ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

NGUYỄN THÙY DUNG

CÁC THUẬT TOÁN CƠ BẢN TRONG LÝ THUYẾT SỐ

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - Năm 2014

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

NGUYỄN THÙY DUNG

CÁC THUẬT TOÁN CƠ BẢN TRONG LÝ THUYẾT SỐ

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số : 60.46.01.13

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS. TS. TẠ DUY PHƯỢNG

Thái Nguyên - Năm 2014

Mục lục

LỜI CẢM ƠN

Với lòng kính trọng và biết ơn sâu sắc em xin chân thành cảm ơn thày PGS. TS. Tạ Duy Phượng đã hướng dẫn và chỉ bảo tận tình cho em trong suốt quá trình làm luận văn. Thầy không chỉ truyền thụ những tri thức khoa học mà còn chỉ dẫn cho em những phương pháp làm việc tốt cùng những lời động viên khuyến khích kịp thời.

Em cũng xin gửi lời cảm ơn chân thành đến Ban giám hiệu, phòng Đào tạo, khoa Toán - Tin Trường ĐHKH, Đại học Thái Nguyên đã tạo điều kiện thuận lợi trong suốt quá trình học tập tại trường.

Xin chân thành cảm ơn gia đình, bạn bè đồng nghiệp và các thành viên trong lớp cao học toán K6B đã luôn quan tâm, động viên, giúp đỡ em trong suốt thời gian học tập và quá trình làm luận văn.

Thái Nguyên, 2014.

Nguyễn Thùy Dung

Mở đầu

Cùng với sự phát triển của máy tính điện tử, tin học ngày càng xâm nhập sâu hơn vào chương trình giảng dạy toán, thậm chí ở cấp phổ thông. Một số thuật toán trong lý thuyết số đã được biết đến từ thời Euclid. Tuy nhiên, thực thi chúng với các số lớn không dễ dàng nếu không có máy tính điện tử. Cùng với sự phát triển của toán và tin học, nhiều thuật toán mới ra đời, đáp ứng những đòi hỏi mới của thực tế (mật mã hóa công khai, phân tích các số nguyên tố lớn,...). Vì vậy, ngành số học thuật toán đã ra đời. Việc tổng hợp, nghiên cứu và xây dựng các chương trình tính toán trong số học là một công việc thú vị và hữu ích. Để đáp ứng nhu cầu học tập và giảng dạy, tác giả đã chọn đề tài " Các thuật toán cơ bản trong lý thuyết số".

Luận văn bao gồm phần mở đầu, hai chương, kết luận và danh mục các tài liệu tham khảo.

Chương 1 *Các thuật toán cơ bản trong lý thuyết số*

Trình bày các thuật toán cơ bản trong Lý thuyết số (tìm ước số chung lớn nhất, bội số chung nhỏ nhất, tìm số dư và thương khi chia một số nguyên cho một số nguyên khác, thuật toán Euclid phân tích một số ra thừa số nguyên tố, thuật toán Lucas- Lehmer tìm số nguyên tố, thuật toán Miller tìm số giả nguyên tố).

Chương 2 *Lập trình và thực thi trên máy tính điện tử một số thuật toán số học*

Trình bày các chương trình có sẵn hoặc tự lập trình cho các thuật toán đã nêu trong chương 1. Thực thi trên máy tính điện tử khoa học (Vinacal 570ES Plus II), chương trình Pascal và chương trình tính toán trên Maple.

Chương 1

Các thuật toán cơ bản trong lý thuyết số

Chương này trình bày một số thuật toán cơ bản liên quan đến ước chung lớn nhất, bội chung nhỏ nhất, tìm số nguyên tố, phân tích một số ra thừa số nguyên tố... Các vấn đề trình bày trong chương này được tham khảo và trích dẫn chủ yếu từ một số tài liệu [4], [5], [6].

1.1 Tìm thương và số dư

Cơ sở lý thuyết của phép chia với dư là *định lý về phép chia có dư*. Định lý này được ứng dụng trong giải thuật Euclid tìm ước chung lớn nhất của hai số nguyên khác 0.

Định lý về phép chia với dư: Với hai số tự nhiên a và b bất kì $(a > b)$, bao giờ cũng tìm được duy nhất các số q và r sao cho $a = qb + r$, trong đó $0 \leq r < b$.

Khi $r = 0$ ta nói a *chia hết cho* b hay b *chia hết* a. Ta cũng nói a là *bội số* của b hay b là *ước số* của a.

Các số nguyên trong định lý được gọi như sau:

q được gọi là *thương* khi chia a cho b.

r được gọi là *số dư* khi chia a cho b.

b được gọi là *số chia*.

a được gọi là *số bị chia*.

Phép toán tìm q và r được gọi là *phép chia với dư*.

