# Prerequisites

a. Modular arithmetic [1, §2.2]
b. Basic properties of divisibility [1, §1.1]
c. Euler's theorem and Fermat's little theorem [1, §2.7]
d. Chinese remainder theorem [1, §2.4]
e. structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ [1, §7.5]
f. Euler's phi function [1, §2.6]
g. Quadratic residues and quadratic reciprocity [1, §2.8, 12.1, 12.2]
h. Arithmetic in finite fields [1, Chap 19]
i. Frobenius automorphism of a finite field [1, §19.2]
j. Basic group theory: Lagrange's theorem [1, §6.3], cyclic groups [1, §6.5], structure of finitely generated abelian groups [1, §6.6]
k. Gaussian elimination (over a general field) [1, §14.4]

# Approximate Schedule

- Week 1 (Sep 10,12,14)

  1. Course overview
  2. Algorithmic complexity
  3. Fast algorithms for multiplication (Karatsuba and FFT) and division [2, §9.5], [1, §3.5];
  4. Exponentiation by repeated squaring (a) [2, §2.1.2, §9.3], [1, §3.4];
  5. The extended Euclidean algorithm (b), (3) [2, §2.1.1, §9.4, 9.6.2], [1, §4.1, 4.2, 17.4];
  6. Introduction to Sage

- Week 2 (Sep 17, 19, **21**)

  7. Computing (inverses) in $\mathbb{Z}/n\mathbb{Z}$ (c), (4), (5) [1, §4.3, 17.4], [2, §2.1.1, §9.3, §9.4.2]
  8. Effective Chinese remainder theorem (d), (7), [1, §4.3, 17.4], [2, §2.1.3];
  9. Multiplicative orders and generators (e), (f) [1, §11.1];
  10. Computing the Jacobi symbol (g) [1, §12.3] [2, §2.3.1]

- Week 3 (Sep 24, 26, 28)

  11. Square roots modulo $p$ (h), (10) [2, §2.3.2] [1, §12.5]
  12. Randomized algorithms [1, Chap 9.];
  13. Miller-Rabin test (c), (e), (12) [1, §10.2], [2, §3.4, 3.5];

- Week 4 (Oct **1**, 3, 5)

  14. Lucas-Lehmer test (g), (i), (9) [2, §3.6.1, 4.2];
  15. Python dictionaries;
  16. Baby-step/giant-step for discrete logs (j), (15) [1, §11.2], [2, §5.3];

- Week 5 (Oct **10**, 12)

  17. Smooth numbers [1, §15.1], [2, §1.4.5, 3.3];
  18. Index-calculus (12), (16), (17) [1, §15.2], [2, §6.4];

- Week 6 (Oct **15**, 17, 19)

19. **Midterm!**
20. Pollard $p-1$ algorithm (c), (5) [2, §5.4];
21. Introduction to elliptic curves [2, §7.1, 7.2];
22. Hasse's theorem (21) [2, §7.3];
23. Elliptic curve method (5), (22) [2, §7.4];

- Week 7 (Oct 22, 24, **26**)

24. Shank-Mestre algorithm (16), (21) [2, §7.5.1]
25. Schoof's algorithm (8), (21), (33), (34) [2, §7.5.2];
26. Goldwasser-Killian test (11), (25) [2, §7.6.1];

- Week 8 (Oct 29, **31**, Nov 2)

27. Introduction to number fields;
28. Computing with ideals (27);
29. Binary quadratic forms [2, §5.6.1]
30. Class groups of quadratic fields (27), (29) [2, §5.6.3];

- Week 9 (Nov 5, 7, **9**)

31. Hilbert class polynomial (27) [2, §7.5.3]
32. Endomorphisms of elliptic curves (21), (27) [2, §7.5.3]
33. Frobenius endomorphism of an elliptic curve (i), (32) [2, §7.5.2]
34. Division polynomials for elliptic curves (21) [2, §7.5.2]

- Week 10 (Nov 14, 16)

35. Cornacchia-Smith for $x^2 + Dy^2 = p$ and $4p$ (11) [2, §2.3.4];
36. Atkin-Morain test (26), (31), (35) [2, §7.5.3, 7.6.1];

- Week 11 (Nov 19, 21, **23**)

37. Sieve of Eratosthenes [1, §5.4], [2, §3.1];
38. Quadratic sieve (e), (k), (5) [2, §6.1], [1, §15.3, 15.4];
39. Number field sieves (27), (38), [2, §6.2];

- Week 12 (Nov 26, 28, 30)

40. square-free factorization (i), (5), [1, §20.3];
41. distinct-degree factorization (40) [1, §20.4.1];
42. Cantor-Zassenhaus (8), (41) [1, §20.4.2];

- Week 13 (Dec 3, 5, **7**)

43. Final project presentations

# References


[1] V. Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge: Cambridge UP, 2008.

[2] R. Crandall and C. Pomerance. Prime Numbers: A Computational Perspective. Dordrecht: Springer-Verlag, 2006.