$140x \equiv 56 \bmod 252$
There is solution exist because GCD(140, 252) = 28 that divides 56.
There are 28 number of solutions each separated by 252/28 or 9.

Solution:
$140x \equiv 56 \bmod 252$
$28.5x \equiv 28.2 \bmod 28.9$
$5x \equiv 2 \bmod 9$
$5.2x \equiv 2.2 \bmod 9$ (multiplied by 2 because 5 is relatively prime to 9 and has an inverse to 1 mod 9, $5.2 \equiv 10 \equiv 1 \bmod 9$)
$x \equiv 4 \bmod 9$
So the solutions are: 4, 13, 22, 31….

$14x \equiv 12 \mod 18$

There is solution exist because GCD(14, 18) = 2 that divides 12.

There are 2 number of solutions each separated by 18/2 or 9.

Solution:

$14x \equiv 12 \mod 18$

$2.7x \equiv 2.6 \mod 2.9$

$7x \equiv 6 \mod 9$

$7.4x \equiv 6.4 \mod 9$ (multiplied by 4 because 7 is relatively prime to 9 and has an inverse to 1 mod 9, $7.4 \equiv 28 \equiv 1 \mod 9$)

$x \equiv 6 \mod 9$

So the solutions are: 6, 15

Find all integers x such that $0 < x < 21$ and $4x + 9 \equiv 13 \bmod 21$.

Solution:

$4x + 9 \equiv 13 \bmod 21$

$16.4x + 16.9 \equiv 16.13 \bmod 21$ (Multiplied by 16)

$x + 16.9 \equiv 16.13 \bmod 21$ (Because $16.4 \equiv 1 \bmod 21$)

$x \equiv (13\text{-}9)16 \bmod 21$

$x \equiv 16.4 \bmod 21$

$x \equiv 64 \bmod 21$

$x \equiv 1 \bmod 21$

Find all integers x and y such that $0 < x < 21$, $0 < y < 21$,
$x + 2y \equiv 4 \bmod 21$ and $3x - y \equiv 10 \bmod 21$.

Solution:

We eliminate y in order to solve for x first.

$3x - y \equiv 10 \bmod 21$

$6x - 2y \equiv 20 \bmod 21$ (Multiplied by 2)…………..(I)

$x + 2y \equiv 4 \bmod 21$ ……………………..(II)

(I) + (II)

$7x \equiv 24 \bmod 21$

$7x \equiv 3 \bmod 21$

$7.3x \equiv 3.3 \bmod 21$ (Multiplied by 3)

$0\,x \equiv 9 \bmod 21$ (Because $7.3 \equiv 0 \bmod 21$)

But this is false. Therefore there is no solution exist for *x* and consequently no solutions for *y*.

Let a, b, c, m be four positive integers with $m > 1$. Assume that a has an inverse modulo m. Prove that if each of b and c is an inverse of a modulo m then we have: $b \equiv c \bmod m$.

Solution 1 Let us assume that each of b and c is an inverse of a modulo m.
Thus, we have

$$ab \equiv 1 \bmod m \text{ and } ac \equiv 1 \bmod m.$$

This implies

$$ab \equiv ac \bmod m.$$

That is:

$$a(b - c) \equiv 0 \bmod m.$$

In other words, m divides $a\,(b - c)$. Since a has an inverse modulo m, we have:

$$\mathrm{GCD}(a, m) = 1.$$

Therefore, m divides $b - c$, that is:

$$b \equiv c \bmod m.$$

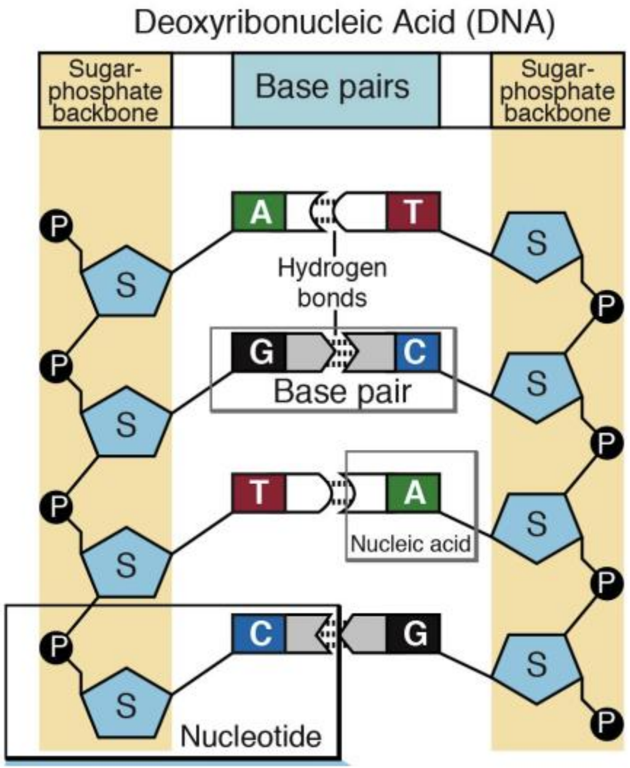
Find s, t, and gcd(a, b) such that $s\,a + t\,b$ = gcd(a, b) holds in the following cases:

1. $a = 2$ and $b = 3$,
2. $a = 11$ and $b = 12$,
3. $a = 12$ and $b = 15$,
4. $a = 3$ and $b = 7$,

Solution

1. -1 . 2 + 1 . 3 = 1 = gcd(a, b),
2. -1 . 11 + 1 . 12 = 1 = gcd(a, b),
3. -1 . 12 + 1 . 15 = 3 = gcd(a, b),
4. -2 . 3 + 1 . 7 = 1 = gcd(a, b),

DNA and genomes



A gene (DNA) can be abstractly represented as a string with elements from the alphabet $\Sigma = \{A, T, C, G\}$ e.g. AGTCTCCATGAAGCACGTTTAC...

Consider all *genes* (strings with $\Sigma = \{A, T, C, G\}$) of length 10.

1. How many genes begin with *AGT* ?
2. How many genes begin with *AG* and end with *T T* ?
3. How many genes begin with *AG* or end with *T T* ?
4. How many genes have exactly four *A*’s?

Solution 2

1. Each of the 7 remaining characters need to be chosen from 4, leading to 4^7 genes.
2. Each of the 6 remaining characters need to be chosen from 4, leading to 4^6 genes.
3. We apply the subtraction rule: $4^8 + 4^8 - 4^6$.
4. We apply the product rule:

• choose where to place the *A*’s:

• choose the 6 remaining charact $\binom{10}{4}$ rom *{T, C, G}*: 3^6

So the answer is: $\binom{10}{4} * 3^6$

RSA Algorithm Step by Step

1. Select two prime numbers p and q where $p \neq q$
2. Calculate n = p *n
3. Calculate f(n) = (p-1)(q-1)
4. Select e such that e is relatively prime to f(n), i.e. gcd(e, f(n))=1
5. Calculate $d = e^{-1}$ mod f(n) or ed = 1 mod f(n)

p = 13, q = 11
n = 13 * 11 = 143
f(n) = (13-1) (11-1) = 120
Let e=13 because gcd(13, 120) = 1
ed = 1 mod 120
13d = 1 mod 120 (gcd(13, 120)=1, there is only one solution)
13.37d = 37 mod 120 (13*37 = 480 = 1 mod 120)
d = 37 mod 120 = 37
Let plain text X = 13
Encryption: $E = X^e \bmod n = 13^{13} \bmod 143 = 52$
Decryption: $P = E^d \bmod n = 52^{37} \bmod 143 = 13$