finite flat $\mathcal{O}$-algebra of the form $A = \mathcal{O}[[X_1, \dots, X_n]]/(f_1, \dots, f_n)$ with $(f_1, \dots, f_n) \subset (X_1, \dots, X_n)$. Write $f_i = \sum_{j=1}^n g_{ij}X_j$, let d be the image of $\det(g_{ij})$ in A, and let I_A be the A-ideal $I_A = (X_1, \dots, X_n)/(f_1, \dots, f_n)$. Then we have*

(i) $\mathrm{Fit}_A(I_A) = \mathrm{Ann}_A(I_A) = (d)$;

(ii) the A-ideal (d) is a direct $\mathcal{O}$-summand of A of $\mathcal{O}$-rank 1.

Proof. Let $P = \mathcal{O}[[X_1, \dots, X_n]]$. We write f for the vector $(f_1, \dots, f_r) \in P^n$. Multiplication with the matrix g_{ij} gives an P-linear map $P^n \longrightarrow P^n$ sending the vector $X = (X_1, \dots, X_n)$ to f. It induces a morphism of Koszul complexes

$$K_\bullet(f, P) \longrightarrow K_\bullet(X, P).$$

The sequence $X_1, \dots, X_n$ is P-regular. Since A is finitely generated as an $\mathcal{O}$-module, there is for every i a monic polynomial $p_i(X_i) \in (f_1, \dots, f_n)$. The sequence $p_1, \dots, p_n$ is $\mathcal{O}[X_1, \dots, X_n]$-regular and by exactness of completion it is also P-regular. By Prop.1.3 the homology groups of both Koszul

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

complexes vanish and we obtain the following commutative diagram with exact rows

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & P & \xrightarrow{(f_1,\dots,f_n)} & P^n & \longrightarrow & \cdots & \longrightarrow & P^n & \xrightarrow{(f_1,\dots,f_n)} & P & \longrightarrow & A & \longrightarrow & 0 \\
 & & \det(g_{ij})\downarrow & & \downarrow & & & & g_{ij}\downarrow & & \| & & \downarrow{\scriptstyle \pi_A} & & \\
0 & \longrightarrow & P & \xrightarrow{(X_1,\dots,X_n)} & P^n & \longrightarrow & \cdots & \longrightarrow & P^n & \xrightarrow{(X_1,\dots,X_n)} & P & \longrightarrow & \mathcal{O} & \longrightarrow & 0.
\end{array}$$

Here π_A is the $\mathcal{O}$-algebra map $A \longrightarrow \mathcal{O}$ with kernel I_A. We now tensor the whole diagram *on the right* with the P-module A. Since the rows are P-free resolutions of A and $\mathcal{O}$, the homology groups of the rows become $\mathrm{Tor}_j^A(A,A)$ and $\mathrm{Tor}_j^A(\mathcal{O},A)$ respectively. Hence, we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Tor}_n^P(A,A) & \longrightarrow & A & \xrightarrow{0} & A^n \\
 & & {\scriptstyle \pi_{A*}}\downarrow & & {\scriptstyle d}\downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Tor}_n^P(\mathcal{O},A) & \longrightarrow & A & \xrightarrow{(X_1,\dots,X_n)} & A^n.
\end{array}$$

It follows that $\mathrm{Tor}_n^P(\mathcal{O},A) \cong \mathrm{Ann}_A(I_A)$. In order to determine this Tor-group and the image of π_{A*}, we tensor the P-resolution $K_\bullet(f,P)$ of A *on the left* with the P-module map $s\colon A \longrightarrow \mathcal{O}$. This gives a map between two complexes with homology groups $\mathrm{Tor}_j^A(A,A)$ and $\mathrm{Tor}_j^A(\mathcal{O},A)$ respectively. Since one can compute Tor-functors using resolutions of either argument [4, Chap. XX, Prop. 8.2'], the same map π_{A*} then makes the following diagram with exact rows commute:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Tor}_n^P(A,A) & \longrightarrow & A & \xrightarrow{0} & A^n \\
 & & {\scriptstyle \pi_{A*}}\downarrow & & {\scriptstyle s}\downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Tor}_n^P(\mathcal{O},A) & \longrightarrow & \mathcal{O} & \xrightarrow{0} & \mathcal{O}^n.
\end{array}$$

