Euclidean Algorithm

Prime Number Theorem

There are an infinite number of primes

The Prime Number Theorem:

Helps us estimate how many prime numbers are in the range 2 through x.

We define $\pi(x)$ as the number of primes from 2 to x.

Then,

$$\lim_{x \to \infty} \left(\frac{\pi(x)}{x/\ln(x)} \right) = 1 \qquad \left(\frac{\pi(x)}{x} \right) \approx \frac{1}{\ln(x)} \qquad \pi(x) \approx \frac{x}{\ln(x)}$$

The ratio of prime numbers between 2 and x to all numbers between 2 and x approaches 1/ln x as x approaches infinity.

Prime Number Theorem

The ratio of primes to all numbers is approximately $1/\ln(x)$.

$$\left(\frac{\pi(x)}{x}\right) \approx \frac{1}{\ln(x)}$$

As x gets larger, the ratio gets smaller.

In other words, primes become more sparse the larger the range.

If we choose a random number between 2 and x, the likelihood that it is prime is $1/\ln(x)$.

The number of primes in the range 2 through x is approximately $\pi(x) \approx \dfrac{x}{\ln(x)}$

Example:
How many primes are there between 2 and 1000?

$$\frac{x}{\ln(x)} = \frac{1000}{\ln(1000)} \approx 145$$

In Python, $\ln(x)$ is `math.log(x)`

Python demo

Greatest Common Divisor (GCD)

- Greatest Common Divisor – Largest integer that divides both numbers (i.e., **the largest factor of both numbers**)

What is the GCD of 24 and 36?

Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24
Factors of 36: 1, 2, 3, 4, 9, 12, 18, 36

Using Prime Factorizations:

24: $2^3 3^1$
36: $2^2 3^2$

Smallest exponents: $2^2 3^1 = 12$

What is the GCD of 6 and 32?

Factors of 6: 1, 2, 3, 6
Factors of 32: 1, 2, 4, 8, 16, 32

Using Prime Factorizations:

6: $2^1 3^1$
32: $2^5 3^0$

Smallest exponents: $2^1 3^0 = 2$

Rosen, Kenneth. *Discrete Mathematics and Its Applications, 7th Edition*. McGraw-Hill, 2012

GCD Theorem

Computing GCD of two integers is computationally difficult for large numbers. Why?

Finding the prime factorization of a large number is difficult. We only know how to do it using brute force.

We have a shortcut!

We can reduce the problem of finding the GCD of large numbers by using **mod**.

Let x and y be two positive integers where $x \neq 0$.

Then $\mathbf{gcd}(\boldsymbol{x}, \boldsymbol{y}) = \mathbf{gcd}(\boldsymbol{x}, \boldsymbol{y} \mathbf{\ mod\ } \boldsymbol{x})$.

In other words, the GCD of two integers is the same if we reduce one of those numbers using **mod** of the other number.

And we can keep going until one of the numbers is reduced to 0.

Example:

$\gcd(6, 32) = \mathbf{2}$

$\gcd(6, 32 \bmod 6) = \gcd(6, 2) = \mathbf{2}$

$\gcd(6 \bmod 2, 2) = \gcd(0, 2) = \mathbf{2}$

Recall the Division Theorem

- Dividing an integer by a positive integer produces a quotient q and remainder r.
- Let n and d be integers.
- Then there exist unique integers q and r where $0 \leq r < d$ such that $\boldsymbol{n = qd + r}$

Euclidean GCD Algorithm

Find the GCD of two numbers:

Using $n = qd + r$.

