Bemerkungen zur Einordnung meiner Vorlesung (VL) anlässlich einer Frage zur Zweckmäßigkeit der Anwendung des chinesischen Restsatzes (chR) bei der Multiplikation großer ganzer Zahlen.

- In meiner VL stehen mathematisch-methodische Grundlagen der Computeralgebra (CA) im Mittelpunkt. Das zweite Standbein - die informatische, implementierende und kompexitätsanalysierende Komponente - wird zwar als Rechtfertigung für die Inhalte der VL herangezogen, aber ansonsten allenfalls in Form von Beispielen und Literaturhinweisen behandelt. (Vgl. die analogen einleitenden Hinweise in der ersten VL.)

- Die VL ist - obwohl in der Masterphase - eine erste VL zum Thema CA und muss an den durchschnittlich vorhandenen Vorkenntnissen insbesondere im Bereich Algebra ansetzen. Weitergehendes muss in der VL zumindest aufbereitet und zunehmend auch hergeleitet werden.

- Die exakte Arithmetik für Polynome und ganze Zahlen ist letztlich die Grundlage aller höheren Verfahren der CA. In dieser computeralgebraischen Arithmetik spielen der raffinierte Wechsel zwischen verschiedenen Darstellungen der Rechenobjekte (insbesondere die Division mit Rest bezüglich verschiedener Moduli, der chR und die diskrete Fouriertransformation), die Ausnutzung darstellungspezifischer Rechenverfahren, algorithmische Strategien (wie z.B. das so genannte „Teilen und Herrschen“ beim Verfahren von Karatsuba oder der schnellen Matrizenmultiplikation) und besondere Implementierungstechniken die zentrale Rolle.

  Das ganze Kapitel I der VL bietet einfache methodentypische Beispiele zu diesem stärker informatisch gefärbten Themenkreis. Die klassische Literaturangabe für „alles“ in diesem Kapitel ist zunächst [K] und dann seit einigen Jahren bereits [GaGe].

- Letzteres gilt auch hinsichtlich der **schnellen Multiplikation großer ganzer Zahlen** und der **Bedeutung des chR dabei**:

  [K] 4.3.2 Modular Arithmetic, 4.3.3 How fast can we multiply,
  4.3.3 B: A Modular Method (hier wird ein Verfahren von Schönhage besprochen). Knuth beginnt den Absatz so:
  „It is very hard to believe at first that this method can be of advantage, since ...“ (p. 287).
  4.3.3 C: Hier wird das berühmte Verfahren von Schönhage und Strassen von 1971 besprochen, das u.A. mit DFT (siehe entsprechendes Beispiel in Kapitel I) arbeitet.

  In [GaGe] (2003) ist das Verfahren von Schönhage und Strassen immer noch i.W. der Höhepunkt. Ihm wird ein (u.A.) chR-gestütztes so genanntes three-prime-Verfahren gegenübergestellt. Dort finden sich auch experimentelle Vergleiche.

  Erst 2007 erscheint der Aufsehen erregende Artikel „Faster Integer Multiplication“ von Martin Fürer, der sogar in der deutschen Presse ein Echo fand (Zeit vom 27. 11. 2008).

  Fürer beginnt übrigens seinen Artikel mit dem Satz:
  „All known methods for integer multiplication (except the trivial school method) are based on some version of the Chinese Remainder Theorem.“