In particular we see that π_{A*} is surjective, so that $(d) = \mathrm{Ann}_A(I_A)$ and (d) is free of rank 1 as an $\mathcal{O}$-module. On the other hand,

$$(d) \;\subset\; \mathrm{Fit}_A(I_A) \;\subset\; \mathrm{Ann}_A(I_A),$$

and therefore we have equality everywhere. By applying what we have already proved to the complete intersection $A \otimes_{\mathcal{O}} k$ over k we see that $d \otimes 1 \neq 0$ in $A \otimes_{\mathcal{O}} k$, so that $d \notin \mathfrak{m}_{\mathcal{O}} A$. By Nakayama's lemma we can therefore make the element d part of an $\mathcal{O}$-basis of A, so that the inclusion $(d) \subset A$ splits as an $\mathcal{O}$-linear map. This proves the proposition.

Corollary 2.2. *If in the situation of Proposition 2.1 the ring $\mathcal{O}$ is a field, then (d) is the unique minimal non-zero ideal of A.*

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

Proof. Proposition 2.1 says that (d) has dimension 1 over $\mathcal{O} = k$, so (d) contains no smaller non-zero ideals. On the other hand, every minimal ideal $\mathfrak{a}$ is annihilated by the maximal ideal I_A of A, and by Proposition 2.1 we have $\mathrm{Ann}_A(I_A) = (d)$, so $\mathfrak{a} \subset (d)$.

Corollary 2.3. *Let A be a finite flat $\mathcal{O}$-algebra with a section $\pi_A : A \longrightarrow \mathcal{O}$ and let $I_A = \ker \pi_A$. If A is a complete intersection over $\mathcal{O}$, then $\mathrm{Fit}_A(I_A) = \mathrm{Ann}_A(I_A)$, and this ideal is a non-zero direct O-summand of A.*

Proof. Suppose $A = \mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$. Since $\mathcal{O}$ is complete, a linear change of variables that replaces X_i by $X_i - \pi_A(X_i)$ gives that $(f_1, \ldots, f_n) \subset (X_1, \ldots, X_n)$. The result now follows from Proposition 2.1.

We conclude this section with some remarks that will not be used in the rest of this paper.

The Gorenstein condition. Let A be a finite flat $\mathcal{O}$-algebra. Then the $\mathcal{O}$-linear dual $A^\vee = \mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$ of A has an A-module structure given by $(af)(x) = f(ax)$ for $f \in A^\vee$ and $a, x \in A$. The algebra A is called *Gorenstein* over $\mathcal{O}$ if $A^\vee$ is a free A-module of rank 1.

It follows from Proposition 2.1 *(ii)* that for A of the form

$$\mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$$

with $(f_1, \ldots, f_n) \subset (X_1, \ldots, X_n)$, there exists an $\mathcal{O}$-linear map $t\colon A \longrightarrow \mathcal{O}$ with $t(d) = 1$. This homomorphism t generates $A^\vee$ as an A-module, so that A is Gorenstein over $\mathcal{O}$. To see this when $\mathcal{O}$ is a field, one notes that $(d) \not\subset \mathrm{Ann}_A(t)$, so that $\mathrm{Ann}_A(t) = 0$ by Corollary 2.2. With Nakayama's lemma the general case then follows as well.

In general, suppose that A is Gorenstein, so there is an A-module isomorphism $s\colon A^\vee \xrightarrow{\sim} A$. Assume in addition that there exists a section $\pi_A\colon A \longrightarrow \mathcal{O}$, and put $I_A = \ker \pi_A$. Then the image of the composite map

$$\mathcal{O} \;\cong\; \mathcal{O}^\vee \xrightarrow{\pi_A^\vee} A^\vee \xrightarrow[s]{\sim} A$$

is $\mathrm{Ann}_A(I_A)$. To see this, one notes that the image of $\pi_A^\vee$ is

$$\mathcal{O} \cdot \pi_A = \{f \in A^\vee : f(I_A) = 0\},$$

and that

$$f(I_A) = 0 \iff I_A \cdot f = 0 \iff s(f) \in \mathrm{Ann}_A(I_A).$$

Applying π_A, we see that the congruence ideal $\eta_A = \pi_A \,\mathrm{Ann}_A(I_A)$ is equal to the $\mathcal{O}$-ideal generated by $\pi_A \circ s \circ \pi_A^\vee(1)$. It is this property that Wiles uses to *define* the congruence ideal in the Gorenstein case.

