TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN MÔN CẤU TRÚC RỜI RẠC**

**…tên đề tài…**

*Người hướng dẫn*: **TRẦN LƯƠNG QUỐC ĐẠI**

*Người thực hiện*: **LỮ PHÚC PHÚ – 52100988**

Lớp **: 21040501**

Khoá  **: 25**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN MÔN CẤU TRÚC RỜI RẠC**

**…tên đề tài…**

Người hướng dẫn: **TRẦN LƯƠNG QUỐC ĐẠI**

Người thực hiện: **LỮ PHÚC PHÚ**

Lớp **: 21040501**

Khoá  **: 25**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

LỜI CẢM ƠN

Bài đồ án cuối kì của tôi có thể hoàn thành nhờ vào giảng viên bộ môn. Tôi xin cảm ơn thầy Trần Lương Quốc Đại, người đã hướng dẫn tôi viết đề tài này, nhờ thầy mà đồ án của tôi có thể hoàn thiện nhất. Nếu báo cáo của tôi có gì thiếu sót, xin thầy cô có thể góp ý thêm để đbài báo cáo của tôi thêm hoàn thiện.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi và được sự hướng dẫn của thầy Lương Quốc Đại. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày 13 tháng 04 năm 2023*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Lữ Phúc Phú*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

T

Bài báo cáo của tôi gồm hai chương. Chương 1 tìm hiểu về nghịch đảo Modulo và xây dựng thuật toán bằng python. Chương 2 tìm hiểu về hệ thống mã hóa RSA đồng thời hiện thực nó bằng python.

Bài báo cáo của tôi nếu có gì thiếu sót xin thầy cô góp ý thêm để hoàn hiện hơn.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc132223897)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc132223898)

[TÓM TẮT iv](#_Toc132223899)

[MỤC LỤC 1](#_Toc132223900)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 3](#_Toc132223901)

[CHƯƠNG 1 – BÀI TOÁN MODULO 4](#_Toc132223902)

[1.1 Tìm hiểu về bài toán 4](#_Toc132223903)

[1.2 Hiện thực bài toán 5](#_Toc132223904)

[CHƯƠNG 2 – TỔNG QUAN 6](#_Toc132223905)

[1.1 Trình bày công thức toán học 6](#_Toc132223906)

[1.2 Trình bày một hình vẽ, sơ đồ 6](#_Toc132223907)

[CHƯƠNG 3 – CƠ SỞ LÝ THUYẾT / NGHIÊN CỨU THỰC NGHIỆM 8](#_Toc132223908)

[3.1 Chèn bảng: 8](#_Toc132223909)

[3.2 Viết tắt 8](#_Toc132223910)

[3.3 Trích dẫn 8](#_Toc132223911)

[3.3.1 Tài liệu tham khảo và cách trích dẫn 8](#_Toc132223912)

[3.3.2 Qui định của Khoa Công nghệ thông tin 9](#_Toc132223913)

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC KÝ HIỆU**

*f Tần số của dòng điện và điện áp (Hz)*

*p Mật độ điện tích khối (C/m3)*

**CÁC CHỮ VIẾT TẮT**

CSTD Công suất tác dụng

MF Máy phát điện

BER Tỷ lệ bít lỗi

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

[Hình 2.1: Kiến trúc FTP 1](#_Toc387689394)

**DANH MỤC BẢNG**

[Bảng 3.1 Ví dụ cho chèn bảng 1](#_Toc387689363)

CHƯƠNG 1 – BÀI TOÁN MODULO

Đồng dư modulo là một công cụ trong số học. Nó được được xây dựng bởi nhà toán học thiên tài Gauss và là hệ thống số học dành cho số nguyên. Trong số học mô đun, các con số được viết bao quanh lấy nhau thành nhiều vòng tròn đến khi chạm tới đích, được gọi là mô đun (Modulus). Trong chương này chúng ta sẽ cùng tìm hiểu sơ qua về bài toán đồng dư Modulo này.

