

Computations you need to be able to do.

1. Find  $\gcd(a, b)$ .
2. Find a linear combination of two integers adding to their gcd.
3. Add, subtract, and multiply mod  $m$ .
4. Multiply high powers mod  $m$ .
5. Find an inverse mod  $m$ .
6. Solve linear congruences.
7. Solve a system of congruences with different moduli.
8. Find the multiplicative order mod  $m$  of a number.
9. Find the number of classes invertible mod  $m$ .
10. Decompose a permutation into disjoint cycles.
11. Multiply two permutations using the cycle decomposition.
12. Find the order of a permutation.
13. Find the number of orbits of an action.
14. Decode a message encrypted with RSA.
15. Determine the number of bits of error that can be corrected for a linear code.
16. Create a list of error-correction vectors for a linear code.
17. Use a list of error-correction vectors to correct a binary transmission.
18. Decide when two 3-dimensional figures have the same symmetry.