Contents

1 Euclid's Algorithm

1.1 Idea

Compute GCD Quickly by repeated division with remainder
Given a problem: $gcd(a, b)$, represent a as:

$$a = bq + r$$

where q is the quotient and r is the remainder. Now:

$$gcd(a, b) = gcd(b, r)$$

Set $a = b$ and $b = r$, then repeat until $r = 0$

1.2 Example

$$gcd(79, 19)$$

$$79 = 4(19) + 3$$
$$19 = 6(3) + 1$$
$$3 = 3(1) + 0$$

$$gcd(79, 19) = gcd(19, 3) = gcd(3, 1) = gcd(1, 0) = 1$$
$$gcd(79, 19) = 3$$

2 Three Ways to Compute GCD

1. Trial division of all numbers up to b
   $O(n), n = min(a, b)$
   Not feasible for large numbers
2. Taking all prime factors
   $O(e^{\sqrt{\log n}}), n = min(a, b)$
   Still not feasible for large numbers
3. Euclid's Algorithm
   $O(\log n), n = min(a, b)$
   Very fast

3 Extended Euclid's Algorithm

3.1 Idea

If $gcd(a, b) = d$ then there exists two integers x and y such that:

$$a(x) + b(y) = d$$

By using Euclid's Algorithm (backwards) we can find x and y

3.2 Example

Lets find x and y such that $79x + 19y = 1$

$$79x + 19y = 1$$

$$79 = 4(19) + 3$$
$$19 = 6(3) + 1$$
$$3 = 3(1) + 0$$

Trick: Starting with the last equation in which the remainder is not zero, solve all equations for the remainder and repeatedly substitute in the remainder from the previous equation.

$$1 = 1(19) - 6(3)$$
$$1 = 1(19) - 6(79 - 4(19))$$
$$1 = 1(19) - 6(79) + 24(19)$$
$$1 = -6(79) + 25(19)$$

$$x = -6, y = 25$$

We can now find $19^{-1} \pmod{79}$

$$1 \equiv -6(79) + 25(19) \pmod{79}$$
$$1 \equiv 0 + 25(19) \pmod{79}$$
$$19^{-1} \equiv 25 \pmod{79}$$

3.3 Mod 26 Example

Find $7^{-1} \pmod{26}$ using Euclid's Extended Alogrithm

$$26 = 3(7) + 5$$
$$7 = 1(5) + 2$$
$$5 = 2(2) + 1$$
$$2 = 2(1) + 0$$

$$gcd(26, 7) = gcd(7, 2) = gcd(5, 2) = gcd(2, 1) = 1$$

$$1 = 5 - 2(2)$$
$$1 = 5 - 2(7 - 1(5))$$
$$1 = 3(5) - 2(7)$$
$$1 = 3(26 - 3(7)) - 2(7)$$
$$1 = 3(26) - 11(7)$$
$$1 \equiv 3(26) - 11(7) \pmod{26}$$
$$1 \equiv 0 - 11(7) \pmod{26}$$
$$1 \equiv (15)(7) \pmod{26}$$
$$7^{-1} = 15 \pmod{26}$$

4 Exponentiation in Modular Arithmetic

4.1 Goal

Find a way to compute $a^b \pmod{m}$ very quickly, even if a, b, or m are large. Computing a^b is not always feasible, could be extremely large.

4.2 Steps

1. Write exponent b in binary
2. Repeatedly square $a \pmod{m}$ as many times as their were digits in b written in binary
3. Multiply together the numbers corresponding to the ones in b as binary

4.3 Example

$$5^{273} \pmod{11}$$

$$273 = 256 + 16 + 1$$
$$273 = 2^8 + 2^4 + 20$$
$$273_{10} = 100010001_2$$

$$5^1 \equiv 5 \pmod{11}$$
$$5^2 \equiv 25 \equiv 3 \pmod{11}$$
$$5^4 \equiv 3^2 \equiv 9 \pmod{11}$$
$$5^8 \equiv 9^2 \equiv 81 \equiv 4 \pmod{11}$$
$$5^{16} \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$$
$$5^{32} \equiv 5^2 \equiv 25 \equiv 3 \pmod{11}$$
$$5^{64} \equiv 3^2 \equiv 9 \pmod{11}$$
$$5^{128} \equiv 9^2 \equiv 81 \equiv 4 \pmod{11}$$
$$5^{256} \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$$

$$5^{273} \equiv 5^{256+16+1} \pmod{11}$$
$$5^{273} \equiv 5^{256} * 5^{16} * 5^1 \pmod{11}$$
$$5^{273} \equiv 5 * 5 * 5 \pmod{11}$$

$$5^{273} \equiv 4 \pmod{11}$$

4.4 Another Example

What is the last digit of 3^{212}?

$$212 = 128 + 64 + 16 + 4$$

$$212 = 2^7 * 2^6 * 2^4 * 2^2$$

$$212_{10} = 11010100_2$$

$$3^1 \equiv 3 \pmod{10}$$

$$3^2 \equiv 9 \pmod{10}$$

$$3^4 \equiv 9^2 \equiv 81 \equiv 1 \pmod{10}$$

$$3^8 \equiv 1^2 \equiv 1 \pmod{10}$$

$$3^{16} \equiv 3^{32} \equiv 3^{64} \equiv 3^{128} \equiv 1 \pmod{10}$$

$$3^{212} \equiv 3^{128} * 3^{64} * 3^{16} * 3^4$$

$$3^{212} \equiv 1 * 1 * 1 * 1 \equiv 1 \pmod{10}$$

The last digit of $3^{212} = 1$