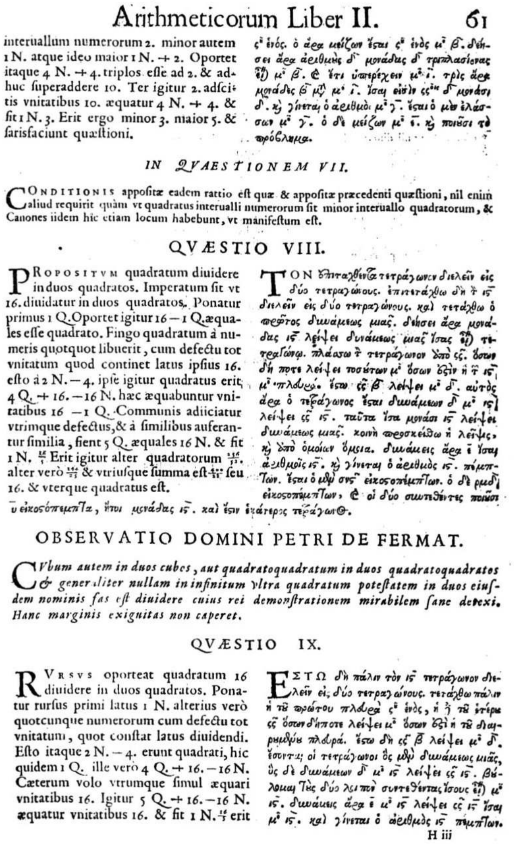
MATH 312: INTRODUCTION TO NUMBER THEORY

UBC, FALL TERM 2014, L. PESKIN



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos eſſe ad 2. & adhuc ſuperaddere 10. Ter igitur 2. adſcitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & ſarisfaciunt quæſtioni.

ςς̅ ἑνός. ὁ ἄρα μείζων ἔσται ςς̅ ἑνὸς μο β̅. δεήσει ἄρα ἀριθμοὺς δ̅ μονάδας δ̅ τριπλασίονας εἶναι μο β̅. καὶ ἔτι ὑπερέχειν μο ι̅. τρὶς ἄρα μονάδες β̅ μετὰ μο ι̅. ἴσαι εἰσὶν ςς̅ δ̅ μονάσι δ̅. καὶ γίνεται ὁ ἀριθμὸς μο γ̅. ἔσται ὁ μὲν ἐλάσσων μο γ̅. ὁ δὲ μείζων μο ε̅. καὶ ποιοῦσι τὸ πρόβλημα.

IN QVAESTIONEM VII.

CONDITIONIS appoſitæ eadem rattio eſt quæ & appoſitæ præcedenti quæſtioni, nil enim aliud requirit quàm vt quadratus interualli numerorum ſit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifeſtum eſt.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum ſit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales eſſe quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipſius 16. eſto à 2 N. − 4. ipſe igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à ſimilibus auferantur ſimilia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriuſque ſumma eſt $\frac{400}{25}$ ſeu 16. & vterque quadratus eſt.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ις̅ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις̅ λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸν τετράγωνον ἀπὸ ςς̅ ὅσων δή ποτε λείψει τοσούτων μο ὅσων ἐστὶν ἡ τῶν ις̅ μο πλευρά. ἔστω ςς̅ β̅ λείψει μο δ̅. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ̅ μο ις̅ λείψει ςς̅ ις̅. ταῦτα ἴσα μονάσι ις̅ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε̅ ἴσαι ἀριθμοῖς ις̅. καὶ γίνεται ὁ ἀριθμὸς ις̅ πέμπτων. ἔσται ὁ μὲν σνς̅ εἰκοστοπέμπτων. ὁ δὲ ρμδ̅ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ̅ εἰκοσόπεμπτα, ἤτοι μονάδας ις̅. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

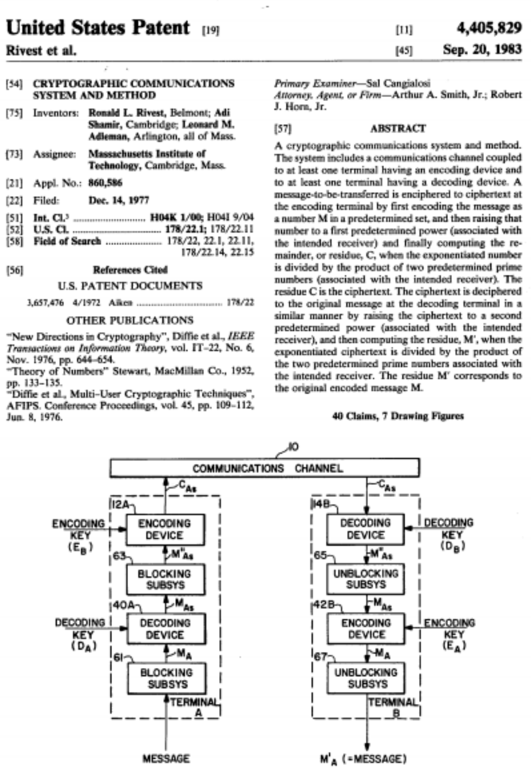
QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rurſus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot conſtat latus diuidendi. Eſto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque ſimul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

