CMPSC & MATH 467 FACTORIZATION AND PRIMALITY TESTING FALL 2025 SYLLABUS

Class number: 29392 & 23260, **Course ID**: 029559
Instructor: Bob Vaughan, 335 McAllister. **Email**: rcv4psu.edu
Web: `https://personal.science.psu.edu/rcv4/`
or (from 1 September) `https://psu-science.github.io/rcv4.github.io/`
Office Hours: MWF 10:10–11:00 and otherwise by arrangement.
Class: MWF 09:05–09:55 Erickson Food Science Bldg 133.
Text: • Vaughan, An Introduction to Factorization and Primality Testing
`https://personal.science.psu.edu/rcv4/FACPRIM.pdf`
or `https://psu-science.github.io/rcv4.github.io/FACPRIM.pdf`
• Bressoud, Factorization and Primality Testing, Springer, ISBN–10: 0387970400, ISBN–13: 978-0387970400.
• A possible alternative is: Wagstaff, The Joy of Factoring, AMS,
ISBN–10: 1470410486, ISBN–13: 978-1470410483.
• A more advanced standard reference is: Crandall and Pomerance, Prime Numbers: A Computational Perspective, Springer, ISBN–10: 0387252827,
ISBN–13: 978-0387252827.
• For theoretical background see:
Vaughan, A Course of Elementary Number Theory; follow the link to my personal web site at `https://personal.science.psu.edu/rcv4/CENT.pdf`
or `https://psu-science.github.io/rcv4.github.io/CENT.pdf`
LeVeque, Fundamentals of Number Theory, Dover, ISBN–10: 0486689069,
ISBN–13:978-0486689067,
Davenport, The Higher Arithmetic, CUP, ISBN–10: 0521722365,
ISBN–13: 978-0521722360.
Homework: Submit Mondays on Canvas or Wednesday when Monday a holiday.
First homework due Wednesday 3rd September.
Grading: • Homework 35%,
• First Midterm Exam: In class Wednesday 24th September 15%,
• Second Midterm Exam: In class Monday 3rd November 15%,
• The final will be a take-home project due Monday 15th December 35%.
Last date for feedback on Final Project Friday 5th December.
Grades: A 90–100%, B 80–89%, C 70–79%, D 60 - 69%, F 0 - 59%. These ranges may be adjusted downward and the ± grades will be within the appropriate ranges.
There is **NO** extra credit work.

Topics. This course is a mix of rigorous mathematical theory, requiring detailed proofs, and the solution of real problems via multi-precision computer calculations. We will discuss Unique factorization and Euclid's Algorithm, Primality, Congruences, RSA, Some Factorization Techniques, Pseudoprimes, Quadratic Reciprocity, The Quadratic Sieve and Primitive Roots, Orders of Magnitude of Arithmetical Functions, especially as that relates to the comparative speed of algorithms.

• Some prior knowledge of computing is essential. The recommended software is PARI/GP, available for free from `http://pari.math.u-bordeaux.fr`
At least some exams, including the final, will be run as computational projects.

Course objective. By the end of the course the student should be able to devise a program which can factor quite large numbers by the quadratic sieve.

• Late homework will not be accepted unless prior permission is granted. No homework will be accepted after the graded ones have been returned to the students.

• No makeup exams are available except by prior arrangement in extenuating circumstances.

• All Penn State Policies regarding academic integrity apply to this course. Academic integrity is the pursuit of scholarly activity in an open, honest and responsible manner. Academic integrity is a basic guiding principle for all academic activity at The Pennsylvania State University, and all members of the University community are expected to act in accordance with this principle. Consistent with this expectation, the University's Code of Conduct states that all students should act with personal integrity, respect other students' dignity, rights and property, and help create and maintain an environment in which all can succeed through the fruits of their efforts.

Academic integrity includes a commitment by all members of the University community not to engage in or tolerate acts of falsification, misrepresentation or deception. Such acts of dishonesty violate the fundamental ethical principles of the University community and compromise the worth of work completed by others.

• Penn State welcomes students with disabilities into the University's educational programs. Every Penn State campus has an office for students with disabilities. Student Disability Resources (SDR) website provides contact information for every Penn State campus
`https://equity.psu.edu/offices/student-disability-resources`
For further information, please visit Student Disability Resources website
`http://equity.psu.edu/sdr/`
In order to receive consideration for reasonable accommodations, you must contact the appropriate disability services office at the campus where you are officially

enrolled, participate in an intake interview, and provide documentation: See documentation guidelines `http://equity.psu.edu/sdr/guidelines`
If the documentation supports your request for reasonable accommodations, your campus disability services office will provide you with an accommodation letter. Please share this letter with your instructors and discuss the accommodations with them as early as possible. You must follow this process for every semester that you request accommodations.

• Many students at Penn State face personal challenges or have psychological needs that may interfere with their academic progress, social development, or emotional wellbeing. The university offers a variety of confidential services to help you through difficult times, including individual and group counseling, crisis intervention, consultations, online chats, and mental health screenings. These services are provided by staff who welcome all students and embrace a philosophy respectful of clients' cultural and religious backgrounds, and sensitive to differences in race, ability, gender identity and sexual orientation.
Counseling and Psychological Services at University Park (CAPS)
(`http://studentaffairs.psu.edu/counseling/`): 814-863-0395
Counseling and Psychological Services at Commonwealth Campuses
(`https://studentaffairs.psu.edu/counseling/caps-campuses`)
Penn State Crisis Line (24 hours/7 days/week): 877-229-6400. Crisis Text Line (24 hours/7 days/week): Text LIONS to 741741

• Consistent with University Policy AD29, students who believe they have experienced or observed a hate crime, an act of intolerance, discrimination, or harassment that occurs at Penn State are urged to report these incidents as outlined on the University's Report Bias webpage (`http://equity.psu.edu/reportbias/`)

• When searching for help with your course, your instructor will always be the best resource for advice. The University is aware of fraudulent companies and scammers who prey on a student's desire for assistance with coursework. A student who hires someone to do work on their behalf demonstrates a clear example of a violation of academic integrity highlighted above. Sharing login credentials with others is also in violation of Penn State Policy AD95 and may be subject to additional disciplinary action. Furthermore, a fraudulent company and/or scammer may extort the student by threats to communicate the student's arrangement with the University. If you find yourself in such a situation, it is best to contact your instructor immediately.