Mathematik ist überall

Prof. Dr. Wolfram Koepf

Universität Kassel
http://www.mathematik.uni-kassel.de/~koepf

Tag der Mathematik
15. Februar 2008
Universität Kassel

Inhaltsangabe

- Sichere Verschlüsselung
- Das RSA-Verfahren
- Prüfzeichenverfahren
- Fehlerkorrigierende Verfahren
- Wo kann man dies nachlesen?

Was ist Kryptologie?

Alles Wissen

- Am 10. Januar 2007 war Verborgene Welten das Thema der Sendung Alles Wissen im dritten Fernsehprogramm des HR.
- Für einen Beitrag zu dieser Sendung wurde auch ich interviewt, und zwar zum Thema Kryptologie.
- Als kurzen Einblick in dieses aktuelle Forschungsgebiet sehen wir uns den fünfminütigen Beitrag über Kryptologie an.

Wie geht es im Vortrag weiter?

- In der Folge werde ich einige wesentlichen Aspekte asymmetrischer Kryptosysteme vorstellen.

Verschlüsselungsverfahren

Verschlüsselungsverfahren

- Bei einem Verschlüsselungsverfahren wird eine Nachricht N mit Hilfe einer Funktion E und eines Schlüssels e verschlüsselt
$$K = E_e(N) .$$
- Die Dekodierung erfolgt mit der (zugehörigen) Funktion D und dem Schlüssel d:
$$D_d(K) = D_d(E_e(N)) = N .$$
- Die Funktionen E und D sollten effizient berechnet werden können.
- Ein Problem ist die Schlüsselübergabe.

Asymmetrische Kryptographie

Asymmetrische Kryptographie

- Das RSA-Verfahren (Rivest, Shamir und Adleman (1978)) ist ein Beispiel eines *asymmetrischen* Verschlüsselungsverfahrens. Internet-Check
- Solche Verfahren wurden 1976 von Diffie und Hellman eingeführt. Internet-Check
- Hierbei verwenden Sender und Empfänger *jeweils eigene* Schlüssel e und d.
- Der Schlüssel e wird jeweils öffentlich bekannt gegeben, während der Schlüssel d geheim bleibt.
- Ein Schlüsselaustausch des jeweils persönlichen Dekodierungsschlüssels d ist demnach nicht erforderlich.

Das RSA-Verfahren

Wo wird das RSA-Verfahren eingesetzt?

- Das RSA-Verfahren wird bei der sicheren Anmeldung auf einem entfernten Computer benutzt (secure shell (`ssh`)).
- Es verbirgt sich hinter sicherer E-Mail mit dem Verfahren PGP (Pretty Good Privacy). Internet-Check
- Es wird verwendet beim sicheren Datentransfer auf *sicheren Webseiten* (`https`), beispielsweise beim Online-Banking. Internet-Check
- Also: Interneteinkauf und Online-Banking (mit `https`!) können wirklich sicher sein.
- Wir wollen das RSA-Verfahren an einem Beispiel testen. zum RSA-Test

Prüfzeichenverfahren

Prüfzeichenverfahren

- Bei einem Prüfzeichenverfahren wird einer Folge von Ziffern ein weiteres Zeichen hinzugefügt, das einer Bedingung genügt.
- Überprüft man diese Bedingung, so kann man erkennen, ob eine fehlerhafte Übertragung vorliegt.

Beispiel (Internationale Buchnummer)

- Eine ISBN besteht aus 9 Ziffern und einem Prüfzeichen. Das Prüfzeichen kann eine von 11 Ziffern sein, ggfs. X.
- Die ISBN wird allerdings gerade auf ein 13-stelliges System umgestellt. Internet-Check
- Beispiel

Prüfzeichenverfahren

Beispiel (Europäische Artikelnummer)

- Ein Scanner an einer Ladenkasse scannt das Muster ein.
- Es wird die 13-stellige EAN ausgelesen.
- Ob der Leseversuch erfolgreich war, kann man überprüfen, denn das 13. Zeichen ist ein Prüfzeichen.
- Ein einzelner Lesefehler wird in jedem Fall erkannt.

