David J. Webb
david.webb@chaminade.edu
Henry Hall 123E

MA-301: NUMBER THEORY AND CRYPTOGRAPHY

Prerequisite: MA-105 or MA-110, or an equivalent course.

Description: Introductory elements of number theory, and their cryptographic applications. Topics include modular arithmetic, divisibility and primes, quadratic reciprocity, quadratic residues, the Legendre and Jacobi symbols, elementary number theoretic functions, Diophantine equations, frequency analysis, Rabin and RSA encryption and an introduction to other encryption systems.

Textbook: I am on a quest to not require textbooks for upper division courses, so I will be uploading course notes to Canvas. I will mostly follow the standard text for a course like this, *Elementary Number Theory* by Kenneth H. Rosen - but I may also pull material from identically named books by James K. Strayer and Charles Vanden Eynden.

Time/Location MWF, 2:30 - 3:20, in Brogan 101.

Office Hours: Officially, my office hours are M-F 11:30 - 12:30, in Henry 123 E, but in general, if my office door is open, feel free to stop in! I am also happy to meet by appointment, if you schedule at least a day in advance. My schedule can be found here.

Attendance: I would prefer not to take attendance, but alas, that is not to be - course attendance within the School of Natural Sciences and Mathematics has not been where it should be. Our class is fairly small, so I will be keeping track!

Grading: The percentage breakdown for the course will be

- 10% Attendance (lecture)
- 35% Homework
- 25% Midterm (Midway through the semester)
- 30% Final Exam (consult the final exam schedule set by the university)

I may alter traditional grade cutoffs, but only to your benefit (for instance an 88% may be an A, but a 91% would never be a B).

I generally grade on a five point scale (or some multiple thereof):

- 5 (a complete and perfect response)
- 4 (excellent with only minor errors)
- 3 (the right idea or approach)
- 2 (some understanding of the relevant ideas, but has substantial errors)
- 1 (some understanding of some ideas, quite off-track)
- 0 (no response)

Homework: Homework will be posted to Canvas intermittently, with a deadline a week or two later. Handwritten or digital copies are fine - if you'd like to learn LaTeX to typeset things, I'd be happy to teach you! **Upload a pdf of your finished work to the Canvas assignment page** - that is the easiest way for me to can grade your work and return it to you.

Late/Makeup Work: I reserve the right not to accept late work without a request in advance -

I may still take it, but it's not a guarantee! Instead, I will drop your lowest homework score at the end of the semester.

Academic Honesty: You are encouraged to discuss problems with others, but the solutions you submit should be your own. Do please tell me who you worked with, if you poked at problems together. Cheating on exams is a serious offense and will be dealt with accordingly.

Electronics: Out of consideration for your classmates, please set your cell phone to silent during class. You are of course more than welcome to take notes digitally, or consult your online textbook during class, whether on a tablet or laptop.

Getting Help: If you feel you are falling behind or struggling with the coursework, please get in touch with me - either come to office hours or send me an e-mail. Rather than let you suffer in silence, I want to help you succeed in this course! I am more than happy to meet outside of office hours if those times don't work, but it's your responsibility to get in touch with me to schedule something.

Disability Access: Any student who feels the need for an accommodation based on the impact of a disability is invited to contact me privately. Students with special needs who meet criteria for the Americans with Disabilities Act (ADA) provisions must provide written documentation of the need for accommodations from Kōkua 'Ike: Center for Student Learning by the end of week three of the class, in order for instructors to plan accordingly. If a student would like to determine if they meet the criteria for accommodations, they should contact the Kōkua 'Ike Coordinator at (808) 739-8305 for further information (ada@chaminade.edu).

Deadlines: The add/drop period this semester runs until **Tuesday, September 2nd**, and the deadline to Withdraw without Record is **Friday, September 26th**.

Tutoring and Writing Services: Chaminade is proud to offer free, one-on-one tutoring and writing assistance to all students. Tutoring and writing help is available on campus at Kōkua 'Ike: Center for Student Learning in a variety of subjects (including math! But also biology, chemistry, nursing, English, etc.) from trained Peer and Professional Tutors. Please check Kōkua 'Ike's website for the latest times, list of drop-in hours, and information on scheduling an appointment.

University Attendance Policy: See the academic handbook. In general, you are expected to attend regularly all classes regularly, and notify me when illness or other extenuating circumstances prevents them from attending class (preferably via email, so I have a written record).

