

Factorization and Primality Testing Syllabus

Robert C. Vaughan

July 24, 2023

The Syllabus

Integrity
Disability
Challenges
Bias

- Welcome to Math 467, Fall 2023.
- I start by giving an overview of the syllabus and general organizational matters.

The Syllabus

Integrity
Disability
Challenges
Bias

- If you need to contact me outside the class, the quickest way is via email at rcv4@psu.edu.

The Syllabus

Integrity
Disability
Challenges
Bias

- If you need to contact me outside the class, the quickest way is via email at rcv4@psu.edu.
- My name is Bob Vaughan

The Syllabus

Integrity
Disability
Challenges
Bias

- If you need to contact me outside the class, the quickest way is via email at rcv4@psu.edu.
- My name is Bob Vaughan
- My normal office hours will be MWF, 10:10-11:00.

The Syllabus

Integrity
Disability
Challenges
Bias

- If you need to contact me outside the class, the quickest way is via email at rcv4@psu.edu.
- My name is Bob Vaughan
- My normal office hours will be MWF, 10:10-11:00.
- We can always set up one-off one-on-one Zoom meetings as necessary.

The Syllabus

Integrity
Disability
Challenges
Bias

- If you need to contact me outside the class, the quickest way is via email at rcv4@psu.edu.
- My name is Bob Vaughan
- My normal office hours will be MWF, 10:10-11:00.
- We can always set up one-off one-on-one Zoom meetings as necessary.
- I strongly urge students to meet with me one-on-one if there are difficulties with the theory or homework.

The Syllabus

Integrity
Disability
Challenges
Bias

- If you need to contact me outside the class, the quickest way is via email at rcv4@psu.edu.
- My name is Bob Vaughan
- My normal office hours will be MWF, 10:10-11:00.
- We can always set up one-off one-on-one Zoom meetings as necessary.
- I strongly urge students to meet with me one-on-one if there are difficulties with the theory or homework.
- I am going to use Beamer in class and these files will be made available on Canvas.

- My notes will be written up as a textbook FACPRIM.pdf file which will be available on Canvas and will be updated as the course progresses.

- My notes will be written up as a textbook FACPRIM.pdf file which will be available on Canvas and will be updated as the course progresses.
- Useful texts are
Bressoud, Factorization and Primality Testing, Springer,
ISBN-10: 0387970400, ISBN-13: 978-0387970400.

- My notes will be written up as a textbook FACPRIM.pdf file which will be available on Canvas and will be updated as the course progresses.
- Useful texts are
Bressoud, Factorization and Primality Testing, Springer, ISBN-10: 0387970400, ISBN-13: 978-0387970400.
- Wagstaff, The Joy of Factoring, AMS, ISBN-10: 1470410486, ISBN-13: 978-1470410483.

- My notes will be written up as a textbook FACPRIM.pdf file which will be available on Canvas and will be updated as the course progresses.
- Useful texts are
Bressoud, Factorization and Primality Testing, Springer, ISBN-10: 0387970400, ISBN-13: 978-0387970400.
- 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://sites.psu.edu/rcv4/16-2/> or look for the
file CENT.pdf on Canvas.

- For theoretical background see:
Vaughan, A Course of Elementary Number Theory; follow
the link to my personal web site at
<https://sites.psu.edu/rcv4/16-2/> or look for the
file CENT.pdf on Canvas.
- LeVeque, Fundamentals of Number Theory, Dover,
ISBN-10: 0486689069, ISBN-13: 978-0486689067.

The Syllabus

- For theoretical background see:
Vaughan, A Course of Elementary Number Theory; follow
the link to my personal web site at
<https://sites.psu.edu/rcv4/16-2/> or look for the
file CENT.pdf on Canvas.
- 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.

The Syllabus

Integrity
Disability
Challenges
Bias

- Homework is due Mondays or the first class in the week when Monday is a holiday, and should be uploaded to CANVAS.

