Ceterum censeo *Descente Infinie* esse disputandam

Ceterum censeo Carthaginem esse delendam.

Hanc marginis exiguitas non caperet.

Claus-Peter Wirth

Diophanti A. Arithmeticorum, Vol. VI, p. 339

Si area trianguli esset quadratus, darentur duo quadratoquadrati quorum differentia esset quadratus; unde sequitur dari duo quadratos quorum et summa et differentia esset quadratus. Datur itaque numerus, compositus ex quadrato et duplo quadrati, aequalis quadrato, ea conditione ut quadrati eum componentes faciant quadratum. Sed, si numerus quadratus componitur ex quadrato et duplo alterius quadrati, eius latus similiter componitur ex quadrato et duplo quadrati, ut facillime possumus demonstrare. Unde concludetur latus illud esse summam laterum circa rectum trianguli rectanguli, et unum ex quadratis illud componentibus efficere basem, et duplum quadratum aequari perpendiculo.

Diophanti A. Arith., Vol. VI, p. 339, contd.

Illud itaque triangulum rectangulum conficietur a duobus quadratis quorum summa et differentia erunt quadrati. At isti duo quadrati minores probabuntur primis quadratis primo suppositis, quorum tam summa quam differentia faciunt quadratum: Ergo, si dentur duo quadrati quorum summa et differentia faciunt quadratum, dabitur in integris summa duorum quadratorum eiusdem naturae, priore minor. Eodem ratiocinio dabitur et minor ista inventa per viam prioris, et semper in infinitum minores invenientur numeri in integris idem praestantes: Quod impossibile est, quia, dato numero quovis integro, non possunt dari infiniti in integris illo minores. Demonstrationem integram et fusius explicatam inserere margini vetat ipsius exiguitas.

SEKIs

SWP-2006-01: Progress in Computer-Assisted Inductive Theorem Proving by Human-Orientedness and *Descente Infinie*?

SWP-2006-02: A Self-Contained and Easily Accessible Discussion of the Method of *Descente Infinie* and Fermat's Only Explicitly Known Proof by *Descente Infinie*

SR-2005-02: Shallow Confluence of Conditional Term Rewriting Systems

DI in Working Mathematician's Style

1. Simplify the conjecture in case analysis.
2. When appropriate:
   Apply conjecture just like a lemma
   (actually: application as an *induction hypothesis*).
3. Search for a single wellfounded ordering in which all induction hypotheses are smaller than the conclusion.

DI: Heuristic Problems?

After *Descente Infinie* had made mathematicians happy for more than two millenia, computer scientist started to worry on heuristic problems in the 1970s.

Invention of the 1970s: Explicit Induction

Idea of Explicit Induction

- Solves the hard tasks of induction already *before* the proof has actually started:

  Hypotheses Task: Martin Protzen: “No solution!” Some heuristic advantage which, however, can be achieved without the price of failure.

  Induction-Ordering Task: Rarely any heuristic advantage. Bad for program synthesis.

- Reduces induction to first-order deduction. But the two are not orthogonal . . .

Is Explicit Induction Good for . . .

. . . **Recursion Analysis?** No! QUODLIBET does it at least as well, even with less restrictive admissibility conditions for the partial definition of recursive functions.

Is Explicit Induction Good for . . .

. . . **Recursion Analysis?** No! QUODLIBET does it at least as well, even with less restrictive admissibility conditions for the partial definition of recursive functions.

. . . **Built-In Arithmetic?** No! QUODLIBET does it better, and its build-in arithmetic even helps to find new needed lemmas.

Is Explicit Induction Good for . . .

. . . **Recursion Analysis?** No! QUODLIBET does it at least as well, even with less restrictive admissibility conditions for the partial definition of recursive functions.

. . . **Built-In Arithmetic?** No! QUODLIBET does it better, and its build-in arithmetic even helps to find new needed lemmas.

. . . **Rippling?** Probably not.

Is Explicit Induction Good for . . .

. . . **Generalization?** No! Only humans with sufficient semantical knowledge can do this well for non-trivial domains.

Is Explicit Induction Good for . . .

. . . **Generalization?** No! Only humans with sufficient semantical knowledge can do this well for non-trivial domains.

