Homework

Gerd Kukemilk
Bonus homework task

December 21, 2021

To find the modular multiplicative inverse we can use the extended Euclidean algorithm to find Bezout Identity $a * s + x * t = 1$. This will give us Bezout coefficients s and t where t_{i-1}, where remainder is 0 is the modular multiplicative inverse if a in the integer for which we look for the inverse and b is the modulus. This works only if the GCD of a and x is 1, meaning that they are relatively prime.

There are two ways to calculate extended Euclidean Algorithm, the so-called backwards substitution, and the iterative way. Backwards substitution is best suited for calculating by hand while the other suits very well for calculating EEA programmatically.

To start, we note that we will calculate the coefficients without backwards substitution. For this we can express the EEA equation as follow:

$$\begin{aligned} a_1 &= 1 * a_1 + 0 * a_2 \\ a_2 &= 0 * a_1 + 1 * a_2 \\ a_i &= s_i * a_1 + t_i * a_2 \\ a_{i+2} &= a_i - q_i * a_{i+1} = \\ (a_1 * s_i + a_2 * t_i) &- q_i(a_1 * s_i + 1 + a_2 * t_{i+1}) = \\ a_1(s_i - q_i * s_{i+1}) &+ a_2(t_i - q_i * t_{i+1}) \end{aligned}$$

Hence we get these equations that we use in our python code:

$$\begin{cases} s_1 = 1 \\ s_2 = 0 \\ s_{i+2} = s_i - q_i * s_{i+1}, i \geq 1 \end{cases} \qquad \begin{cases} t_1 = 0 \\ t_2 = 1 \\ t_{i+2} = t_i - q_i * t_{i+1}, i \geq 1 \end{cases}$$

An example calculation of EEA where a = 3 and b = 8 (a is the integer and b is the modulus for multiplicative inverse)

i	quotient	remainder	s_i	t_i
1		8	1	0
2		3	0	1
3	$8 \div 3 = 2$	$8 - 2 * 3 = 2$	$1 - 2 * 0 = 1$	$0 - 2 * 1 = -2$
4	$3 \div 2 = 1$	$3 - 1 * 2 = 1$	$0 - 1 * 1 = -1$	$1 - 1 * (-2) = 3$
5	$2 \div 1 = 2$	$2 - 2 * 1 = 0$	$1 - 2 * (-1) = 3$	$-2 * -2 * 3 = -8$