More general complete intersections. The statement that finite complete intersection algebras are Gorenstein holds over much more general

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

base rings, and it also holds if there is no section $A \longrightarrow \mathcal{O}$. Moreover, one can omit the flatness condition on A in Proposition 2.1, because it follows from the other assumptions. More precisely, if $\mathcal{O}$ is any ring and the ring $A = \mathcal{O}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ is finitely generated as an $\mathcal{O}$-module, then one can show with Koszul complexes that A is projective as an $\mathcal{O}$-module [3]. An argument of Tate [6, appendix] then implies that $A^\vee$ is free of rank 1 over A. For Noetherian $\mathcal{O}$ the class of finite $\mathcal{O}$-algebras of the form $\mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$ is a subclass of the class of finite algebras of the form $\mathcal{O}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$; see [3]. In particular, these algebras are also projective and Gorenstein over $\mathcal{O}$.

3. Proof of Criterion I

In this section we first prove the theorem in the introduction and then show Criterion I. Using Nakayama's lemma we first show that the question whether φ is an isomorphism reduces to the case that $\mathcal{O}$ is a field.

Lemma 3.1. *Let $f\colon A \longrightarrow B$ be a surjective homomorphism of Noetherian local $\mathcal{O}$-algebras for which B is finite flat over $\mathcal{O}$. Suppose that the induced map $\overline{f}\colon A \otimes_{\mathcal{O}} k \longrightarrow B \otimes_{\mathcal{O}} k$ is an isomorphism. Then f is an isomorphism.*

Proof. By applying Nakayama's lemma to B as an $\mathcal{O}$-module we see that f is surjective. Since B is $\mathcal{O}$-free, $(\ker f) \otimes_{\mathcal{O}} k$ is the kernel of $\overline{f}$, which is zero. The ring A is Noetherian, so $\ker f$ is finitely generated as an A-module. Since $\mathfrak{m}_{\mathcal{O}}$ is contained in the maximal ideal of A we can apply Nakayama's lemma to the A-module $\ker f$ and conclude that $\ker f = 0$.

Now we give the proof of the theorem stated in the introduction. Recall that we have a commutative triangle of surjective homomorphisms of complete Noetherian local $\mathcal{O}$-algebras with T finite and flat over $\mathcal{O}$:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & T \\ & {\scriptstyle \pi_R}\searrow \quad \swarrow{\scriptstyle \pi_T} & \\ & \mathcal{O}. & \end{array}$$

We let $I_R = \ker \pi_R$ and $I_T = \ker \pi_T$.

Theorem. *The map φ is an isomorphism between complete intersections over $\mathcal{O}$ if and only if $\varphi\,\mathrm{Fit}_R(I_R) \not\subset \mathfrak{m}_{\mathcal{O}} T$.*

Proof. In order to show "only if", we note that by Corollary 2.3, $\mathrm{Fit}_T(I_T)$ is a non-zero direct $\mathcal{O}$-summand of T and in particular $\varphi\,\mathrm{Fit}_R(I_R) = \mathrm{Fit}_T(I_T) \not\subset \mathfrak{m}_{\mathcal{O}} T$.

To show "if", suppose first that $\mathcal{O} = k$ is a field. Since R is complete and Noetherian, we can write $R = k[[X_1, \ldots, X_n]]/J_R$ where J_R is a $k[[X_1, \ldots, X_n]]$-ideal. Since T is a finite dimensional k-vector space, we

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

can do this in such a way that the elements $\varphi(X_i \bmod J_R)$ generate I_T as a k-vector space. The kernel J_T of the composite map

$$k[[X_1, \ldots, X_n]] \longrightarrow\!\!\!\!\rightarrow R \xrightarrow{\varphi} T$$

is contained in the ideal $I = (X_1, \ldots, X_n)$. We assume that $\varphi \mathrm{Fit}_R(I_R) \neq 0$, which means that there are polynomials $g_{ij} \in k[[X_1, \ldots, X_n]]$ so that $\sum_j g_{ij} X_j \in J_R$ for $i = 1, \ldots, n$ and $\det(g_{ij}) \notin J_T$.