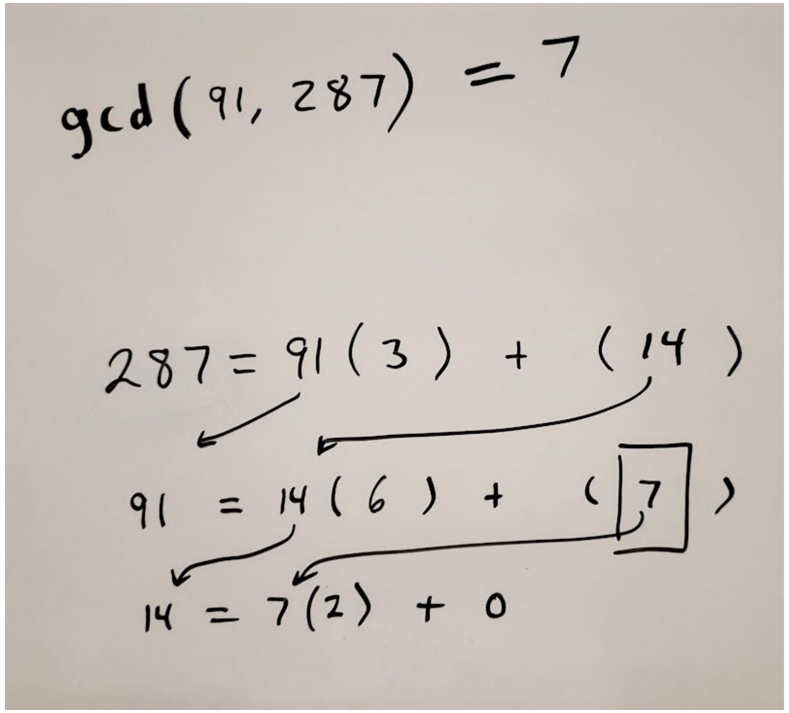
1. Divide larger number n by smaller number d to get q and r.
2. Shift d and r to be the new n and d.
3. Divide n by d to get a new q and r.
4. Repeat until the remainder is 0. The last non-zero remainder is the GCD.

Find gcd(97,11)

Find gcd(97,11)

1. $97 = (8)11 + 9$
2. $11 = (1)9 + 2$
3. $9 = (4)2 + \boxed{1}$
4. $2 = (2)1 + 0$

- Find the gcd(91, 287)



Find gcd(97,11)