. . . **Human-Interaction?**

Krchrchrch.

QUODLIBET provides the Flexibility...

... needed for searching for hard induction proofs:

- Generation of induction hypotheses:
  eager / lazy / mutual
- Choice of induction Ordering: eager / lazy
- Open lemmas
- Alternative proof attempts in parallel:
  forest of and/or-trees

The fundamental practical advantage of *DI*

Constraints of the inductive proof search can now be solved together with all other constraints of the whole deduction in any suitable order.

What price do we have to pay for *DI*?

- It comes for free!

- „Eine neue wissenschaftliche Wahrheit pflegt sich nicht in der Weise durchzusetzen, daß ihre Gegner überzeugt werden und sich als belehrt erklären, sondern viel mehr dadurch, daß die Gegner allmählich aussterben und daß die heranwachsende Generation von vornherein mit der Wahrheit vertraut gemacht ist.“

Max Planck, Wissenschaftliche Selbstbiographie, Johann Ambrosius Barth (Leipzig, 1948), p. 22.

Conclusion

- While the heuristics developed within the paradigm of explicit induction remain the method of choice for routine tasks, explicit induction is an obstacle to progress in program synthesis and in the automation of difficult proofs, where the proper induction axioms cannot be completely guessed in advance.

Conclusion

- While the heuristics developed within the paradigm of explicit induction remain the method of choice for routine tasks, explicit induction is an obstacle to progress in program synthesis and in the automation of difficult proofs, where the proper induction axioms cannot be completely guessed in advance.
- Shifting to the paradigm of descente infinie overcomes this obstacle without sacrificing previous achievements.

Fermat's Theorem, Observations XLV

- The area of a non-trivial Pythagorean triangle with integer sides lengths is not a square of a natural number.
- If $x_0, x_1 \in \mathbf{N}_+$ and $x_2, x_3 \in \mathbf{N}$ and $x_0^2 + x_1^2 = x_2^2$, then $x_0 x_1 \neq 2x_3^2$.

Fermat's Proof, Modern Version

Corollary 1 $(x = 0) \vee (y \mid z)$ *iff* $xy \mid xz$.

Lemma 2 (Euclid's Elements, Proposition VII.30)

If p *is prime and* $p \mid x_1 x_2$, *then* $p \mid x_1$ *or* $p \mid x_2$.

Lemma 3 (Euclid's Elements, Proposition VIII.14)

$x \mid y$ *iff* $x^2 \mid y^2$.

Lemma 4 *If* a, b *are coprime and* $ab = x^2$,
then there are coprime y, z *with* $a = y^2$, $b = z^2$, *and* $x = yz$.

Lemma 5

$l_1, \ldots, l_n$ *are not coprime iff* $\exists p$ *prime.* $\forall i \in \{1, \ldots, n\}.\ (p \mid l_i)$.

Lemma 6 *Suppose* $a \succeq b$, $x \mid a-b$, *and* $x \mid a+b$. *Then we have:*

(1) $x \mid 2a$ *and* $x \mid 2b$.

(2) If a, b *are coprime, then* $x \preceq 2$.

Fermat's Proof, Modern Version

Lemma 7

If p, q are coprime with $p \succeq q$, then pq, p^2-q^2 are coprime, and pq, p^2+q^2 are coprime.

Corollary 8 *If $x_0^2 + x_1^2 = x_2^2$ and x_0, x_1, x_2 are coprime, then, for some $i \in \{0,1\}$, there are coprime p, q such that one of them is odd and one of them is even, $p \succ q$, $x_i = 2pq$, $x_{1-i} = p^2-q^2$, and $x_2 = p^2+q^2$.*

Corollary 9 *If $x_0^2 + 2x_1^2 = x_2^2$ and x_0, x_1, x_2 are coprime, then there are $m \in \mathbf{N}$ and $k \in \mathbf{N}_+$ such that $2m, k$ are coprime, $2m^2 \neq k^2$, $x_0 = |2m^2-k^2|$, $x_1 = 2mk$, and $x_2 = 2m^2+k^2$.*

Fermat's Proof, Modern Version

We show the theorem by *descente infinie*:

- Assuming the existence of x_0, x_1, x_2, x_3 with $x_0, x_1 \in \mathbf{N}_+$ and $x_0^2 + x_1^2 = x_2^2$ and $x_0 x_1 = 2x_3^2$,
- we show the existence of y_0, y_1, y_2, y_3 with $y_0, y_1 \in \mathbf{N}_+$ and $y_0^2 + y_1^2 = y_2^2, \quad y_0 y_1 = 2y_3^2$, and $y_2 \prec x_2$.

