ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THỊ MỴ

KHẢO SÁT CÁC THUẬT TOÁN KIỂM ĐỊNH SỐ NGUYÊN TỐ LỚN VÀ ỨNG DỤNG.

Chuyên ngành: KHOA HỌC MÁY TÍNH
Mã số : 60.48.01.01

LUẬN VĂN THẠC SĨ

HƯỚNG DẪN KHOA HỌC: PGS TSKH NGUYỄN XUÂN HUY

THÁI NGUYÊN – 2017

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi, số liệu và kết quả nghiên cứu trong luận văn này là trung thực và không trùng lặp với các đề tài khác. Tôi cũng xin cam đoan rằng mọi sự giúp đỡ cho việc thực hiện luận văn này đã được cảm ơn và các thông tin trích dẫn trong luận văn đã được chỉ rõ nguồn gốc.

Tác giả

Nguyễn Thị Mỵ

\

LỜI CẢM ƠN

Tôi xin bày tỏ sự kính trọng và lòng biết ơn sâu sắc đến **PGS.TSKH. Nguyễn Xuân Huy** - người đã tận tình hướng dẫn và giúp đỡ tôi trong suốt quá trình học tập, nghiên cứu và hoàn thành luận văn, xin cảm ơn các thầy, cô giáo trong và ngoài trường đã cung cấp kiến thức và tạo điều kiện thuận lợi cho quá trình học tập và rèn luyện của bản thân tôi.

Tôi cũng xin được bày tỏ lòng biết ơn chân thành đến Ban Giám Hiệu, các thầy giáo, cô giáo phòng Sau đại học trường Đại học Công Nghệ Thông Tin &TruyềnThông, các thầy giáo ở Viện Công Nghệ Thông Tin đã giảng dạy và tạo mọi điều kiện cho tôi học tập, nghiên cứu và hoàn thành luận văn này.

Xin cảm ơn gia đình, bạn bè đã hết lòng giúp đỡ, khích lệ, động viên tôi để tôi hoàn thành luận văn.

Thái Nguyên, tháng 03 năm 2017

Tác giả

Nguyễn Thị Mỵ

DANH MỤC CÁC KÝ HIỆU TRONG LUẬN VĂN

Kí hiệu	Ý nghĩa
$\mathbb{R}$	Tập số thực
$\mathbb{R}^+$	Tập số thực không âm
$\mathbb{N}$	Tập số tự nhiên (kể cả 0)
$\mathbb{Z}$	Tập số nguyên
$\mathbb{Z}^+$	Tập số nguyên không âm, $\mathbb{Z}^+ = \mathbb{N}$
(a, b), gcd (a,b)	Ước chung lớn nhất của a và b
$\mathrm{Ord}_n(b)$	Bậc của b theo modulo n
$\mathbb{Z}/n$	Vành nguyên theo modulo n. Nếu n nguyên theo thì $\mathbb{Z}/n$ là trường
$\mathbb{Z}[x]$	Vành các đa thức nguyên
$\equiv$	Toàn đẳng, tương đương, đồng dư
$\phi(n)$	Hàm phi Euler
L, BitLen(n)	Số bit biểu diễn nhị phân n
log$n$	logarit cơ số 2 của n
lgamma(n)	log((n−1)!)
$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$	Tổ hợp chập k của n

DANH MỤC CÁC BẢNG TRONG LUẬN VĂN

Bảng	Tên các bảng trong luận văn	Trang
1.1	Phân bố số nguyên tố	10
1.2	Một vài số nguyên tố Mersenne	16
1.3	Một số cặp nguyên tố sinh đôi	17
1.4	Một số số nguyên tố Sophie Germain	17
1.5	Vài số giai thừa nguyên tố	18
1.6	20 số nguyên tố đầu tiên và các hàm n#, p_n#	19
1.7	Một số số nguyên tố giai thủy đã biết	20
1.8	Thời gian máy tính dùng để phân tíchsố n ra thừa số nguyên tố	24
2.1	Các số nguyên tố và hợp số trong khoảng 2−100-1 là số đặc biệt	31
2.2	Các phép + và · trong vành ℤ/7	49
3.1	Các phương thức của lớp BI	52
3.2	Bậc của các số trong ℤ/7	61
3.3	Hai phần tử sinh của ℤ/7	62