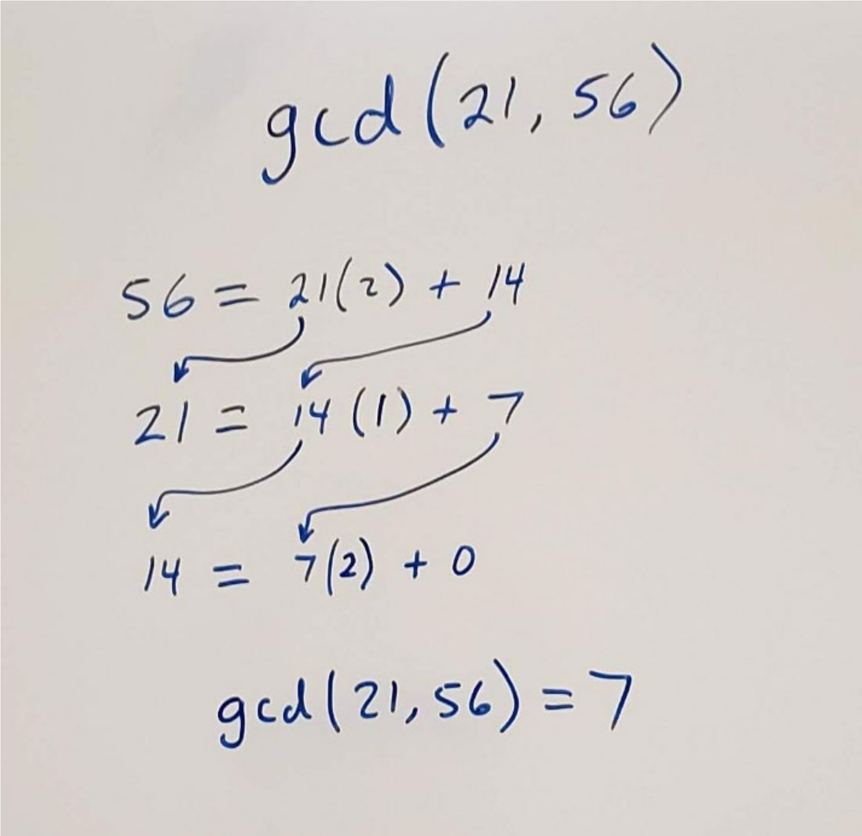
1. $97 = (8)11 + 9$

2. $11 = (1)9 + 2$

3. $9 = (4)2 + 1$

4. $2 = (2)1 + 0$

- Find gcd(21, 56)



Extended Euclidean Algorithm

Recall Theorem 9.1.1:
If x | y and x | z, then x | (sy + tz)
for any integers s and t.

The GCD of x and y can be expressed as a linear combination of x and y:

$\gcd(x, y) = sx + ty$ for some s and t. By the GCD Theorem, $\gcd(x, y) = \gcd(x, y \bmod x)$.

$\gcd(44, 38) = \gcd(44 \bmod 38, 38) = \gcd(6, 38) = \gcd(38 \bmod 6, 6) = \gcd(2, 6) = \gcd(6 \bmod 2, 2) = \gcd(0,2) = 2$

$\gcd(44, 38) = 2$. We can express this as a linear combination, $2 = s \cdot 44 + t \cdot 38$.

