Algorithms reference

Greatest common factors — Euclidean algorithm

To compute the greatest common factor of a and b:

1. Put a and b in the first column of a table (bigger number on top).
2. Fill in the next column: if the previous column contains x and y, the next column contains y and $x \bmod y$.
3. Repeat step 2 until you get a 0. The number above the 0 is the greatest common factor of a and b.

a	…	x	y	…	greatest common factor
b	…	y	$x \bmod y$	…	0

Multiplicative inverses — extended Euclidean algorithm

To compute the multiplicative inverse of a modulo q:

1. Write down the Euclidean algorithm table for a and q. A multiplicative inverse exists as long as the greatest common factor of a and q is 1.
2. Add another row to the table: if some column contains x and y, the third row will contain $x \div y$ rounded **downwards**. Ignore the column with 0.

x
y
round$(x \div y)$

3. Add a fourth row: put a 1 under the first column and a 0 sticking out to the left of the 1, then fill in each entry with (cell two to the left) – (cell to left) × (cell above left).

	z	
x	y	$x - y \times z$

4. When you reach the second-last column, the last number in the fourth row is the multiplicative inverse of a modulo q.

Modular powers

To compute $a^b \bmod q$:

1. Set $T = 1$.
2. Convert b to binary, and read left to right. For each digit:
   - If the digit is 0: replace T with $T^2 \bmod q$.
   - If the digit is 1: replace T with $T^2 \times a \bmod q$.
3. The final value of T is $a^b \bmod q$.