1.1 Tìm hiểu về bài toán

Bài toán đồng dư Modulo được phát biểu như sau: Với một số nguyên n > 1, gọi là mô đun, hai số nguyên a và b được gọi là đồng dư modulo n, nếu hiệu của chúng chia hết cho n (đó là, nếu tồn tại một số nguyên k sao cho a – b = kn).

Đồng dư mô đun n là một quan hệ đồng dư, tức là một quan hệ tương tương thích với các phép cộng, trừ và nhân. Đồng dư mô đun n được ký hiệu là:

(1.1)

Dấu ngoặc nghĩa lag (mod n) áp dụng cho toàn bộ phương trình, không chỉ mỗi vế phải (b). Ký hiệu này mang ý nghĩa khác với b mod n (không chứa dấu ngoặc), dùng để chỉ phép toán modulo. Cụ thể hơn, b mod n ký hiệu số dư khi chia n cho b, tức số nguyên a thỏa mãn và

Ví dụ:

Trong mô đun 12, ta có thể viết:

Vì 38 – 14 = 24, một bội của 12. Một cách khác thể hiện điều này là cả 38 và 14 có cùng số dư là 2 khi chia cho 12.

Định nghĩa đồng dư cũng áp dựng cho số nguyên âm, ví dụ như sau:

Quan hệ đồng dư thỏa mãn các tính chất của một quan hệ tương đương:

- Phản xạ:

- Đối xứng: khi và chỉ khi với mọi a, b

- Bắc cầu: nếu và thì

1.2 Hiện thực bài toán

Trong phần này tôi sẽ xây dựng bài toán trên bằng giải thuật thay thế Euclidean với ngôn ngữ Python, đồng thời giải thích về ý tưởng mà tôi xây dựng.

Bài toán này tôi xây dựng trên file 52100988\_1.py trong đây tôi tạo ra hai hàm bao gồm extended\_euclidean(a, b) và inverse\_modulo(a, b)

Với hàm extended\_euclidean(a, b) tôi đã tạo một hàm đệ quy và viết như sau:

Ảnh có chứa văn bản

Mô tả được tạo tự động

Hình 1.1: Kiến trúc FTP

Nguồn: (Postel & Reynolds 1985)

CHƯƠNG 2 – TỔNG QUAN

*Tổng quan*: phân tích, đánh giá các công trình nghiên cứu đã có của tác giả, các tác giả khác trong và ngoài nước liên quan mật thiết đến đề tài; nêu những vấn đề còn tồn tại; chỉ ra những vấn đề mà đề tài cần tập trung nghiên cứu, giải quyết;

1.1 Trình bày công thức toán học

Công thức toán học cần nhất quán trong toàn bộ luận văn. Sử dụng công cụ của MS Word và đánh số theo chương, số thứ tự trong chương. Ví dụ công thức sau đây đánh là 2.1.

(2.1)

Trong công thức, nếu có các kí hiệu là lần đầu tiên sử dụng, cần phải giải thích rõ kí hiệu đó đại diện cho phần tử nào và đơn vị là gì.

(2.2)

Trong công thức 2.2:

* a: độ dài cạnh góc vuông của tam giác, đơn vị mét (*m*).
* b: độ dài cạnh góc vuông còn lại của tam giác, đơn vị mét (*m*).
* c: độ dài cạnh huyền của tam giác, đơn vị mét (*m*).

1.2 Trình bày một hình vẽ, sơ đồ

Việc đánh số bảng biểu, hình vẽ, phương trình phải gắn với số chương (Thí dụ hình 3.4 có nghĩa là hình thứ 4 trong Chương 3). Mọi bảng biểu, đồ thị lấy từ các nguồn khác phải được trích dẫn đầy đủ (ví dụ: *Nguồn:* *Tr.35, Tạp chí Tín dụng (2012), Số 15, NXB Tài chính, TP.HCM*). Nguồn được trích dẫn phải được liệt kê chính xác trong Danh mục tài liệu tham khảo. Đầu đề của bảng, biểu ghi phía trên bảng, biểu; đầu đề của hình vẽ ghi phía dưới hình. Thông thường những bảng ngắn và đồ thị nhỏ phải đi liền với phần nội dung đề cập tới các bảng và đồ thị này ở *lần thứ nhất*. Các bảng dài có thể để ở những trang riêng nhưng cũng phải tiếp ngay theo phần nội dung đề cập tới bảng này ở lần đầu tiên.