$2 = 38 \bmod 6 = 38 - (\quad) \cdot 6 = 38 - (6) \cdot 6$

$2 = 38 - 6 \cdot 6$

$6 = 44 \bmod 38 = 44 - (\quad) \cdot 38 = 44 - (1) \cdot 38$

$6 = 44 - 1 \cdot 38$

$2 = 38 - 6 \cdot (44 - 1 \cdot 38)$ substitute $(44 - 1 \cdot 38)$ for 6

$2 = 38 - 6 \cdot 44 + 6 \cdot 38$ simplify

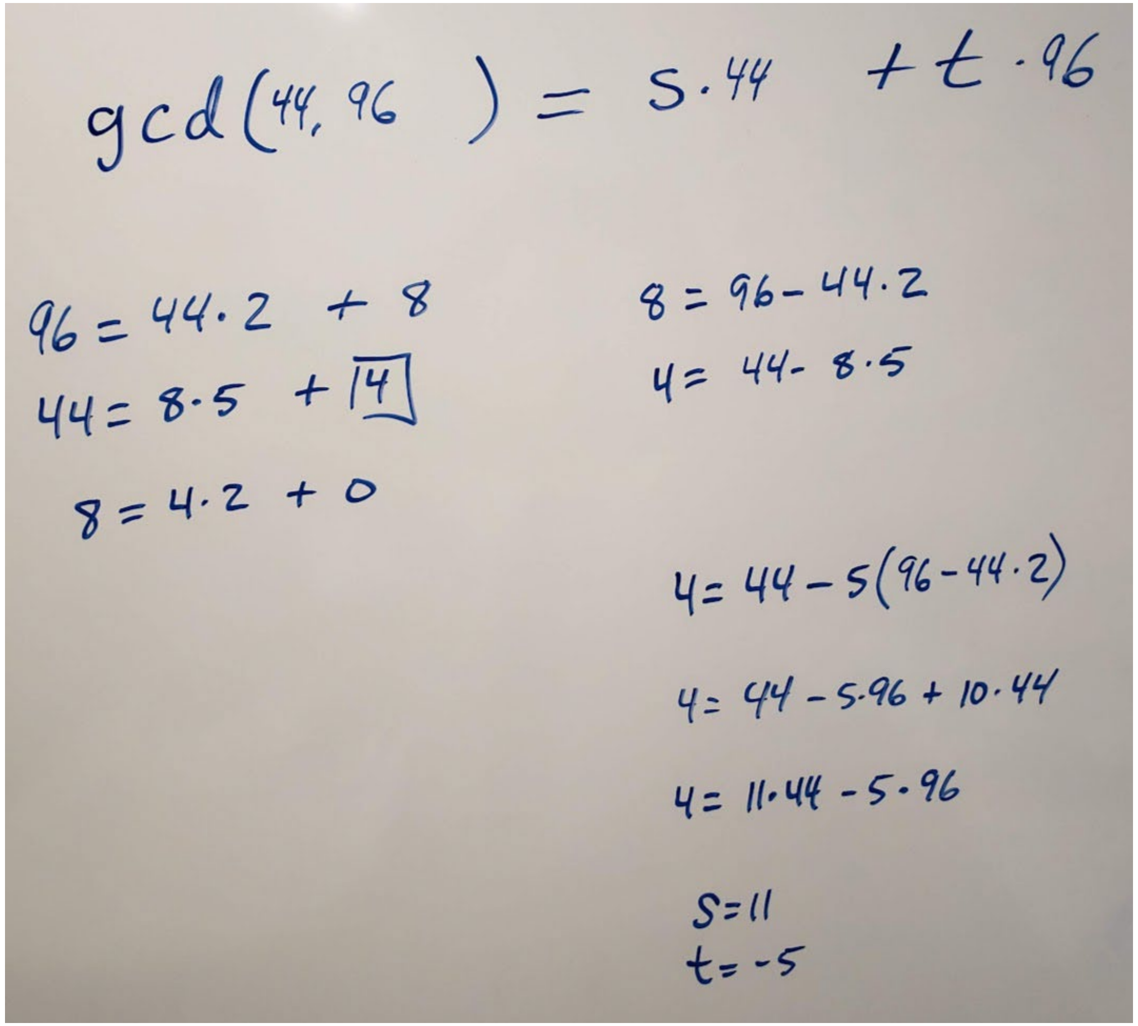
$2 = -6 \cdot 44 + 7 \cdot 38$ We have our linear combination

$s = -6$

$t = 7$

Demo

Find s and t such that $\gcd(44, 96) = s \cdot 44 + t \cdot 96$



Multiplicative Inverse (MMI)

The **MMI of $\boldsymbol{a}$** is an integer $\boldsymbol{x}$ such that $\boldsymbol{ax \bmod m = 1}$ where $x < m - 1$.

To find x, ask yourself "What number multiplied by a will result in 1 mod m?"

> Note: To have an MMI, a and m must be **relatively prime**.

Example:

What is the MMI of 5 under mod 7?

$5x \bmod 7 = 1$

What is x? Let's try a few numbers:

$5 \cdot 1 \bmod 7 = 5$, so it is not 1

$5 \cdot 2 \bmod 7 = 3$, so it is not 2

$5 \cdot 3 \bmod 7 = 1$, it is **3**. The MMI of 5 under mod 7 is 3.

0
6 1
5 2
4 3

MMI

Modular Multiplicative Inverse or Inverse Mod m or Multiplicative Inverse Mod m

MMIs are used in cryptography, especially the RSA Algorithm

$2x \equiv 1 \pmod{17}$

$2x \equiv_{17} 1$

What multiple of 2 is one more than a multiple of 17?

9

9 is an MMI of 2 under mod 17

The MMI exists only if a and m are coprime.

$ax \ mod \ m = 1$
$ax \equiv_m 1$
$ax \equiv 1 \ (mod \ m)$

What is the MMI of:

3 (mod 7)   (What multiple of 3 is one more than a multiple of 7?)

$3 \cdot x \equiv_7 1$

$x = 5$, so 5 is the MMI for 3 (mod 7).