Chứng minh

Trước tiên ta nhớ lại

Tiên đề Archimede *Với mọi số thực $x > 0$ và mọi số thực y thì tồn tại một số tự nhiên n sao cho $nx > y$.*

Hệ quả *Với mọi số thực $x < 0$ và mọi số thực y thì tồn tại một số tự nhiên n sao cho $nx < y$.*

Nguyên lý sắp thứ tự tốt *Mọi tập con khác rỗng các số tự nhiên đều có phần tử bé nhất.*

Chứng minh định lý gồm hai phần: đầu tiên chứng minh sự tồn tại của q và r, thứ hai, chứng minh tính duy nhất của q và r.

Sự tồn tại

Xét tập hợp $S = \{a - nb, n \in \mathbb{Z}\}$.

Ta khẳng định rằng S chứa ít nhất một số nguyên không âm. Có hai trường hợp như sau.

Nếu $b < 0$, thì $-b > 0$, và theo tính chất Archimede, có một số nguyên n sao cho $-bn \geq -a$, nghĩa là $a - bn \geq 0$.

Nếu $b > 0$, thì cũng theo tính chất Archimede, có một số nguyên n sao cho $bn \geq -a$, nghĩa là $a - b(-n) = a + bn \geq 0$.

Như vậy S chứa ít nhất một số nguyên không âm. Theo nguyên lý sắp thứ tự tốt, trong S có một số nguyên không âm nhỏ nhất, ta gọi số ấy là r. Đặt $q = \dfrac{a-r}{b}$, thì q và r là các số nguyên và $a = qb + r$. Ta còn phải

chỉ ra rằng $0 \leq r < |b|$. Tính không âm của r là rõ ràng theo cách chọn r. Ta sẽ chứng tỏ dấu bất đẳng thức thứ hai.

Giả sử ngược lại $r \geq |b|$. Vì $b \neq 0, r > 0$ nên $b > 0$ hoặc $b < 0$.

Nếu $b > 0$, thì $r \geq b$ suy ra $a - qb \geq b$. Từ đó $a - qb - b \geq 0$, lại dẫn tới $a - (q+1)\, b \geq 0$.

Đặt $r^{'} = a - (q+1)\, b$ thì $r^{'} \in S$ và $r^{'} = a - (q+1)\, b = r - b < r$, điều này mâu thuẫn với tính chất r là phần tử không âm nhỏ nhất của S.

Nếu $b < 0$ thì $r \geq -b$ do đó $a - qb \geq -b$. Từ đó suy ra rằng $a - qb + b \geq 0$, tiếp tục suy ra $r^{'} = a - (q-1)\, b \geq 0$. Do đó, $r^{'} \in S$ và vì $r^{'} = r + b$ với $b < 0$ ta có $r^{'} = a - (q-1)\, b < r$, mâu thuẫn với giả thiết r là số nguyên không âm nhỏ nhất trong S. Như vậy ta đã chứng minh sự tồn tại của q và r.

Tính duy nhất

Giả sử rằng tồn tại q, $q^{'}$, r, $r^{'}$ với $0 \leq r, r^{'} < |b|$ sao cho $a = q + r$ và $a = q^{'} + r^{'}$. Không mất tính tổng quát giả sử $q \leq r^{'}$.

Từ hai đẳng thức trên ta có $b\left(q^{'} - q\right) = r - r^{'}$.

Nếu $b > 0$ thì $r^{'} \leq r$ và $r < b \leq b + r^{'}$, và như vậy $r - r^{'} < b$. Còn nếu $b < 0$ thì $r \leq r^{'}$ và $r^{'} < -b \leq -b + r$, và do đó $-\left(r - r^{'}\right) < -b$. Trong cả hai trường hợp ta có $\left|r - r^{'}\right| < |b|$.

Mặt khác đẳng thức $b\left(q^{'} - q\right) = \left(r - r^{'}\right)$ chứng tỏ rằng $|b|$ chia hết $\left|r - r^{'}\right|$, do đó $|b| \leq \left|r - r^{'}\right|$ hoặc $\left|r - r^{'}\right| = 0$. Nhưng vì $\left|r - r^{'}\right| \leq |b|$, nên chỉ có thể $r = r^{'}$. Thay vào đẳng thức $b\left(q^{'} - q\right) = \left(r - r^{'}\right)$ ta có $bq = bq^{'}$ và vì b khác 0, nên $q = q^{'}$. Tính duy nhất đã được chứng minh.

Thuật toán chia Để chia một số tự nhiên a cho một số tự nhiên d $(a > d)$, ta thực hiện theo ví dụ sau:

Ví dụ 1.1 Chia $a = 1542014$ cho $d = 135$.

Giải Phân tích số $a = 1542014$ theo cơ số 10 ta được: