MATH 312: INTRODUCTION TO NUMBER THEORY

UBC, SUMMER 1 TERM 2015, L. PESKIN

61

Arithmeticorum Liber II.

Interuallum numeroums, minoraurem ℓ^{-1} intervol ALL LICUL ALL IN. arque ideo maior IN. +2. Oportet est de si de si

IN QVAESTIONEM VII.

CONDITIONIS appofitz eadem ratio eft quz & appofitz przeedenti quzflioni, nil enim Caliud requirit quàm ve quadratus internalli numerorum fit minor internallo quadratorum, & Canones iidem hie etiam locum habebunt, ve manifeftum eft.

QVÆSTIO VIII.

QVESTIO VIII. Province de la conserve d'arte d

OBSERVATIO DOMINI PETRI DE FERMAT.

O'bum autem in duos cubes, aut quadratoquadratum in duos quadratoquadratos dem nominis fas eft duidere cuius rei duosfrationem mirabilem fane detexi, Hane marginis exignitas non caperei.

QVÆSTIO IX.

R diuidere in duos quadratum 16 tur rurfus primi latus 1 N. alterius verò the runus primi ratus 1 N, shering vero quotcunque numerorum cum defectu tor vnitatum, quot conflat latus diuidendi. Effo itaques N. – 4; erunt quadrati, hic quidem 1 Q, ille vero 4 Q, + 16, – 16 N. Cærtenum volo vtrumque finul aquari vnitatibus 16. [gitur 5 Q, = 16, – 16 N. æquatur vnitatibus 16. & fit 1 N, ⁴ erit

E Σ T Ω d'à màn rào să repapara di-chină ai, d'o respandare, rescheman i re quáreu radegi el bêc, i î re irique că card direa teleface de carde carde carde publica radegi. Seu dir că J sailu el J. Serre și oregiona de că di dudane cură le ch dudane J. et a Mella că s. gui ch dudane J. et a Nella că s. gui איז וד. אמן ז'ויודמו ם מפוטאוטק וד H iii

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

United States Patent [19] 4,405,829 [11] Sep. 20, 1983 Rivest et al. [45] [54] CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD ald L. Rivest, Belma mir, Cambridge; Lee eman, Arlington, all [75] Inventors: Ro [57] ABSTRACT [73] Assignce: al having an end oding dev [21] Appl. No.: 860,586 Dec. 14, 1977 [22] Filed: 4K 1/00; H04I 9/04 178/22.1; 178/22.11 178/22, 22.1, 22.11, 178/22, 14, 22.15 [56] References Cited U.S. PATENT DOCUMENTS 3,657,476 4/1972 Aiken ... OTHER PUBLICATIONS New Directions in Cryptography", Diffie et al., *IEEE* ransactions on Information Theory, vol. IT-22, No. 6, lov. 1976, pp. 644-654. Theory of Numbers' Stewart, MacMillan Co., 1952, p. 133-135. er) and i at is d vo pre er. The r

usery of Numbers' Stewart, macrossen 133-135. iffle et al., Multi-User Cryptographic Techniques'', "Be Conference Proceedings, vol. 45, pp. 109-112,

d by the p

40 Claims, 7 Drawing Figure



RSA cryptosystem patent (US #4405829), 1983.

http://www.google.com/patents/US4405829

GENERAL INFO

Lectures: 201 LSK, 10:00-12:00 TuThFri and 9:30-10:30 Wed Office hours: TuTh 1:00-2:30 and by appointment, 300C LSK **Instructor:** Laura Peskin Instructor email: lpeskin@math.ubc.ca Grader: Thomas Roehrl Course webpage: http://www.math.ubc.ca/~lpeskin/ma312s15.html Textbook: Elementary Number Theory and Its Applications, Kenneth H. Rosen, 6th edition. Midterm exam date: Thursday, June 4, in class Final exam date: TBA

1

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 four parts, each with its own set of goals:

- (1) **Divisibility, modular arithmetic, and linear systems of congruences** (weeks 1-3). Topics include the Euclidean Algorithm, Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem. The ideas will be quite concrete and we will 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) Polynomial congruences, quadratic residues, and primitive roots (weeks 3-5). 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) **Payoff #1: Diophantine equations** (week 5). In the fifth week, we'll come back to the question of when it is possible to find integer solutions to certain Diophantine equations, using Fermat descent to prove the Two-Square Theorem and perhaps even a case of Fermat's Last Theorem. We'll also use Hensel's Lemma to analyze the existence of integer solutions to certain kinds of quadratic equations.
- (4) **Payoff #2: Primality testing and public key cryptography** (week 6). Finally, we'll apply the ideas of the first two parts to understand how two people can exchange secret information (such as a password or credit card number) over an insecure channel (such as a public wifi network). In particular, we'll talk about the Miller-Rabin probabilistic primality test, the Diffie-Hellman key exchange protocol, and the RSA cryptosystem.

A detailed list of topics (with references to the textbook) is posted on the course webpage and will be updated as the course progresses.

EVALUATION

Grading scheme: 20% weekly homeworks (5 assignments, weighted equally), 30% midterm exam, 50% final exam.

Homework info: Homework assignments are due at 9:30am in class on Wednesdays, beginning on May 20. 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 three to five 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.

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 two 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.