Since the elements X_i generate I/J_T as a k-vector space, the monomials $X_i X_j$ generate I^2/IJ_T as a k-vector space. This implies that every element of the quotient ring $k[[X_1, \ldots, X_n]]/IJ_T$ is represented by a polynomial of total degree at most 2. Therefore, we can, for $i = 1, \ldots, n$, find polynomials p_i and q_i of total degree at most 2, so that

$$p_i \equiv \sum_j g_{ij} X_j \pmod{IJ_T},$$
$$q_i \equiv X_i^3 \pmod{IJ_T}.$$

We now let the polynomials $f_1, \ldots, f_n$ be

$$f_i = X_i^3 - q_i + p_i \qquad \text{for } i = 1, \ldots, n.$$

Note first that $f_i \in IJ_T + J_R \subset J_T$ and that $f_i = \sum_j G_{ij} X_j$ with $G_{ij} \equiv g_{ij} \bmod J_T$.

The k-algebra $B = k[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ has finite dimension as a k-vector space, because every element in B is represented by a polynomial of degree at most 2 in each variable. Therefore, B is Artinian and it is a finite product of local Artinian rings. Hence, the completion $\hat{B} = k[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$ of B at $(X_1, \ldots, X_n)$ is a factor of B, so it is also finite dimensional over k. By Corollary 2.2 the $\hat{B}$-ideal generated by $\det(G_{ij})$ is the unique minimal non-zero ideal of $\hat{B}$. Since $\det(G_{ij}) \equiv \det(g_{ij}) \not\equiv 0 \pmod{J_T}$, this minimal ideal does not map to 0 in T. It follows that the map $\hat{B} \longrightarrow T$ is an isomorphism. Thus, T is a complete intersection over k, and $J_T = (f_1, \ldots, f_n) \subset IJ_T + J_R$. By Nakayama's lemma we must have $J_T = J_R$ so that φ is an isomorphism. This completes the proof in the case that $\mathcal{O} = k$.

We now prove the "if" part for general $\mathcal{O}$. The map $\pi_R\colon R \longrightarrow \mathcal{O}$ is an $\mathcal{O}$-split surjection, so the induced map $R \otimes_{\mathcal{O}} k \longrightarrow k$ has kernel $I_R \otimes_{\mathcal{O}} k$. Since $\mathrm{Fit}_k(I_R \otimes_{\mathcal{O}} k)$ is the image in $R \otimes_{\mathcal{O}} k$ of $\mathrm{Fit}_R(I_R)$, the case that we proved already implies that the map $R \otimes_{\mathcal{O}} k \longrightarrow T \otimes_{\mathcal{O}} k$ is an isomorphism between complete intersections over k. Lemma 3.1 implies that φ is an isomorphism. Moreover, we can lift any k-algebra isomorphism

$$k[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n) \xrightarrow{\sim} T \otimes_{\mathcal{O}} k.$$

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

to a surjective $\mathcal{O}$-algebra homomorphism ψ: $\mathcal{O}[[X_1,\dots,X_n]] \longrightarrow T$. The kernel of ψ contains lifts $\tilde{f}_i$ of the elements f_i, and by Lemma 3.1 the induced map

$$\mathcal{O}[[X_1,\dots,X_n]]/(\tilde{f}_1,\dots,\tilde{f}_n) \longrightarrow\!\!\!\!\!\rightarrow T.$$

is an isomorphism. This proves the theorem.

Proof of Criterion I. First we show the inequality. By Prop.1.1 *(i)* we have $\operatorname{Fit}_R(I_R) \subset \operatorname{Ann}_R(I_R)$. Since the map $I_R \xrightarrow{\varphi} I_T$ is surjective, we have $\varphi \operatorname{Ann}_R(I_R) \subset \operatorname{Ann}_T(I_T)$. Hence we see that

$$\pi_R \operatorname{Fit}(I_R) = \pi_T \varphi \operatorname{Fit}_R(I_R) \ \subset \ \pi_T \operatorname{Ann}_T(I_T) = \eta_T = \mathfrak{m}_{\mathcal{O}}^{\operatorname{length}_{\mathcal{O}}(\mathcal{O}/\eta_T)}.$$

Viewing $\mathcal{O}$ as an R-algebra via π_R: $R \longrightarrow \mathcal{O}$ we have $I_R \otimes_R \mathcal{O} = I_R/I_R^2$. By Prop.1.1 *(ii)* this implies that

$$\pi_R \operatorname{Fit}_R(I_R) = \operatorname{Fit}_{\mathcal{O}}(I_R/I_R^2) = \mathfrak{m}_{\mathcal{O}}^{\operatorname{length}_{\mathcal{O}}(I_R/I_R^2)},$$

and it follows that $\operatorname{length}_{\mathcal{O}}(I_R/I_R^2) \geq \operatorname{length}_{\mathcal{O}}(\mathcal{O}/\eta_T)$. Moreover, if φ is an isomorphism between complete intersections, then by Corollary 2.3 we have $\varphi \operatorname{Fit}_R(I_R) = \operatorname{Ann}_T(I_T)$, and therefore the two lengths are equal.

To show the converse, assume that the two lengths are equal, i.e., we have that $\pi_R \operatorname{Fit}_R(I_R) = \pi_T \operatorname{Ann}_T(I_T)$. We first show that $I_T \cap \operatorname{Ann}_T(I_T) = 0$. Since $\eta_T \neq 0$ there is an element $y \in \operatorname{Ann}_T(I_T)$ for which $\pi_T(y) \neq 0$. For any element $x \in I_T \cap \operatorname{Ann}_T(I_T)$ we clearly have $xy = 0$ and $x(y - \pi_T(y)) = 0$. But then $\pi_T(y)x = 0$, and since T is free as a module over the discrete valuation ring $\mathcal{O}$ this implies that $x = 0$. This shows that $I_T \cap \operatorname{Ann}_T(I_T) = 0$.

It follows that the map π_T: $\operatorname{Ann}_T(I_T) \longrightarrow \eta_T$ is an isomorphism. Since

$$\pi_T \varphi \operatorname{Fit}_R(I_R) = \pi_R \operatorname{Fit}_R(I_R) = \pi_T \operatorname{Ann}_T(I_T),$$

we conclude that $\varphi \operatorname{Fit}_R(I_R) = \operatorname{Ann}_T(I_T)$. This non-zero $\mathcal{O}$-submodule of T cannot be contained in $\mathfrak{m}_{\mathcal{O}} T$ because $T/\operatorname{Ann}_T(I_T)$ injects canonically to $\operatorname{End}_{\mathcal{O}}(I_T)$, which is torsion free as an $\mathcal{O}$-module. By the theorem this can only happen if φ is an isomorphism of complete intersections. This proves Criterion I.

Remark. If T is Gorenstein over $\mathcal{O}$ (see the end of Section 2), or if $\mathcal{O}$ is a complete discrete valuation ring, then it is not hard to show that $\operatorname{Ann}_T(I_T)$ is a non-zero direct $\mathcal{O}$-summand of T. By Corollary 2.3 the condition $\varphi \operatorname{Fit}_R(I_R) \not\subset \mathfrak{m}_{\mathcal{O}} T$ in the theorem can then be replaced by $\varphi \operatorname{Fit}_R(I_R) = \operatorname{Ann}_T(I_T)$. This may fail for other rings $\mathcal{O}$. For instance, let k be a field, and let $\mathcal{O} = k[\varepsilon]$ with $\varepsilon^2 = 0$. The ring $T = \mathcal{O}[[X,Y]]/(X^2, Y^2, XY - \varepsilon X - \varepsilon Y)$, with $I_T = (X,Y)$, is a finite flat $\mathcal{O}$-algebra with $\operatorname{Fit}_T(I_T) = \operatorname{Ann}_T(I_T) = (\varepsilon X, \varepsilon Y)$, but T is not a complete intersection over $\mathcal{O}$.

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

4. Proof of Criterion II

In this section we prove Criterion II. Just as in Section 3, we first give the argument over a field, and then apply Nakayama's lemma.