ΕΣΤΩ δὴ πάλιν τὸν ις̅ τετράγωνον διελεῖν εἰς δύο τετραγώνους. τετάχθω πάλιν ἡ τοῦ πρώτου πλευρὰ ςς̅ ἑνός, ἡ δὲ τοῦ ἑτέρου ςς̅ ὅσων δήποτε λείψει μο ὅσων ἐστὶν ἡ τοῦ διαιρουμένου πλευρά. ἔστω δὴ ςς̅ β̅ λείψει μο δ̅. ἔσονται οἱ τετράγωνοι ὃς μὲν δυνάμεως μιᾶς, ὃς δὲ δυνάμεων δ̅ μο ις̅ λείψει ςς̅ ις̅. βούλομαι τοὺς δύο λοιπὸν συντεθέντας ἴσους εἶναι μο ις̅. δυνάμεις ἄρα ε̅ μο ις̅ λείψει ςς̅ ις̅ ἴσαι μο ις̅. καὶ γίνεται ὁ ἀριθμὸς ις̅ πέμπτων.

H iii

Arithmetica, Diophantus (c. 200s AD), edition of 1670.
http://commons.wikimedia.org/wiki/File:Diophantus-II-8-Fermat.jpg



United States Patent [19]
Rivest et al.

[11] 4,405,829
[45] Sep. 20, 1983

[54] CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD

[75] Inventors: Ronald L. Rivest, Belmont; Adi Shamir, Cambridge; Leonard M. Adleman, Arlington, all of Mass.

[73] Assignee: Massachusetts Institute of Technology, Cambridge, Mass.

[21] Appl. No.: 860,586

[22] Filed: Dec. 14, 1977

[51] Int. Cl.[3] H04K 1/00; H04I 9/04
[52] U.S. Cl. 178/22.1; 178/22.11
[58] Field of Search 178/22, 22.1, 22.11, 178/22.14, 22.15

[56] References Cited

U.S. PATENT DOCUMENTS

3,657,476 4/1972 Aiken 178/22

OTHER PUBLICATIONS

"New Directions in Cryptography", Diffie et al., *IEEE Transactions on Information Theory*, vol. IT-22, No. 6, Nov. 1976, pp. 644-654.
"Theory of Numbers" Stewart, MacMillan Co., 1952, pp. 133-135.
"Diffie et al., Multi-User Cryptographic Techniques", AFIPS. Conference Proceedings, vol. 45, pp. 109-112, Jun. 8, 1976.

Primary Examiner—Sal Cangialosi
Attorney, Agent, or Firm—Arthur A. Smith, Jr.; Robert J. Horn, Jr.

[57] ABSTRACT

A cryptographic communications system and method. The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by first encoding the message as a number M in a predetermined set, and then raising that number to a first predetermined power (associated with the intended receiver) and finally computing the remainder, or residue, C, when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver). The residue C is the ciphertext. The ciphertext is deciphered to the original message at the decoding terminal in a similar manner by raising the ciphertext to a second predetermined power (associated with the intended receiver), and then computing the residue, M', when the exponentiated ciphertext is divided by the product of the two predetermined prime numbers associated with the intended receiver. The residue M' corresponds to the original encoded message M.

40 Claims, 7 Drawing Figures

RSA cryptosystem patent (US #4405829), 1983.
http://www.google.com/patents/US4405829

General Info

Lectures: MWF 11:00-12:00, 460 LSK
Office hours: MW 9:50-10:50 and by appointment, 300C LSK
Instructor: Laura Peskin
Instructor email: `lpeskin@math.ubc.ca`
Course webpage: `http://www.math.ubc.ca/~lpeskin/ma312.html`
Textbook: *Elementary Number Theory and Its Applications*, Kenneth H. Rosen, 6th edition.
Midterm exam dates: Thurs, Oct. 9 and Thurs, Nov. 6, both exams 6:30–7:30pm, 202 Macleod.