Fehlerkorrigierende Verfahren

Fehlerkorrigierende Codes

- Bei einem fehlerkorrigierenden Code werden einer Folge von Ziffern zwei weitere Zeichen hinzugefügt, die zwei Bedingungen genügen.
- Überprüft man beide Bedingungen, so kann man erkennen,
  - an welcher Position eine fehlerhafte Übertragung vorliegt
  - und wie groß der Fehler ist.

  Man kann also einen Fehler korrigieren.
- In analoger Weise können mit komplizierteren fehlerkorrigierenden Codes durch Hinzufügen weiterer Redundanz mehrere Fehler in einem Ziffernblock korrigiert werden.

Fehlerkorrigierende Verfahren

Beispiel (Compact Disc)

- Dies wird beim Lesen einer Musik-CD extensiv genutzt.
- Ohne fehlerkorrigierende Codes gäbe es bei der CD keinerlei Musikgenuss.
- Eine zerkratzte CD kann Hunderttausende von Fehlern enthalten!
- Bei einer CD-ROM darf es (nach der Fehlerkorrektur!) überhaupt keine Lesefehler mehr geben!

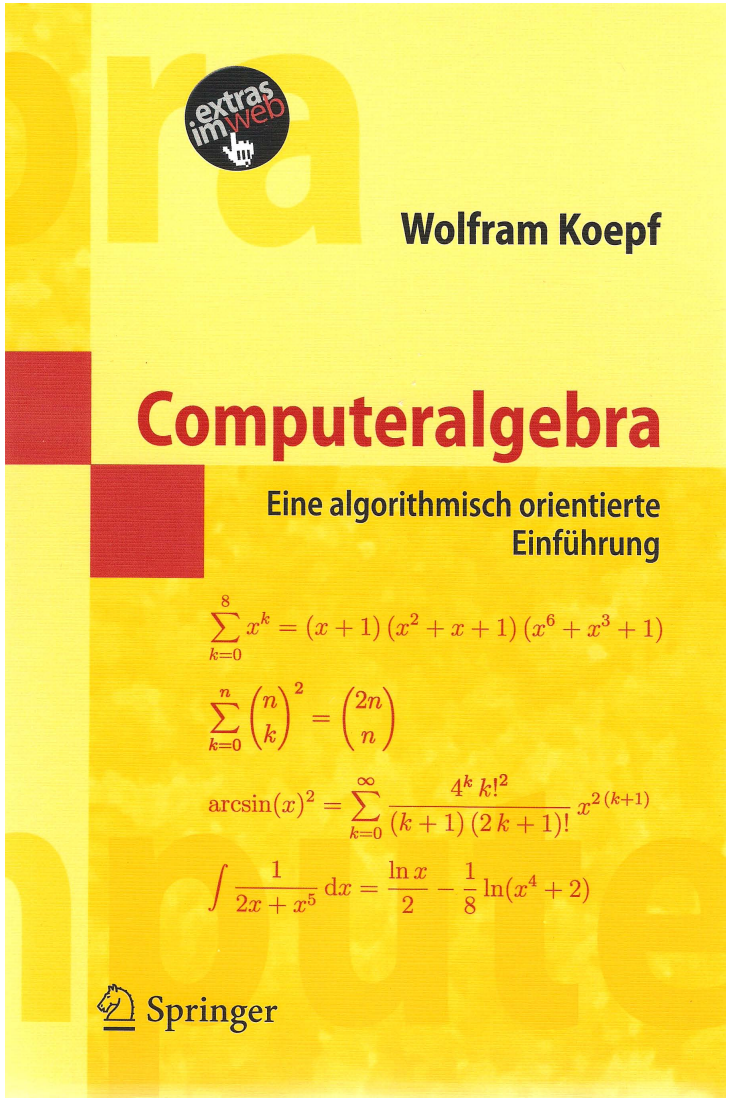
Beispiel (Reed-Solomon-Code)

Wir sehen uns als Beispiel einen 2-fehlerkorrigierenden Reed-Solomon-Code an. Beispiel