Lemma 4.1. *Let k be a field and let $n \geq 1$. Suppose we have k-algebra homomorphisms*

$$k[[S_1, \ldots, S_n]] \longrightarrow k[[X_1, \ldots, X_n]] \xrightarrow{f} A$$

with f surjective, and suppose that the k-algebra $A/(S_1, \ldots, S_n)A$ has finite dimension d as a vector space over k. Assume that for some $N > n^{n-1}d^n$, the induced map

$$k[[S_1, \ldots, S_n]]/(S_1^N, \ldots, S_n^N) \xrightarrow{g} A/(S_1^N, \ldots, S_n^N)A$$

is injective. Then f induces an isomorphism of k-algebras

$$k[[X_1, \ldots, X_n]]/(S_1, \ldots, S_n) \xrightarrow{\sim} A/(S_1, \ldots, S_n)A.$$

Proof. The ring $k[[X_1, \ldots, X_n]]$ is a local ring with maximal ideal $I = (X_1, \ldots, X_n)$. Since $A/(S_1, \ldots, S_n)A$ has length d as a module over the ring $k[[X_1, \ldots, X_n]]$, it is annihilated by I^d. Writing $J = \ker f$, this means that

$$I^d \subset J + (S_1, \ldots, S_n),$$

where $(S_1, \ldots, S_n)$ denotes the ideal of $k[[X_1, \ldots, X_n]]$ generated by the S_i. We will show that $J \subset I^{d+1}$ by assuming that we can find $\alpha \in J$ with $\alpha \notin I^{d+1}$, and deriving a contradiction. Consider the multiplication by α map:

$$\begin{aligned} 0 \longrightarrow \ker \longrightarrow\ & k[[X_1, \ldots, X_n]]/I^{ndN} \\ & \xrightarrow{\alpha} k[[X_1, \ldots, X_n]]/I^{ndN} \longrightarrow \operatorname{cok} \longrightarrow 0. \end{aligned}$$

Since $k[[X_1, \ldots, X_n]]/I^{ndN}$ has finite dimension over k, it follows that $\dim_k(\ker) = \dim_k(\operatorname{cok})$. We give estimates for these two dimensions. We have inclusions of $k[[X_1, \ldots, X_n]]$-ideals

$$I^{ndN} \subset (J + (S_1, \ldots, S_n))^{nN} \subset J + (S_1^N, \ldots, S_n^N),$$

so the cokernel $\operatorname{cok} = k[[X_1, \ldots, X_n]]/(I^{ndN} + (\alpha))$ now maps surjectively to the quotient ring $k[[X_1, \ldots, X_n]]/(J + (S_1^N, \ldots, S_n^N)) = A/(S_1^N, \ldots, S_n^N)A$. Since g is injective this gives

$$\begin{aligned} \dim_k \operatorname{cok} &\geq \dim_k A/(S_1^N, \ldots, S_n^N)A \\ &\geq \dim_k k[[S_1, \ldots, S_n]]/(S_1^N, \ldots, S_n^N) = N^n. \end{aligned}$$

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

On the other hand, since $\alpha \notin I^{d+1}$, we have $\ker \subset I^{ndN-d}/I^{ndN}$, so that the $\dim_k(\ker)$ is at most the number of monomials of degree δ with $ndN - d \le \delta < ndN$. Therefore

$$\dim_k \ker \;\le\; \sum_{\delta=ndN-d}^{ndN-1} \binom{\delta+n-1}{n-1} \;\le\; d(ndN)^{n-1}.$$

Combining the two estimates we see that $N^n \le d(ndN)^{n-1}$, which contradicts the assumption that $N > n^{n-1}d^n$. This proves that $J \subset I^{d+1}$.

To finish the proof of the lemma, consider the inclusions

$$I^d \;\subset\; J + (S_1, \ldots, S_n) \;\subset\; I^{d+1} + (S_1, \ldots, S_n).$$

By Nakayama's lemma we see that $I^d \subset (S_1, \ldots, S_n)$, so that

$$\ker f = J \subset I^{d+1} \subset (S_1, \ldots, S_n).$$

Since f induces an isomorphism $k[[X_1, \ldots, X_n]]/J \xrightarrow{\sim} A$, the lemma follows.

We now return to the setting in which Criterion II is formulated: we let $\mathcal{O}$ be a complete Noetherian local ring and suppose that its residue field k has characteristic $p > 0$. Let $n \ge 1$ and for $m \ge 0$ let J_m be the $\mathcal{O}[[S_1, \ldots, S_n]]$-ideal $(\omega_m(S_1), \ldots, \omega_m(S_n))$, where $\omega_m(S)$ denotes the polynomial $(1+S)^{p^m} - 1$.

