8/28/2020 - Extended Euclidean Algorithm

Divisibility and Mod Definitions

We say that a | b, "b is divisible by a" if and only if, there exists some integer c such that b = ac.

So true statements are 6 | 18, 22 | 22, 173 | 0, 7 | 98, etc.

When I say that a ≡ b (mod n), this means that n | (a - b). (Intuitively, it's like saying that a and b yield the same remainder when divided by n.) Some true mod statements are:

13 ≡ 5 (mod 8)	because 8 | (13 - 5)
127 ≡ 7 (mod 10)	because 10 | (127 - 7)
127 ≡ 107 (mod 10)	because 10 | (127 - 107)
-5 ≡ 21 (mod 26)	because 26 | (-5 -21)
-5 ≡ 73 (mod 26)	because 26 | (-5 - 73)

In general if we know that a ≡ b (mod n), a is also equivalent to (b + any multiple of n) mod n. so, we can get different equivalent mods by adding or subtracting multiples of n.

21 mod 26, some equivalent mods are -5, 47, 73, 99, etc.

Affine Cipher

Encryption Function f(x) = (ax + b) mod 26, keys are a, and b.
a has to be from the set {1,3,5,7,9,11,15,17,19,21,23,25}
b is any int from 0 to 25.
312 possible keys.

Why are there only some possible values of a?

F(x) = (ax + b) mod 26

So, to do this backwards, we must solve for x in this equation. So usually when we invert functions, we swap x and y and then solve for y:

x ≡ (ay + b) mod 26

(x - b) ≡ ay mod 26

Now we are stuck because we are NOT allowed to divide under mod.

But for some values of a, we can multiply the equation through and solve for y anyway…

$(x - 19) \equiv 5y \bmod 26$ (for example a = 5, b = 19)

$21(x - 19) \equiv 21(5y) \bmod 26$

$21x - 399 \equiv 105y \bmod 26$

Since $105 \equiv 1 \bmod 26$, then we can say

$21x - 399 \equiv y \bmod 26$
$y = (21x - 399) \bmod 26$
$y = (21x + 17) \bmod 26$

Question: How do I find the magic value? Also, when does the magic value exist and when doesn't it exist?

General form of what we are trying to solve is

$ay \equiv (x - b) \bmod n$

Here I use n instead of 26 to allow for different alphabet sizes.

What we are really looking for is some value a', such that

$aa' \equiv 1 \pmod n$

Consider a situation where a and n have some common factor c, where $c > 1$.

This means there is some integer d such that $a = dc$, and there is some integer e such that $n = ec$

$(dc)a' \equiv 1 \pmod{ec}$

Let's consider the difference between dca' and 1.

dca' - 1, can NOT have a factor of c, because c is greater than 1, and we can pull it out of the first term but not the second. This isn't divisible by c.

But, ec IS divisible by c.

If two things are going to be equivalent mod ec, they must be equivalent mod c, but they aren't which means that the equation is impossible to satisfy.

$4x \equiv 1 \pmod{26}$

There is no value of x that satisfies this equation…the reason is that the LHS is always even and the right hand side is always odd…

$30x \equiv 1 \pmod{999}$

In this situation the LHS is always divisible by 3, but the RHS is never divisible by 3.

if $ax \equiv 1 \pmod{n}$, then if a and n share a common factor, say c,

Then the lefthand side is divisible by c, but the right hand side is NOT divisible by c, which means there is no possible integer value of x which makes the equation true.

What we've proven so far, AND THIS IS CRITICAL, is that we CAN NOT INVERT the affine cipher if there is a common factor greater than 1 between a and n, where n is the alphabet size.

Step 2: Can we find that magic value if a and n share no common factors?
If so, how?

Answer: Yes, the how is by using the Extended Euclidean Algorithm

Regular Euclidean Algorithm

Given positive integer values, a and b, find the greatest common divisor of a and b.

a = 105, b = 39, idea is to divide a by b, and get the quotient and remainder.

105 = 2 x 39 + 27
39 = 1 x 27 + 12
27 = 2 x 12 + **3, this is the gcd(105, 39) = 3, the last non-zero remainder in the**
12 = 4 x 3 **process.**

This means, for example, that there is no solution to

$39x \equiv 1 \pmod{105}$

Let's say we have values of a and b that don' share a common factor:

a = 143, b = 105

143 = 1 x 105 + 38 — 143 - 1 x 105 = 38
105 = 2 x 38 + 29 — 105 - 2 x 38 = 29
38 = 1 x 29 + 9 — 38 - 1 x 29 = 9
29 = 3 x 9 + 2 — 29 - 3 x 9 = 2
9 = 4 x 2 + **1, greatest common divisor is 1.**
2 = 2 x 1

Now, we are interested in finding the answer to

$105x \equiv 1 \pmod{143}$

9 - 4 x 2 = 1
9 - 4 (29 - 3 x 9) = 1
9 - 4 x 29 + 12 x 9 = 1
13 x 9 - 4 x 29 = 1
13(38 - 1 x 29) - 4 x 29 = 1
13 x 38 - 13 x 29 - 4 x 29 = 1
13 x 38 - 17 x 29 = 1
13 x 38 - 17(105 - 2 x 38) = 1
13 x 38 - 17 x 105 + 34 x 38 = 1
47 x 38 - 17 x 105 = 1

47(143 - 1 x 105) - 17 x 105 = 1
47 x 143 - 47 x 105 - 17 x 105 = 1
47 x 143 - 64 x 105 = 1

Now, let's take this equation mod 143:

47 x 143 - 64 x 105 ≡ 1 (mod 143)
-64 x 105 ≡ 1 (mod 143)

So, our magic value that we multiply 105 by to obtain 1 (mod 143) is -64. Normally, we are going to want to express this as a number in between 1 and 142, so let's add 143 to it to get our final answer: -64 + 143 = 79.

79 x 105 ≡ 1 (mod 143)

Goal of the Extended Euclidean Algorithm is to find the value a' such that

aa' ≡ 1 (mod n)

We can do this so long as gcd(a, n) = 1, using the process outlined above.

What we say is that

$105^{-1} \equiv 79 \pmod{143}$