Hình 2.: Kiến trúc FTP

Nguồn: (Postel & Reynolds 1985)

CHƯƠNG 3 – CƠ SỞ LÝ THUYẾT / NGHIÊN CỨU THỰC NGHIỆM

*Những nghiên cứu thực nghiệm hoặc lý thuyết*: trình bày các cơ sở lý thuyết, lý luận, giả thuyết khoa học và phương pháp nghiên cứu sẽ được sử dụng trong Luận văn, Luận án;

3.1 Chèn bảng:

|  |  |  |
| --- | --- | --- |
| **STT** | **Tiêu đề A** | **Tiêu đề B** |
| 1 | Nội dung 1 | Nội dung 4 |
| 2 | Nội dung 2 | Nội dung 5 |
| 3 | Nội dung 3 | Nội dung 6 |

Bảng 3.Ví dụ cho chèn bảng

Khi cần chèn tên bảng thì chọn References \ Caption và chọn “Bảng …”

3.2 Viết tắt

Không lạm dụng việc viết tắt. Chỉ viết tắt những từ, cụm từ hoặc thuật ngữ *được sử dụng nhiều lần trong luận văn*. Không viết tắt những cụm từ dài, những mệnh đề hoặc những cụm từ ít xuất hiện. Nếu cần viết tắt những từ, thuật ngữ, tên các cơ quan, tổ chức... thì được viết tắt sau lần viết thứ nhất có kèm theo chữ viết tắt trong ngoặc đơn. Nếu có quá nhiều chữ viết tắt thì phải có bảng danh mục các chữ viết tắt (xếp theo thứ tự A, B, C) ở phần đầu luận văn.

3.3 Trích dẫn

3.3.1 Tài liệu tham khảo và cách trích dẫn

Mọi ý kiến, khái niệm, phân tích, phát biểu, diễn đạt... có ý nghĩa, mang tính chất gợi ý *không phải của riêng tác giả* và mọi tham khảo khác **phải được trích dẫn và chỉ rõ nguồn trong danh mục Tài liệu tham khảo của luận văn**. Phải nêu rõ cả việc sử dụng những đề xuất hoặc kết quả của đồng tác giả (*đối với công trình đã công bố khác thì phải trích dẫn bình thường như một tài liệu tham khảo*). Nếu sử dụng tài liệu của người khác và của đồng tác giả (bảng biểu, hình vẽ, công thức, đồ thị, phương trình, ý tưởng...) mà không chú dẫn tác giả và nguồn tài liệu thì **luận văn không được duyệt để bảo vệ**.

Không trích dẫn những kiến thức phổ biến, mọi người đều biết tránh làm nặng nề phần tham khảo trích dẫn.

Nếu người dẫn liệu không có điều kiện tiếp cận được một tài liệu gốc mà phải trích dẫn thông qua một tài liệu khác của một tác giả khác, thì phải nêu rõ cách trích dẫn (*lưu ý phải ghi* *đúng nguyên văn từ chính tài liệu tham khảo và hạn chế tối đa hình thức này).* Nếu cần trích dẫn dài hơn thì phải tách phần này thành một đoạn riêng khỏi phần nội dung đang trình bày, in nghiêng, với lề trái lùi vào thêm 2 cm. Khi mở đầu và kết thúc đoạn trích này không phải sử dụng dấu ngoặc kép. Việc trích dẫn là theo thứ tự của tài liệu ở danh mục Tài liệu tham khảo và được đặt trong ngoặc vuông, khi cần có cả số trang, ví dụ [15, tr.314-315]. Đối với phần trích dẫn từ nhiều tài liệu khác nhau, số của từng tài liệu được đặt độc lập trong từng ngoặc vuông, theo thứ tự tăng dần, ví dụ [19], [25], [41], [42].

