From classical arithmetics to information science: some applications of abstract research

Michel Waldschmidt

Institut de Mathématiques de Jussieu

Université Pierre et Marie Curie

miw@math.jussieu.fr

http://www.math.jussieu.fr/∼miw/

March 21, 2006

Abstract

Theoretical research in number theory has a long tradition, in particular in India and in France. Since many centuries, the main goal of these investigations is a better understanding of the abstract theory. Numbers are basic not only for mathematics, but more generally for all sciences; a deeper knowledge of their properties is fundamental for further progress. Remarkable achievements have been obtained, especially recently, as many conjectures have been settled. Yet, a number of old questions still remain open.

Among the unexpected features of recent developments in technology are the connections between classical arithmetic on the one hand, and new methods for reaching a better security of data transmission on the other. We will illustrate this aspect of the subject by showing how modern cryptography is related to our knowledge of some properties of natural numbers. As an example, we explain how prime numbers play a key role in the process which enables you to withdraw safely your money from your bank account using your PIN (Personal Identification Number) secret code.