Marianist Values: This class represents one component of your education at Chaminade University of Honolulu. An education in the Marianist Tradition is marked by five principles and you should take every opportunity possible to reflect upon the role of these characteristics in your education and development:

(1) Education for formation in faith
(2) Provide an integral, quality education
(3) Educate in family spirit
(4) Educate for service, justice and peace
(5) Educate for adaptation and change

Native Hawaiian Values: Education is an integral value in both Marianist and Native Hawaiian culture. Both recognize the transformative effect of a well-rounded, value-centered education on

society, particularly in seeking justice for the marginalized, the forgotten, and the oppressed, always with an eye toward God (Ke Akua). This is reflected in the ʻOlelo Noʻeau (Hawaiian proverbs):

(1) **Mana**: E ola au i ke akua (ʻŌlelo Noʻeau 364)
May I live by God
(2) **Naʻauao**: Lawe i ka maʻalea a kūʻonoʻono (ʻŌlelo Noʻeau 1957)
Acquire skill and make it deep
(3) **ʻOhana**: ʻIke aku, ʻike mai, kōkua aku kōkua mai; pela iho la ka nohana ʻohana (ʻŌlelo Noʻeau 1200)
Recognize others, be recognized, help others, be helped; such is a family relationship
(4) **Aloha**: Ka lama kū o ka noʻeau (ʻŌlelo Noʻeau 1430)
Education is the standing torch of wisdom
(5) **Aina**: ʻAʻohe pau ka ʻike i ka hālau hoʻokahi (ʻŌlelo Noʻeau 203)
Not all knowledge is taught in the same school

Program Learning Outcomes (PLOs)

(1) To demonstrate the understanding and skills in reading, interpreting, and communicating mathematical concepts which are integrated into other disciplines or appear in everyday life.
(2) To gain understandings of, and practical skills in logical thinking, deductive and inductive reasoning.
(3) To articulate the understanding of more advanced mathematical concepts and computational skills to support the study of other disciplines, including skills with numeric, analytic, and graphical methods.
(4) Where relevant, to develop mathematical maturity to undertake higher-level studies in mathematics and related fields.

Course Learning Outcomes (CLOs)

(1) Understand and apply modular arithmetic, divisibility, and the finite fields $\mathbb{Z}/p\mathbb{Z}$.
(2) Solve linear congruences and apply the Chinese remainder theorem
(3) Compute the Legendre and Jacobi symbols, and understand their properties
(4) Understand the importance of number theoretic concepts in cryptographic applications, such as public-key cryptography

Student Conduct Policy: Campus life is a unique situation requiring the full cooperation of each individual. For many, Chaminade is not only a school, but a home and a place of work as well. That makes it a community environment in which the actions of one students may directly affect other students. Therefore, each person must exercise a high degree of responsibility. Any community must have standards of conduct and rules by which it operates. At Chaminade, these standards are outlined so as to reflect both the Catholic, Marianist values of the institution and to honor and respect students as responsible adults. All alleged violations of the community standards are handled through an established student conduct process, outlined in the Student Handbook, and operated within the guidelines set to honor both students' rights and campus values.

Students should conduct themselves in a manner that reflects the ideals of the University. This includes knowing and respecting the intent of rules, regulations, and/or policies presented in the Student Handbook, and realizing that students are subject to the University's jurisdiction from the time of their admission until their enrollment has been formally terminated. Please refer to the Student Handbook for more details. A copy of the Student Handbook is available on the Chaminade website under Student Life. For further information, please refer to the Chaminade Catalog.

Title IX Compliance: Chaminade University of Honolulu recognizes the inherent dignity of all individuals and promotes respect for all people. Sexual misconduct, physical and/or psychological abuse will NOT be tolerated at CUH. If you have been the victim of sexual misconduct, physical and/or psychological abuse, we encourage you to report this matter promptly. As a faculty member, I am interested in promoting a safe and healthy environment, and should I learn of any sexual misconduct, physical and/or psychological abuse, I must report the matter to the Title IX Coordinator. If you or someone you know has been harassed or assaulted, you can find the appropriate resources by visiting Campus Ministry, the Dean of Students Office, the Counseling Center, or the Office for Compliance and Personnel Services.

Credit Hour Policy The unit of semester credit is defined as university-level credit that is awarded for the completion of coursework. One credit hour reflects the amount of work represented in the intended learning outcomes and verified by evidence of student achievement for those learning outcomes. Each credit hour earned at Chaminade University should result in a minimum of 45 hours of engagement, regardless of varying credits, duration, modality, or degree level. This equates to one hour of classroom or direct faculty instruction and a minimum of two hours of out-of-class student work each week for approximately fifteen weeks for one semester. Terms that have alternative lengths, such as 10 week terms, should have an equivalent amount of faculty instruction and out-of-class student work to meet each credit hour. Direct instructor engagement and out-of-class work result in total student engagement time of 45 hours for one credit. The number of engagement hours may be higher, as needed to meet specific learning outcomes.

Specific Credit Situation: The minimum 45 hours of engagement per credit hour can be satisfied in fully online, internship, or other specialized courses through several means, including (a) regular online instruction or interaction with the faculty member and fellow students and (b) academic engagement through extensive reading, research, online discussion, online quizzes or exams; instruction, collaborative group work, internships, laboratory work, practica, studio work, and preparation of papers, presentations, or other forms of assessment. This policy is in accordance with federal regulations and regional accrediting agencies.

How This Course Meets The Credit Hour Policy This is a three-credit hour course requiring 135 clock hours of student engagement, per the official CUH Credit Hour Policy. Students enrolled in this course are anticipated to spend 40 hours in class, 10 hours studying for the midterm, and 10 hours studying for the final. There will be an additional $\sim$4.5 hours of work required each week beyond what is listed here, mainly in the form of homework assignments.