Course Description

This is a first course in number theory, aimed at students who have some (but not necessarily much) experience with reading and writing proofs. The course has three parts, each with its own set of goals:

(1) **Divisibility, modular arithmetic, and linear systems of congruences** (weeks 1-6). Topics include the Euclidean Algorithm, Fundamental Theorem of Arithmetic, Chinese Remainder Theorem, and Hensel's Lemma. The ideas will be quite concrete and we will be able to prove almost all statements from the ground up. We'll pay careful attention to proof structure during this part, and students will get plenty of practice at writing their own proofs.

(2) **Quadratic congruences, reciprocity, and primitive roots** (weeks 6-10). Deeper exploration of the multiplicative properties of modular arithmetic, including Fermat's Little Theorem, the quadratic reciprocity law, the Euler ϕ-function, and existence criteria for primitive roots. This part will be more abstract than the first, introducing theorems which are beautiful in their own right but which also form the seeds of modern algebraic number theory.

(3) **Applications of number theory** (weeks 10-13) After a brief introduction to the analysis of algorithms, we'll apply the ideas of the first two parts to primality testing, fast factorization, and public key cryptography.

A detailed list of topics appears at the end of this document. During the course, however, it's better to consult the course webpage (URL above) for the most up-to-date schedule and references.

Evaluation

Grading scheme: 20% weekly homeworks (12 assignments, lowest two scores dropped), 30% midterm exams (two exams, weighted equally), 50% final exam.

Homework info: Homework assignments are due at 11am on Wednesdays. Assignments will be posted on the course webpage (URL above) one week in advance. Homework problems will ask students to apply theorems from class to carry out calculations, and also to write their own proofs of related facts. Homework assignments are really the most important part of this course: allow yourself plenty of time to solve them carefully, and don't get behind! Late homework will not be accepted.

Homework collaboration policy: Every student must write up their own solutions without looking at any other student's written work. "Live" collaboration (i.e., discussing problems in person, without sharing written work) is allowed and encouraged. It's also fine to ask the instructor or TA for help, though you will benefit most from this if you've already spent some time thinking about the problem by yourself.

Homework grading: Not every assigned problem will be graded; typically two or three problems will be graded in detail, with a small number of points to be given for completing the rest of the assignment. Homework grading schemes will be posted together with solutions. The two lowest homework scores will be dropped.

Exams: All exams will be closed-book, closed-note. Sample exams will be posted in due time. Requests for make-up midterm exams will be considered only with at least three weeks' notice *and* with documented academic or medical justification. If you must miss a midterm exam on shorter notice for a documented medical reason, then you may request to have the weight of that exam transferred to the final exam.

Syllabus

This syllabus may change a bit as the course progresses. See the course webpage for the most up-to-date schedule and for more specific references. All section numbers refer to the course textbook.

(1) **Divisibility, modular arithmetic, and linear systems of congruences**
- The division algorithm (§1.5)
- Prime numbers: infinitude, Sieve of Eratosthenes (§3.1)
- Bezout's Theorem (§3.3)
- The Euclidean algorithm (§3.4)
- The Fundamental Theorem of Arithmetic (§3.5)
- The extended Euclidean algorithm (§3.4)
- Solvability criteria for linear Diophantine equations (§3.7)
- Congruences: definition and basic properties (§4.1)
- Representations of integers (§2.1)
- Modular exponentiation (§4.1)
- Modular inverses (§4.2)
- Chinese Remainder Theorem (§4.3)
- Hensel's Lemma (§4.4)
- Solving linear systems of congruences (§4.5)
- Applications of congruences: divisibility tests (§5.1), and if time permits: character ciphers (§8.1), checksums (§5.4)

(2) **Quadratic congruences, reciprocity, and primitive roots**
- Special congruences modulo primes: Wilson's Theorem, Fermat's Little Theorem (§6.1)
- Euler's criterion and Gauss's lemma on quadratic residues (§11.1)
- Quadratic reciprocity (§11.2)
- Jacobi symbols (§11.3)
- Euler's Theorem; Euler ϕ-function (§6.3, §7.1)
- Multiplicative order and primitive roots (§9.1)
- Primitive roots modulo primes: Lagrange's Theorem (§9.2)
- Existence criterion for primitive roots (§9.3)
- Discrete logarithm and index arithmetic (§9.4)

(3) **Applications of number theory**

- Algorithmic efficiency and $\mathcal{O}$-notation (§2.2)
- Primality testing using Fermat's Little Theorem (§6.2)
- Primality testing using orders and primitive roots (§9.5)
- Factorization techniques: Pollard Rho method (§4.6), Pollard $p-1$ method (§6.1)
- Public key cryptography: textbook RSA (§8.4), improvements, and attacks
- Public key cryptography: Diffie-Hellman key exchange (§8.6)
- Public key cryptography: Hash functions and digital signatures
- (If time permits) Pseudorandom number generation