Use Extended Euclidean to find MMI

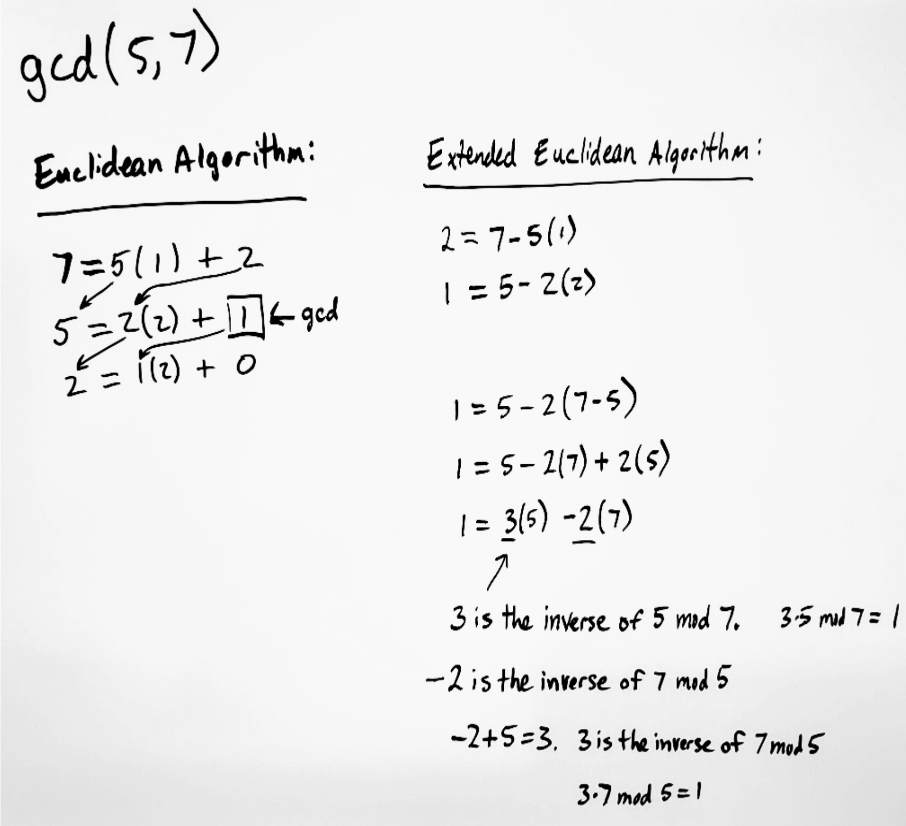
If $\gcd(x, n) \neq 1$, then there is no MMI.

If x and n are relatively prime, then $\gcd(x, n) = 1$, so we can find a linear combination $1 = sx + tn$.

s is the MMI of x under mod n because $sx - 1 = -tn$, so sx is 1 more than a multiple of n.

