

THE GENERALIZATION OF PROOFS AND CALCULATIONS
Matthias Baaz

In this lecture, we discuss the logical generalization of proofs and calculations. Consider the following famous calculation by Euler demonstrating that the 5. Fermat number $F_5 = 2^{2^5} + 1$ is compound:

$$\begin{aligned}
 5 \cdot 2^7 + 1 &\equiv 0 \pmod{5 \cdot 2^7 + 1} \\
 5 \cdot 2^7 &\equiv -1 \pmod{5 \cdot 2^7 + 1} \\
 5^4 \cdot 2^7 &\equiv 1 \pmod{5 \cdot 2^7 + 1} \\
 5^4 + 2^4 &= 5 \cdot 2^7 + 1 \\
 5^4 &\equiv -2^4 \pmod{5 \cdot 2^7 + 1} \\
 1 \equiv 5^4 \cdot 2^{7 \cdot 4} &\equiv \underbrace{-2^4 \cdot 2^{7 \cdot 4}}_{-2^{25}} \pmod{\underbrace{(5 \cdot 2^7 + 1)}_{641}}
 \end{aligned}$$

Can this calculation be applied to other/all Fermat $F_n = 2^{2^n} + 1$, $n > 5$? In this lecture we will show that the calculation above cannot be extended to other Fermat numbers, but if the condition

$$5^4 + 2^4 = 5 \cdot 2^7 + 1$$

is replaced by the condition

$$5^4 + 2^4 \equiv 0 \pmod{5 \cdot 2^7 + 1}$$

then all Fermat numbers F_n , $n \geq 5$ can be shown to be compound in this way. This lecture provides a comprehensive introduction to this topic

- 1. unit** Introduction to proof theory, cut-elimination, proof diagrams and skeletons of proofs, reconstruction of proofs and Herbrand disjunctions
- 2. unit** generalizations of especially simple form for cut-free proofs w.r.t. skeletons, Kreisel's conjecture for finitely axiomatized number theories
- 3. unit** generalizations in the presence of schemata for order induction, successor induction and identity, generalization w.r.t. blockwise introductions of quantifiers, the splitting criterion for systems with one-placed function symbols

4. **unit** the (un)provability of k-provability in the general case, applications of Gentzen's second consistency proof, representation theorems
5. **unit** the generalization of quantifier free proofs and calculations w.r.t. underlying semantical interpretations.

References:

Matthias Baaz. *Note on the generalization of calculations*. Theoretical Computer Science 224 (1999), 3–11.