The Syllabus

Integrity
Disability
Challenges
Bias

- Homework is due Mondays or the first class in the week when Monday is a holiday, and should be uploaded to CANVAS.
- 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.

The Syllabus

Integrity
Disability
Challenges
Bias

- Homework is due Mondays or the first class in the week when Monday is a holiday, and should be uploaded to CANVAS.
- 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.
- Collaboration is allowed on homework, but only if it is described in the submission and the collaborators listed. Copying is strictly banned and will lead to penalties.

The Syllabus

Integrity
Disability
Challenges
Bias

- Homework 35%,

The Syllabus

Integrity
Disability
Challenges
Bias

- Homework 35%,
- Midterm Exams: Wednesday 27th September 10%,
Wednesday 8th November 20%,

The Syllabus

Integrity
Disability
Challenges
Bias

- Homework 35%,
- Midterm Exams: Wednesday 27th September 10%,
Wednesday 8th November 20%,
- Final Exam 35%,

The Syllabus

Integrity
Disability
Challenges
Bias

- Homework 35%,
- Midterm Exams: Wednesday 27th September 10%,
Wednesday 8th November 20%,
- Final Exam 35%,
- At least some exams, including the final, will be run as computational projects.

The Syllabus

Integrity
Disability
Challenges
Bias

- Homework 35%,
- Midterm Exams: Wednesday 27th September 10%,
Wednesday 8th November 20%,
- Final Exam 35%,
- At least some exams, including the final, will be run as computational projects.
- No makeup exams are available except by prior arrangement in extenuating circumstances.

- We will discuss Unique factorization and Euclid's Algorithm, Primality, Congruences, RSA, Some Factorization Techniques, Pseudoprimes, Quadratic Reciprocity, The Quadratic Sieve and Primitive Roots.

- We will discuss Unique factorization and Euclid's Algorithm, Primality, Congruences, RSA, Some Factorization Techniques, Pseudoprimes, Quadratic Reciprocity, The Quadratic Sieve and Primitive Roots.
- If there is time there might be some discussion of Elliptic Curves, and The Number Field Sieve.

- We will discuss Unique factorization and Euclid's Algorithm, Primality, Congruences, RSA, Some Factorization Techniques, Pseudoprimes, Quadratic Reciprocity, The Quadratic Sieve and Primitive Roots.
- If there is time there might be some discussion of Elliptic Curves, and The Number Field Sieve.
- Very little prior knowledge of computing is required. The recommended software is PARI/GP, available for free from <http://pari.math.u-bordeaux.fr/>

- We will discuss Unique factorization and Euclid's Algorithm, Primality, Congruences, RSA, Some Factorization Techniques, Pseudoprimes, Quadratic Reciprocity, The Quadratic Sieve and Primitive Roots.
- If there is time there might be some discussion of Elliptic Curves, and The Number Field Sieve.
- Very little prior knowledge of computing is required. The recommended software is PARI/GP, available for free from <http://pari.math.u-bordeaux.fr/>
- 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.

- We will discuss Unique factorization and Euclid's Algorithm, Primality, Congruences, RSA, Some Factorization Techniques, Pseudoprimes, Quadratic Reciprocity, The Quadratic Sieve and Primitive Roots.
- If there is time there might be some discussion of Elliptic Curves, and The Number Field Sieve.
- Very little prior knowledge of computing is required. The recommended software is PARI/GP, available for free from <http://pari.math.u-bordeaux.fr/>
- 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.
- Note that this course is a mix of theory and practical projects. Importantly the theory will involve proofs, and the projects will involve the production of computer programs which will act as proofs.

- 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.

The Syllabus

Integrity
Disability
Challenges
Bias

- 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 (<http://equity.psu.edu/sdr/disability-coordinator>). For further information, please visit Student Disability Resources website (<http://equity.psu.edu/sdr/>).

The Syllabus

Integrity
Disability
Challenges
Bias

- 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://senate.psu.edu/faculty/counseling-services-at-commonwealth-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

The Syllabus

Integrity
Disability
Challenges
Bias

- 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/>)