Corollary 4.2. *Suppose we have $\mathcal{O}$-algebra homomorphisms*

$$\mathcal{O}[[S_1, \ldots, S_n]] \;\longrightarrow\; \mathcal{O}[[X_1, \ldots, X_n]] \;\xrightarrow{f}\!\!\!\!\rightarrow\; A$$

with f surjective, and $A/(S_1, \ldots, S_n)A$ free of rank $d > 0$ over $\mathcal{O}$. If, for some m with $p^m > n^{n-1}d^n$ the quotient ring A/J_mA is free as a module over $\mathcal{O}[[S_1, \ldots, S_n]]/J_m$, then the induced map

$$h\colon\ \mathcal{O}[[X_1, \ldots, X_n]]/(S_1, \ldots, S_n) \;\longrightarrow\; A/(S_1, \ldots, S_n)A$$

is an isomorphism between complete intersections over $\mathcal{O}$.

Proof. Taking everything modulo $\mathfrak{m}_{\mathcal{O}}$ we see that for the k-algebra $\overline{A} = A \otimes_{\mathcal{O}} k$, the quotient ring $\overline{A}/(S_1^{p^m}, \ldots, S_n^{p^m})\overline{A}$ is a non-zero free module over $k[[S_1, \ldots, S_n]]/(S_1^{p^m}, \ldots, S_n^{p^m})$. By Lemma 4.1 we see that h is an isomorphism modulo $\mathfrak{m}_{\mathcal{O}}$, and Lemma 3.1 then implies that h is an isomorphism. In particular we see that $\mathcal{O}[[X_1, \ldots, X_n]]/(S_1, \ldots, S_n)$ is finitely generated as an $\mathcal{O}$-module, so that it is a complete intersection. This shows 4.2.

Proof of Criterion II. Let d denote the $\mathcal{O}$-rank of T, and let m be so large that $p^m > n^{n-1}d^n$. By property *(i)* there is a surjection

$$\mathcal{O}[[X_1, \ldots, X_n]] \longrightarrow\!\!\!\!\rightarrow R_m.$$

pp. 343–355 in: *Modular Forms and Fermat's Last Theorem*, Cornell, Silverman, Stevens (eds.), Springer-Verlag 1997.

We now lift the homomorphism $\mathcal{O}[[S_1,\dots,S_n]] \longrightarrow R_m$ to an O-algebra homomorphisms $\mathcal{O}[[S_1,\dots,S_n]] \longrightarrow \mathcal{O}[[X_1,\dots,X_n]]$ and we apply Corollary 4.2 with $A = T_m$. We conclude that the composite map

$$\begin{aligned}\mathcal{O}[[X_1,\dots,X_n]]/(S_1,\dots,S_n) &\twoheadrightarrow R_m/(S_1,\dots,S_n)R_m \\ &\twoheadrightarrow T_m/(S_1,\dots,S_n)T_m\end{aligned}$$

is an isomorphism between complete intersections. It follows from property *(iii)* that φ is an isomorphism between complete intersections as well.

Bibliography

[1] Bruns, W. and Herzog, J.: *Cohen-Macaulay rings*, Cambridge University Press, Cambridge 1993.

[2] De Shalit, E.: Hecke rings and universal deformation rings, these proceedings.

[3] De Smit, B. and Lenstra, H.W.: Finite complete intersection algebras and the completeness radical, Technical Report 96-06, Universiteit van Amsterdam, 1996.

[4] Lang, S.: Algebra, 3rd ed., Addison-Wesley, Reading, Mass., 1993.

[5] Lenstra, H.W.: Complete intersections and Gorenstein rings, In J. Coates and S.T. Yau: *Elliptic curves, modular forms and Fermat's Last Theorem*, International Press, Cambridge 1995.

[6] Mazur, B. and Roberts, L.: Local Euler characteristics, *Invent. Math.* **9** (1970), 201–234.

[7] Ribet, K.: p-adic modular deformations and Wiles' "Main Conjecture", these proceedings.

[8] Tate, J.T.: Homology of Noetherian rings an local rings, *Illinois Math. Journal* **1** (1957), 14–27.

[9] Taylor, R. and Wiles, A.: Ring theoretic properties of certain Hecke algebras, *Annals of Math.* **141** (1995), 553–572.

[10] Wiebe, H.: Über homologische Invarianten lokaler Ringe, *Math. Annalen* **179** (1969), 257–274.

[11] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem, *Annals of Math.* **141** (1995), 443–551.