LỜI NÓI ĐẦU

Trong những năm gần đây, sự phát triển của Tin học đã làm thay đổi nhiều ngành truyền thống của Lí thuyết số (trong cuốn sách này, chúng ta thường dùng từ "Số học"). Nếu như trước thập kỷ 70, số học vẫn được xem là một trong những ngành lí thuyết xa rời thực tiễn nhất, thì ngày nay, nhiều thành tựu mới nhất của số học có ứng dụng trực tiếp vào các vấn đề của đời sống, như thông tin, mật mã, kĩ thuật máy tính. Một phương hướng mới của số học ra đời và phát triển mạnh mẽ: số học thuật toán. Có thể nói, đó là chiếc cầu nối giữa số học với tin học. Với việc sử dụng rộng rãi máy tính trong nghiên cứu số học, nhiều người cho rằng, số học ngày nay đã thành một khoa học thực nghiệm! Điều đó thể hiện khá rõ trong những "thuật toán xác suất" được đề cập đến trong cuốn sách này.

Mục đích của cuốn sách nhỏ này là cung cấp cho người đọc một số kiến thức sơ bộ về số học thuật toán. Cuốn sách không đòi hỏi ở người đọc một kiến thức chuẩn bị nào về lý thuyết số. Vì thế cũng có thể gọi nó là "Nhập môn thuật toán vào số học". Điều đó có nghĩa là, trong nhiều con đường khác nhau để đi vào số học, ta chọn con đường thuật toán: các định lí, khái niệm của số học được trình bày cùng với các thuật toán xây dựng chúng. Trong nhiều trường hợp, các thuật toán có kèm theo đánh giá sơ bộ về độ phức tạp.

Cuốn sách nhằm một số đối tượng khá rộng rãi: những sinh viên, nghiên cứu sinh về số học và tin học, những người quan tâm đến lí thuyết và ứng dụng của số học hiện đại. Nhiều phần của cuốn sách có thể có ích cho học sinh các lớp chuyên toán và chuyên tin học.

Chương đầu tiên của cuốn sách được dành để giới thiệu vài định nghĩa cơ bản nhất của lí thuyết thuật toán. Ba chương tiếp theo trình bày những vấn đề cơ sở của số học. Chương 5, ngoài việc chuẩn bị kiến thức cho những phần tiếp theo, có bình luận ít nhiều về vai trò của sự tương tự giữa số và đa thức trong sự phát triển của số học hiện đại.

Để người đọc có thể hình dung phần nào các ứng dụng của số học thuật toán, cuốn sách dành chương 6 để nói về lí thuyết mật mã. Một vài ứng dụng gần đây của lí thuyết đường cong elliptic vào mật mã được trình bày trong chương 7. Cũng có thể xem Chương 7 là một nhập môn ngắn và sơ cấp vào lí thuyết đường cong elliptic, một trong những lí thuyết phong phú nhất của Hình học đại số số học.

Cuối mỗi chương đều có một số bài tập dành cho độc giả muốn đọc cuốn sách "một cách tích cực". Một số bài tập mang tính chất luyện tập và tính toán thực hành, một số khác là mở rộng lí thuyết. Trừ chương cuối về đường cong elliptic, các chương còn lại đều có kèm theo hướng dẫn thực hành tính toán bằng chương trình MAPLE. Phần hướng dẫn thực hành này do Tạ Thị Hoài An biên soạn. Cuối cuốn sách có phần tự kiểm tra kiến thức dành cho những độc giả học giáo trình này với sự trợ giúp của máy tính.

Do nhiều nguyên nhân khác nhau, cuốn sách chắc chắn còn rất nhiều thiếu sót. Tác giả hy vọng nhận được những lời phê bình của bạn đọc.

Hà nội, 1998
Hà Huy Khoái