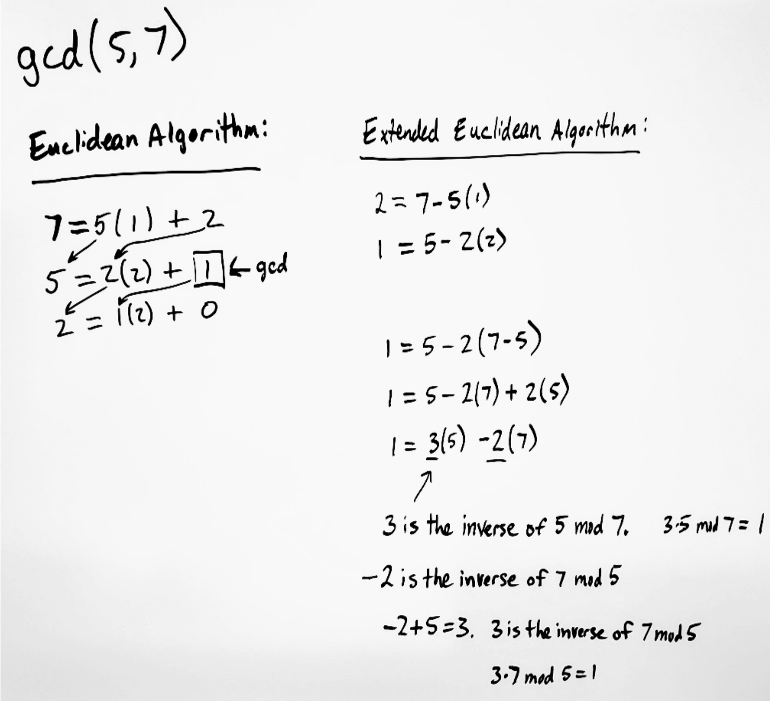
Example

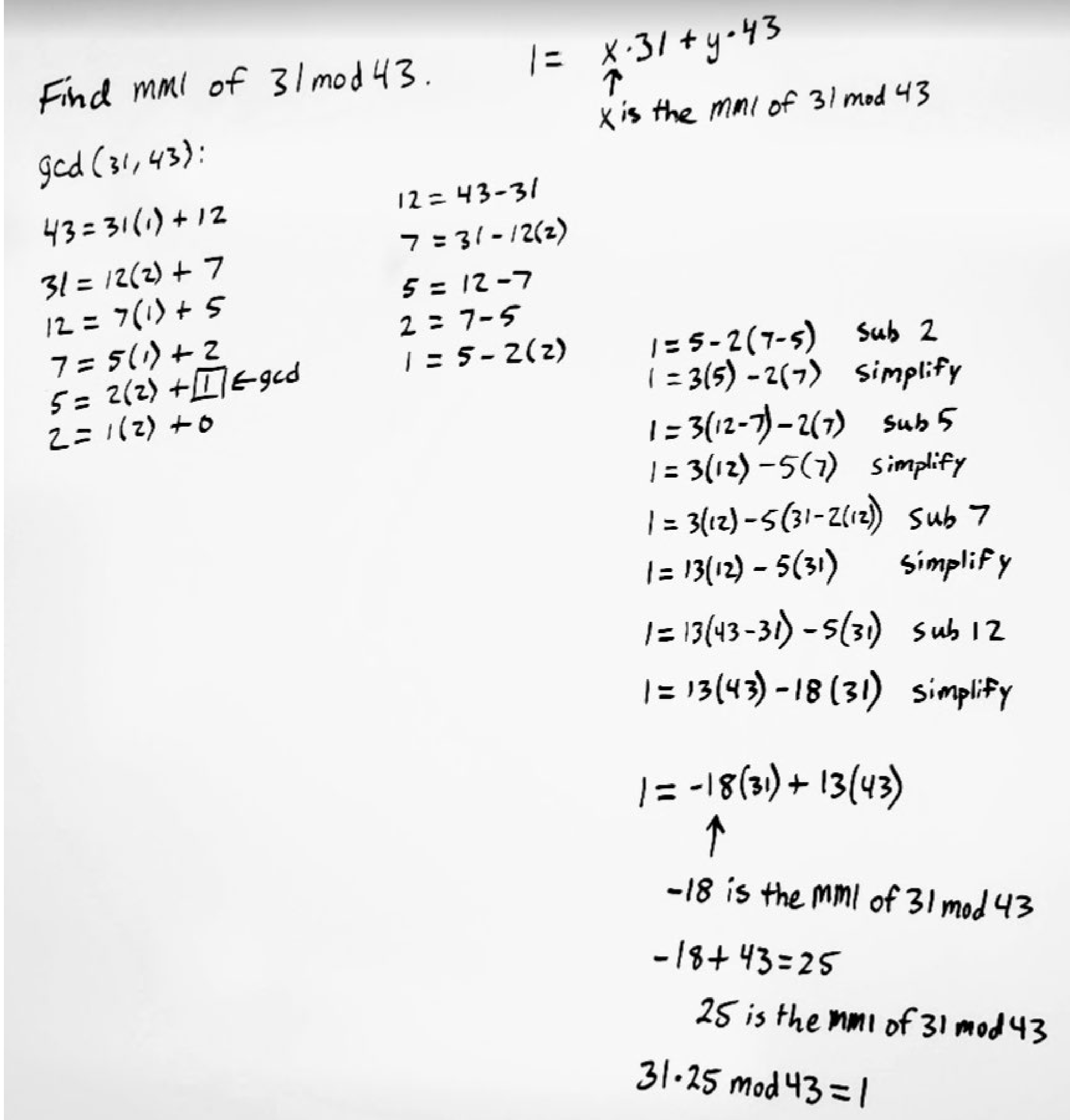
Find gcd(5,7)



