El. Math. *51* (1996) 0013-6018/96/010043-02$1.50 + 0.20/0

Bücher und Computersoftware

P. Giblin: Primes and Programming – An Introduction to Number Theory with Computing. vi + 235 pages, relié, $ 44.95, broché, $ 19.95. Cambridge University Press, 1993; ISBN 0-521-40182-8, ISBN 0-521-40988-8.

F. Ischebeck: Einladung zur Zahlentheorie. 192 pages, CHF 26.80. Bibliographisches Institut Wissenschaftsverlag, Mannheim, Zürich 1992; ISBN 3-411-15451-9.

La théorie des nombres présente actuellement un intérêt grandissant pour le maître de mathémathiques enseignant au niveau gymnasial. Cette discipline longtemps considérée par les mathématiciens eux-mêmes comme la quintessence de la pureté de leur science, s'ouvre maintenant aux applications, notamment par le truchement de la conservation du secret dans le vaste secteur des communications. La théorie des nombres fournit aussi l'occasion – le prétexte – d'une bonne entrée en matière d'algorithmique; on sait qu'on aboutit souvent à des résultats intéressants avec des programmes informatiques de quelques lignes seulement. L'aisance que l'ordinateur apporte, par son utilisation didactique dans la salle de cours, permet de multiplier des expériences numériques dont l'objet est facilement accessible aux élèves et qui contribuent fortement au développement de leurs facultés imaginatives. Toutefois, les conjectures ainsi formulées ne deviendront des certitudes que si une déduction correcte peut venir les justifier; les grandes vertus de la démarche mathématique n'en seront que mieux comprises. La théorie des nombres peut aussi servir d'illustration privilégiée aux notions mathématiques un peu plus générales que l'enseignement gymnasial s'efforce d'intégrer, depuis quelques années déjà, avec parfois plus ou moins de bonheur.

La parution d'ouvrages accessibles consacrés à la théorie des nombres constitue donc, en soi, un apport bienvenu à la littérature mathématique sur laquelle se penchent volontiers les enseignants soucieux de conserver dynamisme, efficacité et satisfaction dans l'exercice de leur activité pédagogique. Les deux livres mentionnés ici participent pleinement de cette vision des choses. Comme on va le voir, ils sont, en quelque sorte, complémentaires. Leur lecture est agréable; chacun d'eux apporte à ses lecteurs des bases solides et suffisamment étendues de théorie des nombres, illustrées par des exercices variés, sélectionnés à bon escient.

Comme son titre le laisse supposer, le premier de ces deux ouvrages est davantage consacré aux nombres premiers et au développement d'algorithmes relatifs à la théorie des nombres. Il se compose de 11 chapitres:

The Fundamental Theorem, Greatest Common Divisors and Least Common Multiples
Listing Primes
Congruences
Power and Pseudoprimes
Miller's Test and Strong Pseudoprimes
Euler's Theorem, Orders and Primality Testing
Cryptography
Primitive Roots
The Number of Divisors d and the Sum of Divisors σ
Continued Fractions and Factoring
Quadratic Residues

complétés par un index des notations, par une liste de programmes développés et par une assez riche bibliographie (livres et articles de revues) comprenant 81 titres.

Les exercices, bien incorporés au texte, sont d'un très grand intérêt. Tout en éclairant fort judicieusement le propos de l'auteur, ils augmentent de manière appréciable les connaissances et surtout les performances du lecteur. A côté des *Exercises*, de caractère plus théorique, des *Computing exercises* incitent à la programmation tandis que des *Projects* invitent à des recherches personnelles plus approfondies tout en apportant des matériaux précieux pour un enseignement donné dans l'esprit préconisé par *Geometrie von Fall zu Fall* de Hans Rudolf Schneebeli.

Les exemples de programmes proposés sont rédigés en Turbo Pascal. L'auteur a ainsi pris le parti, tout à fait honorable, de privilégier l'explication sur la performance et le spectaculaire. Le lecteur ne s'en plaindra pas. Au demeurant, il conservera toute liberté de s'en inspirer lorsqu'il voudra effectuer des expériences sur des entiers de plus grande taille, en recourant à des logiciels très performants, tel que *Mathematica*, par exemple.

Quant au livre de F. Ischebeck, il donne une présentation des éléments de théorie des nombres qui est davantage axée sur la terminologie – et les méthodes – de l'algèbre dite moderne; une orientation également très fructueuse pour l'enseignement gymnasial contemporain. Il se compose de 16 chapitres:

Der Ring $\mathbb{Z}$ der ganzen Zahlen

Untergruppen von $\mathbb{Z}$, grösster gemeinsamer Teiler

Eindeutige Primfaktorzerlegung

Primzahlen

Restklassen, Kongruenz, Restklassenringe von $\mathbb{Z}$

Zyklische Gruppen

Faktorgruppen, Restklassenringe und Homomorphismen

Direkte Produkte, Chinesischer Restsatz

Polynomringe, $(\mathbb{Z}/p)^*$

$(\mathbb{Z}/p^n)^*$

Das quadratische Reziprozitätsgesetz

Etwas mehr über Ringtheorie

Der Gausssche Zahlenring und Summen zweier Quadrate

Der Satz von Lagrange

Pythagorastripel, Fermatvermutung für den Exponenten 4

Die Fermatvermutung für den Exponenten 3

complétés par une annexe d'une vingtaine de pages sur la construction des nombres naturels et des nombres entiers, par une liste chronologique de 67 mathématiciens nés avant 1900 et qui ont contribué de manière significative au développement de cette matière, ainsi que par une liste de références bibliographiques portant sur 29 livres.

Les exercices, moins nombreux que dans le livre de P. Giblin mais également fort bien choisis, sont placés en fin de chapitre avec, cas échéant, quelques indications quant à leur résolution. Leur nature est assez variéé et – ce qui n'est pas un mal – certains exercices débouchent même sur des aspects plus ludiques de la théorie des nombres.

Ces deux ouvrages constituent incontestablement une manne très précieuse pour l'enseignant; la qualité de leur présentation et la modicité de leur prix devraient leur permettre de trouver une place – de choix – dans toute bibliothèque personnelle.

Pierre Bolli, Le Vaud

Typesetting & Layout: *mathScreen online, CH-4123 Allschwil*