Fermat's Proof, Modern Version

First, let us consider the case that there is some prime number z that divides x_0, x_1, i.e. that there are y_i with $x_i = zy_i$ for $i \in \{0, 1\}$.
Then we have $z^2(y_0^2 + y_1^2) = x_2^2$, i.e. $z^2 \mid x_2^2$. By Lemma 3, we get $z \mid x_2$. Thus, there is some $y_2 \in \mathbf{N}_+$ with $x_2 = zy_2$.
Then we also have $z^2(y_0^2 + y_1^2) = z^2 y_2^2$, i.e. $y_0^2 + y_1^2 = y_2^2$. Moreover, we have $z^2 y_0 y_1 = 2x_3^2$, i.e. $z^2 \mid 2x_3^2$. As z is prime, from the latter we get $z \mid 2$ or $z \mid x_3^2$ by Lemma 2.
By Corollary 1, $z = 2$ and $z^2 \mid 2x_3^2$ implies $z \mid x_3^2$.
Thus, we have $z \mid x_3^2$ in both cases, and then $z \mid x_3$ by Lemma 2 again. Thus, as $x_3 \in \mathbf{N}_+$, there is some y_3 with $x_3 = zy_3$.
Then $z^2 y_0 y_1 = 2x_3^2 = z^2 2y_3^2$, i.e. $y_0 y_1 = 2y_3^2$.
From $x_i \in \mathbf{N}_+$ we get $y_i \in \mathbf{N}_+$ for $i \in \{0, 1, 2, 3\}$. Finally, we have $y_2 \prec x_2$, which finishes this case by *descente infinie*.

Fermat's Proof, Modern Version

Thus, we may assume x_0, x_1 to be coprime by Lemma 5, and—a fortiori— x_0, x_1, x_2 to be coprime, too.

Claim I: There are coprime p, q such that one of them is odd and one of them is even, $p \succ q$, and there are some c, e, f with $x_2 \succ e \succ f \succ 0$ such that

$$p = e^2, \quad q = f^2, \text{ and } p^2 - q^2 = c^2.$$

Fermat's Proof, Modern Version

Proof of Claim I: By Corollary 8 there are coprime p and q such that one of them is odd and one of them is even and, for some $i \in \{0,1\}$, $p \succ q$, $x_i = 2pq$, $x_{1-i} = p^2 - q^2$, and $x_2 = p^2 + q^2$. Due to $x_i \in \mathbf{N}_+$, we have $p, q \in \mathbf{N}_+$. From $x_0 x_1 = 2x_3^2$, we get $2pq(p^2 - q^2) = 2x_3^2$, i.e. $pq(p^2 - q^2) = x_3^2$. By Lemma 7, we know that pq and $p^2 - q^2$ are coprime, too. Thus, by Lemma 4 there must be some coprime $b, c \in \mathbf{N}_+$ with $x_3 = bc$, $pq = b^2$, and $p^2 - q^2 = c^2$. By the coprimality of p, q, due to $pq = b^2$, by Lemma 4 there must be some coprime $e, f \in \mathbf{N}_+$ with $b = ef$, $p = e^2$, and $q = f^2$. Moreover $e \succ f \succ 0$, as $e \preceq f$ would imply the contradictory $p \preceq q$. Furthermore, from $q \in \mathbf{N}_+$, we get $x_2 = p^2 + q^2 \succ p^2 = e^4 \succeq e$. Q.e.d. (Claim I)