MỤC LỤC

LỜI CẢM ƠN II
DANH MỤC CÁC KÝ HIỆU TRONG LUẬN VĂN III
DANH MỤC CÁC BẢNG TRONG LUẬN VĂN IV
MỞ ĐẦU 1
CHƯƠNG1. TỔNG QUAN VỀ SỐ NGUYÊN TỐ 4
1.1 Các định nghĩa và khái niệm mở đầu 4
1.2 Một số tính chất của số nguyên tố 7
1.3 Sự phân bổ của số nguyên tố 9
1.4 Số giả nguyên tố 11
1.5 Số Mersenne 13
1.6 Số Fermat 16
1.7 Các số nguyên tố lớn 17
1.7.1 Các số nguyên tố sinh đôi 17
1.7.2 Các số nguyên tố Sophie Germain 17
1.7.3 Các số giai thừa nguyên tố 18
1.7.4 Các số nguyên tố giai thủy 19
1.8 Ứng dụng của số nguyên tố 21
1.8.1 Mật mã và số nguyên tố 21
1.8.2 Các hệ mật mã công khai 21
CHƯƠNG 2. CÁC THUẬT TOÁN KIỂM ĐỊNH SỐ NGUYÊN TỐ 26
2.1 Các lớp P và NP 26
2.2 Thuật toán kiểm định theo $\sqrt{n}$ 28
2.3 Sàng Eratosthenes 30
2.4 Thuật toán kiểm định theo xác suất MILLER-RABIN 31
2.4.1 Cơ sở toán học 31
2.4.2 Thuật toán Miller Test 36

2.4.3 Thuật toán Miller-Rabin 36
2.4.4 Các trường hợp đặc biệt 37
2.5 Kiểm định theo giả thuyết Riemann 38
2.6 Thuật toán kiểm định tính nguyên tố AKS 39
2.6.1 Giới thiệu chung 39
2.6.2 Định lí AKS 40
2.6.3 Thuật toán 41
2.6.4. Một số kiến thức toán học 42
2.7 Thuật toán Bernstein 46
2.7.1 Định lí Bernstein 46
2.7.2 Thuật toán Bernstein 47
CHƯƠNG 3. CÀI ĐẶT VÀ ỨNG DỤNG 48
3.1 Lớp BI 49
3.1.1 Nhận xét chung 49
3.1.2 Các trường dữ liệu 49
3.1.3 Các phương thức 49
3.2 Lớp ARITHM 55
3.2.1 Ước chung lớn nhất 55
3.2.2 Hàm phi Euler 55
3.2.3 Số chính căn 56
3.2.4 Bậc theo modulo 58
3.2.5 Căn nguyên thủy 59
3.2.6 Số nguyên tố sát sau 61
3.2.7 Kiểm tra ước nguyên tố 62
3.2.8 Ước nguyên tố lớn nhất 64
3.2.9 Nhân modulo 66
3.2.10 Lũy thừa modulo 67

3.3 Lớp BIPOL 67
3.3.1 Các trường dữ liệu 67
3.3.2 Các phương thức 67
3.4 Lớp MR 72
3.5 Lớp AKS 72
3.6 Ứng dụng 72
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 73
TÀI LIỆU THAM KHẢO 79

MỞ ĐẦU

Số nguyên tố là số tự nhiên lớn hơn một và chỉ chia hết cho một và chính nó.

Định nghĩa về số nguyên tố mặc dù đơn giản và ngắn gọn nhưng những vấn đề xoay quanh nó luôn làm các nhà toán học quan tâm.

