

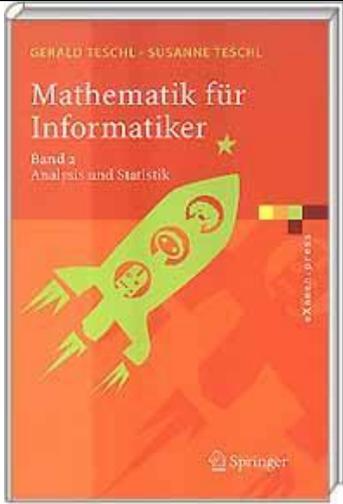
Diskrete Mathematik (AI, 3. Sem)

Kommentiertes Literaturverzeichnis

[Download als PDF](#)

Bücher zur Vorlesung

Es existieren zahlreiche Bücher, welche die in der Vorlesung behandelten Themen abdecken, ja sogar meist viel mehr als das bieten.

	<p>[Teschl05] Teschl, Gerald und Teschl, Susanne "Mathematik für Informatiker" Springer Verlag Bd. 1, Diskrete Mathematik, Juli 2005, 25 € Sehr gute Stoffpräsentation, viele aktuelle Anwendungsbsp. für Informatiker, griffige Erklärungen. S. 91ff: (erweiterter) Euklid-Algo und diophantische Gleichungen, Chinesischer Restsatz. S. 74ff: Hashfunktionen.</p> <p>Alle Kapitel online verfügbar (PDF) unter SpringerLink an FHK.</p>
--	---

Online-Materialien

CrypTool ist ein umfangreiches Lernprogramm (Uni Siegen + Uni Darmstadt) zu Kryptographieverfahren und Zahlentheorie

www.cryptool.de

Einige Beispiele

- Einzelverfahren – Zahlentheorie interaktiv... – Lernprogramm Zahlentheorie
- Einzelverfahren – Anwendung Chinesischer Restsatz – Astronomie
- Besonders interessant ist auch das zu CrypTool gehörige Skript als PDF „Kryptographie, Mathematik und mehr“ (über 200 Seiten)
- [Esslinger07] Esslinger, B und das CrypTool-Team: Kryptologie mit CrypTool V1.4.10 - Einführung in Kryptographie und Kryptoanalyse: Umfang, Technik und Zukunft von CrypTool. Als PDF im CrypTool-Verzeichnis nach Installation verfügbar.

Interessante JavaScripts und Java-Applets rund um Primzahlen, insbesondere Lösungsverfahren für lineare diophantische Gleichungen mit mehr als 2 Variablen:

www.ardt-bruenner.de/mathe/scripts/diophant.htm

Schön sind auch in vielen Fällen die "Algorithmen der Woche" aus dem [Informatikjahr 2006](#): Viele davon befassen sich mit Themen der Diskreten Mathematik, für uns besonders interessant ist das Teilen von Geheimnissen

J. Blömer: „Teilen von Geheimnissen“, 28. Algorithmus der Woche im Informatikjahr 2006. <http://www-i1.informatik.rwth-aachen.de/~algorithmus/algo28.php>.



Multimediale Lernhilfen zum Mathematikstoff für die Oberstufe und die Universität, mathematische Hintergründe, ein mathematisches Lexikon, interaktive Tests und weitere Mathe-Links stehen auf der schönen Seite

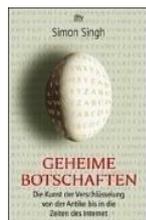
www.mathe-online.at

Allgemeines über die Mathematik bietet die Seite

www.mathematik.de

Weiterführende Literatur

[Aigner96] Martin Aigner: *Diskrete Mathematik*. Vieweg Verlag, 2. Auflage, 1996. Weiterführende Informationen zu Graphentheorie, Kombinatorik und anderen Themen der Diskreten Mathematik. Vom Niveau her etwas anspruchsvoller, aber noch gut lesbar. Viele Aufgaben, z.T. mit Lösungen. Bringt den Beweis zum Satz von Euler.



[Singh01] Simon Singh: *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*. Dtv, 2001. Ein sagenhaft gutes Buch!. Absolut spannend wird die Geschichte der Verschlüsselung von der Antike bis heute aufgerollt. Gleichzeitig erfährt man viel über die dahinterstehenden mathematischen Verfahren der Kryptographie und der Codierung, modulare Arithmetik ohne Formeln usw.

[Vöcking08] Vöcking, B.; Alt, H. et al. (Hrsg.) **Taschenbuch der Algorithmen**, Reihe: [eXamen.press](#), 448 Seiten, 20€, Springer, Berlin Heidelberg, 2008. Ein Kapitel daraus (Friedrich Eisenbrand, Uni Paderborn) erklärt gut den Euklidischen Algorithmus und seine Komplexität. Alle Kapitel online verfügbar unter SpringerLink an FHK.

[Shamir79] Shamir, A.: How to share a secret, Comm. of the ACM, 22, p. 612-613, Nov. 1979.
http://lardedbucket.org/blog/wp-content/uploads/2007/10/shamir_how_to_share_a_secret.pdf.