3.3.2 Qui định của Khoa Công nghệ thông tin

**- Đạo văn** là việc sử dụng từ ngữ hay ý tưởng của người khác như là của mình trong hoạt động học thuật nói riêng và trong hoạt động sáng tạo nói chung. Tại Đại học Hoa Sen, những hành vi sau đây được xem là đạo văn:

* Sao chép nguyên văn **02** (hai) câu liên tiếp mà không dẫn nguồn đúng quy định;
* Sao chép nguyên văn **03** (ba) câu không liên tiếp mà không dẫn nguồn đúng quy định;
* Diễn đạt lại (rephrase) hoặc dịch (translate) toàn bộ một ý nào đó của người khác mà không dẫn nguồn đúng quy định;
* Sử dụng hơn 30% nội dung của một báo cáo cuối kỳ do chính mình viết để nộp cho 2 lớp khác nhau (cùng học kỳ hoặc khác học kỳ) mà không có sự đồng ý của giảng viên;
* Sao chép một phần hoặc toàn bộ bài làm của người khác.

- Khi luận văn, đồ án, bài tập lớn, được chấm điểm, nếu bị phát hiện đạo văn thì ngay lập tức bị điểm 0. Sinh viên sẽ tiếp tục bị xử lý kỷ luật theo các qui định của Nhà trường.

**TÀI LIỆU THAM KHẢO**

**Tiếng Việt**

1. Quách Ngọc Ân (1992), “Nhìn lại hai năm phát triển lúa lai”, *Di tuyền học ứng dụng*, 98(1), tr. 10-16.
2. Bộ nông nghiệp & PTNT (1996), *Báo cáo tổng kết 5 năm (1992-1996) phát triển lúa lai,* Hà Nội.
3. Nguyễn Hữu Đống, Đào Thanh Bằng, Lâm Quang Dụ, Phan Đức Trực (1997), *Đột biến –* *Cơ sở lý luận và ứng dụng,* Nhà xuất bản nông nghiệp, Viện khoa học kỹ thuật nông nghiệp Việt Nam, Hà Nội.
4. Nguyễn Thị Gấm (1996), *Phát hiện và đánh giá một số dòng bất dục đực cảm ứng nhiệt* *độ,* Luận văn thạc sĩ khoa học nông nghiệp, Viện khoa học kỹ thuật nông nghiệp Việt Nam, Hà Nội.

……….

1. Võ Thị Kim Huệ (2000), *Nghiên cứu chẩn đoán và điều trị bệnh…,* Luận án Tiến sĩ y khoa, Trường đại học y Hà Nội, Hà Nội.

**Tiếng Anh**

1. Anderson J.E. (1985), The Relative Inefficiency of Quota, The Cheese Case, *American* *Economic Review*, 75(1), pp. 178-90.
2. Borkakati R. P.,Virmani S. S. (1997), Genetics of thermosensitive genic male sterility in Rice, *Euphytica* 88, pp. 1-7.
3. Boulding K.E. (1955), *Economics Analysis*, Hamish Hamilton, London.
4. Burton G. W. (1988), “Cytoplasmic male-sterility in pearl millet (penni-setum glaucum L.)”, *Agronomic Journal* 50, pp. 230-231.
5. Central Statistical Oraganisation (1995), *Statistical Year Book*, Beijing.
6. FAO (1971), *Agricultural Commodity Projections (1970-1980)*, Vol. II. Rome.
7. Institute of Economics (1988), *Analysis of Expenditure Pattern of Urban Households in* *Vietnam,* Departement pf Economics, Economic Research Report, Hanoi.

**PHỤ LỤC**

Phần này bao gồm những nội dung cần thiết nhằm minh họa hoặc hỗ trợ cho nội dung luận văn như số liệu, biểu mẫu, tranh ảnh. . . . nếu sử dụng những câu trả lời cho một *bảng câu hỏi thì bảng câu hỏi mẫu này phải được đưa vào phần Phụ lục ở dạng nguyên bản* đã dùng để điều tra, thăm dò ý kiến; **không được tóm tắt hoặc sửa đổi**. Các tính toán mẫu trình bày tóm tắt trong các biểu mẫu cũng cần nêu trong Phụ lục của luận văn. Phụ lục không được dày hơn phần chính của luận văn