Fermat's Proof, Modern Version

Claim II: There are coprime $g, h \in \mathbf{N}_+$ and some e, f with $x_2 \succ e \succ f \succ 0$ such that

$$e^2+f^2=g^2 \text{ and } e^2-f^2=h^2.$$

Proof of Claim II: Note we will not use any information on the current proof state besides Claim I here. By Claim I, $p+q, p-q \in \mathbf{N}_+$. By Claim I and Lemma 6(2), the only prime that may divide both $p+q$ and $p-q$ is 2; but this is not the case because one of p, q is even and one is odd. Thus, by Lemma 5, $p+q, p-q$ are coprime and due to $(p+q)(p-q)=p^2-q^2=c^2$, by Lemma 4, there are coprime $g, h \in \mathbf{N}_+$ with $c=gh$, $p+q=g^2$, $p-q=h^2$. Q.e.d. (Claim II)

Fermat's Proof, Modern Version

As in Fermat's original proof the induction hypothesis is not the theorem, but Claim II, let us forget anything about the current proof state but Claim II here. The following two Claims are trivial in the context of Claim II:

Claim IIa: $h^2+2f^2=g^2$.

Claim IIb: $h^2+f^2=e^2$.

Fermat's Proof, Modern Version

As g, h are coprime, h, f, g are coprime, too. Thus, by Claim IIa and Corollary 9, there are m, k such that $2m, k$ coprime, $h = |2m^2 - k^2|$, $f = 2mk$, and $g = 2m^2 + k^2$. Set $y_0 := 2m^2$, $y_1 := k^2$, $y_2 := e$, $y_3 := mk$. By Claim II we have $x_2 \succ y_2 \succ 0$. As $f \in \mathbf{N}_+$, we have $m, k \in \mathbf{N}_+$, and $y_0, y_1, y_3 \in \mathbf{N}_+$. Moreover, we have $y_0 y_1 = 2y_3^2$, $g = y_0 + y_1$, and $f^2 = 2y_0 y_1$. Finally, by Claim IIa and Claim IIb, we have $y_0^2 + y_1^2 = (y_0 + y_1)^2 - 2y_0 y_1 =$

$$g^2 - f^2 \underset{\text{(IIa)}}{=} h^2 + 2f^2 - f^2 = h^2 + f^2 \underset{\text{(IIb)}}{=} e^2 = y_2^2.$$ **Q.e.d. (Theorem)**

Fermat's Proof, Annotated Translation

If the area of a [*right-angled*] triangle were a square, there would be given two squares of squares of which the difference were a square [*Claim I*]; whence it follows that two squares would be given, of which both the sum and the difference would be squares [*Claim II*]. And thus a number would be given, composed of a square and the double of a square, equal to a square [*Claim IIa*], under the condition that the squares composing it make a square [*Claim IIb*].

Fermat's Proof, Annotated Translation

But, if a square number is composed of a square and the double of another square, its side [*i.e. its square root* g] is similarly composed of a square and the double of a square [$g = k^2 + 2m^2$], as we can most easily demonstrate [*Corollary 9*].

Fermat's Proof, Annotated Translation

Whence one concludes that this side $[g]$ is the sum of the sides $[y_0, y_1]$ about the right angle of a triangle $[g = y_0 + y_1,\ y_0^2 + y_1^2 = y_2^2]$, and that one of the squares composing it constitutes the base $[k^2 = y_1]$, and the double square is equal to the perpendicular $[2m^2 = y_0]$.

Fermat's Proof, Annotated Translation

[*Instead of applying the theorem as induction hypothesis now, Fermat descends the inductive reasoning cycle until Claim II can be applied as induction hypothesis.*]

Hence, this right triangle is composed of two squares of which the sum and difference are squares. But these two squares will be proved to be smaller than the first squares initially posited, of which the sum as well as the difference also made squares: therefore, if two squares are given of which the sum and the difference are squares, there exists in integers the sum of two squares of the same nature, less than the former [e^2+f^2].

Fermat's Proof, Annotated Translation

[*Finally Fermat illustrates the Method of Descente Infinie.*]

By the same argument there will be given in the prior manner another one less than this, and smaller numbers will be found indefinitely having the same property. Which is impossible, because, given any integer, one cannot give an infinite number of integers less than it.

The smallness of the margin forbids to insert the proof completely and with all detail.

Conclusion

- Is this a proof?