Die vorgestellten Programme wurden entwickelt für mein Buch

Computeralgebra
Eine algorithmisch orientierte Einführung
Springer, Berlin/Heidelberg, 2006

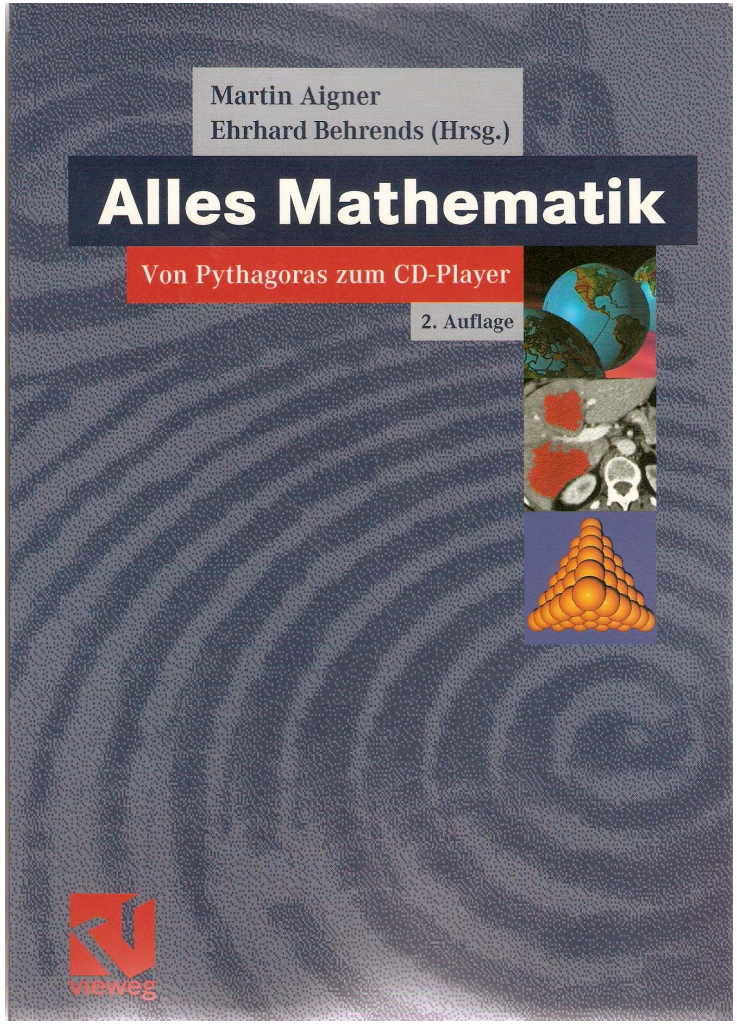
und können von meiner Homepage heruntergeladen werden:



http://www.mathematik.uni-kassel.de/~koepf/CA

Viele weitere Anwendungsbeispiele, die zeigen, wo in der heutigen Gesellschaft überall Mathematik eine Rolle spielt, findet man in dem Buch

Martin Aigner, Ehrhard Behrends:
Alles Mathematik
Von Pythagoras zum CD-Player
Vieweg, Braunschweig/Wiesbaden,
2000/2002



Finale

Erkenntnisse

Ich hoffe, mein Vortrag hat Ihnen Folgendes gezeigt:

- Mit geeigneten mathematischen Algorithmen kann man eine sichere Datenübertragung erreichen.
- Also: Interneteinkauf, Online-Banking (mit `https`!), Computerzugriff von Ferne (`ssh`) etc. kann wirklich sicher sein.
- Mit Mathematik können wir lebenspraktische Probleme lösen. Und dies waren nur einige Beispiele von vielen.
- Auch Pay-TV, MP3-Player, Bildkompression (`jpg`), Handys, Satelliten, Navigationsgeräte, Computertomographen und vieles mehr funktionieren nur mit „Mathe inside“!
- Mathematik macht Spaß!

Vielen Dank für Ihr Interesse und weiterhin viel Spaß beim Tag der Mathematik!