Số nguyên tố là một trong những khái niệm xưa nhất của toán học. Các số nguyên tố là vật liệu cơ bản xây dựng nên các số tự nhiên. Vì các số nguyên tố tăng lên vô hạn nên câu hỏi đầu tiên đặt ra là: *Có bao nhiêu số nguyên tố*? Có thể liệt kê tất cả chúng ra hay chúng lập thành một dãy số vô hạn. Để chứng minh điều này Euclid đã đưa ra một lập luận, xuất phát từ giả thiết phản chứng rằng dãy số nguyên tố là hữu hạn, sau đó chỉ ra một số nguyên tố mới khác với số nguyên tố đã có. Mâu thuẫn này cho biết tập các số nguyên tố là *vô hạn*.

Sau khi Euclid chứng minh có vô số các số nguyên tố, nhiều câu hỏi xung quanh các số nguyên tố được đưa ra. Một số những câu hỏi đó, dưới những phát biểu đơn giản, đã trở thành những bài toán trong lịch sử toán học mà cho đến nay vẫn chưa có được lời giải trọn vẹn.

Người ta không tìm thấy một sự tuần hoàn nào trong dãy số nguyên tố. Sự phân bố của các số nguyên tố tỏ ra phức tạp và không có quy luật. Việc phát hiện các số nguyên tố lớn trong một thời gian dài là sự quan tâm của nhiều nhà toán học. Tuy nhiên cho đến nay trong số học vẫn còn tồn tại nhiều giả thuyết mở về số nguyên tố. Hơn nữa, trong thời đại công nghệ thông tin ngày nay việc nghiên cứu số nguyên tố đang được kích thích bởi sự kiện là các số nguyên tố tỏ ra rất có ích trong việc mã hóa và giải mã thông tin. Tính bảo mật và an toàn của quá trình trao đổi khóa và các hệ mật mã khóa công khai được đảm bảo bằng độ phức tạp của bài toán số học phân tích một số nguyên thành tích các thừa số nguyên tố. Nói cách khác, vấn đề thời gian tiêu tốn cho việc chạy máy tính để thực hiện bài toán phân tích một số nguyên đủ

lớn thành các thừa số nguyên tố được sử dụng làm chỉ tiêu đánh giá độ an toàn của hầu hết các hệ mật mã khóa công khai nói chung và hệ mật mã RSA nói riêng. Đó cũng là lí do để các hệ mật mã nói chung và hệ mật mã khóa công khai RSA được cộng đồng quốc tế chấp nhận rộng rãi trong thương mại điện tử và trao đổi thông tin.

Trong khuôn khổ của mình, luận văn sẽ trình bày các thuật toán liên quan đến số nguyên tố và ứng dụng của thuật toán trên để từ đó cài đặt chương trình thử nghiệm nhằm nhấn mạnh vai trò của số nguyên tố trong việc mã hóa và giải mã thông tin.

Đối tượng và phạm vi nghiên cứu

Luận văn tập trung tìm hiểu về số nguyên tố và các đối tượng có quan hệ mật thiết đến số nguyên tố, bao gồm các thuật toán kiểm định số nguyên tố, hệ mật mã khóa công khai. Ngoài ra luận văn quan tâm đến một số lớp số nguyên tố đặc biệt thường được khuyến cáo tránh sử dụng khi xây dựng các hệ mật mã vì thuật toán kiểm định những số nguyên tố này thường có độ phức tạp không cao.

Những nội dung nghiên cứu chính

Nội dung của luận văn chủ yếu tập trung vào nghiên cứu các vấn đề chính sau đây:

Chương 1. Tổng quan về số nguyên tố và các khái niệm liên quan

Trong chương này học viên trình bày về tổng quan số nguyên tố: Giới thiệu chung về số nguyên tố, các định lý quan trọng và một vài lớp số nguyên tố quan trọng trong lịch sử toán học.

Chương 2. Giới thiệu một số thuật toán kiểm định số nguyên tố

Trong chương này, luận văn tập trung trình bày các thuật toán kiểm định số nguyên tố lớn dựa trên các tiếp cận khác nhau: phương pháp tất định và phương pháp xác suất.