Use the Extended Euclidean Algorithm to find the MMI of 31 mod 43.

1. Use Euclidean Algorithm to find gcd(31,43)
2. Use Extended Euclidean Algorithm to solve $1 = 31x + 43y$.
3. Now x is the MMI of 31 mod 43. (And y is the MMI of 43 mod 31)





Use the Extended Euclidean Algorithm to find the inverse of x mod n for each of the following:

x=35, n=48 11

x=25, n=84 37

$\gcd(x, n) = sx + tn$

If $\gcd(x, n) = 1$, then solve for s and t:

$$1 = sx + tn$$

s is the inverse of x mod n

Inverse of 35 mod 48:

gcd(35, 48):

$48 = 35 \cdot 1 + 13$

$35 = 13 \cdot 2 + 9$

$13 = 9 \cdot 1 + 4$

$9 = 4 \cdot 2 + 1$

Solve $1 = s \cdot 35 + t \cdot 48$

$13 = 48 - 1 \cdot 35$

$9 = 35 - 2 \cdot 13$

$4 = 13 - 1 \cdot 9$

$1 = 9 - 2 \cdot 4$

Substitute:

$1 = 9 - 2 \cdot (13 - 1 \cdot 9)$

$1 = 9 - 2 \cdot 13 + 2 \cdot 9$

$1 = 3 \cdot 9 - 2 \cdot 13$

$1 = 3 \cdot (35 - 2 \cdot 13) - 2 \cdot 13$

$1 = 3 \cdot 35 - 6 \cdot 13 - 2 \cdot 13$

$1 = 3 \cdot 35 - 8 \cdot 13$

$1 = 3 \cdot 35 - 8 \cdot (48 - 1 \cdot 35)$

$1 = 3 \cdot 35 - 8 \cdot 48 + 8 \cdot 35$

$1 = 11 \cdot 35 - 8 \cdot 48$

$s = 11$ $t = -8$

The inverse of 35 mod 48 is 11

Inverse of 25 mod 84:

gcd(25, 84)

$84 = 25 \cdot 3 + 9$

$25 = 9 \cdot 2 + 7$

$9 = 7 \cdot 1 + 2$

$7 = 2 \cdot 3 + 1$

$1 = s \cdot 25 + t \cdot 84$

$9 = 84 - 3 \cdot 25$

$7 = 25 - 2 \cdot 9$

$2 = 9 - 1 \cdot 7$

$1 = 7 - 2 \cdot 3$

$1 = 7 - 3 \cdot (9 - 1 \cdot 7)$

$1 = 7 - 3 \cdot 9 + 3 \cdot 7$

$1 = 4 \cdot 7 - 3 \cdot 9$

$1 = 4 \cdot (25 - 2 \cdot 9) - 3 \cdot 9$

$1 = 4 \cdot 25 - 8 \cdot 9 - 3 \cdot 9$

$1 = 4 \cdot 25 - 11 \cdot 9$

$1 = 4 \cdot 25 - 11(84 - 3 \cdot 25)$

$1 = 4 \cdot 25 - 11 \cdot 84 + 33 \cdot 25$

$1 = 37 \cdot 25 - 11 \cdot 84$

$s = 37$

37 is inverse of 25 mod 84

$25 \cdot 37 \mod 84 = 1$