

How to compute the modular inverse of a matrix

I. STEP 1: GET MATRIX INVERSE

Refer to <http://mathworld.wolfram.com/MatrixInverse.html>

For a 2×2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

the matrix inverse is

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

For example¹

$$A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

the matrix inverse is

$$A^{-1} = \frac{1}{-121} \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix}$$

or equivalently,

$$A^{-1} = 121^{-1} \begin{pmatrix} -3 & 8 \\ 17 & -5 \end{pmatrix}$$

II. STEP 2: GET MODULAR INVERSE

Refer to <http://www.geocities.com/hjsmithh/Numbers/InvMod.html>

Now let's get 121^{-1} , the modular inverse of 121 mod 26. We can either use the PowerMod function in Mathematica (Ref: <http://mathworld.wolfram.com/ModularInverse.html>) or apply the following method. (Ref: <http://www.geocities.com/hjsmithh/Numbers/InvMod.html>)

Let $n = 26$, $x = 121$. First let's compute the extended greatest common divisor² of x and n .

$$(u, v, g) = \text{GCDe}(x, n);$$

You can use the online software at http://www.hostsrv.com/webmaa/app1/MSP/webm1010/extended_gcd.msp. Specifically, $a = x$, $b = n$ are used as input parameters. $u = s$, $v = t$, g – the greatest common divisor are the output results. In our example, the output is

$$1 = 121(-3 + 26k) + 26(14 - 121k)$$

for any integer k . If we take $k = 1$, then $g = 1$, $u = -3 + 26 = 23$, $v = 14 - 121 = -107$. Finally,

$$z = u \bmod n = 23 \bmod 26 = 23$$

¹This matrix is the same as the one in textbook [WS] at page 39, so that you can easily compare the results.

²Ref: <http://mathworld.wolfram.com/ExtendedGreatestCommonDivisor.html>.

III. STEP 3: PUT THINGS TOGETHER

Now we have

$$A^{-1} = 23 \times \begin{pmatrix} -3 & 8 \\ 17 & -5 \end{pmatrix} = \begin{pmatrix} -69 & 184 \\ 391 & -115 \end{pmatrix}$$

It is obvious that

$$184 \pmod{26} = 2 \tag{1}$$

$$391 \pmod{26} = 1 \tag{2}$$

$$-69 \pmod{26} = -17 \pmod{26} = 9 \tag{3}$$

$$-115 \pmod{26} = -11 \pmod{26} = 15 \tag{4}$$

$$\tag{5}$$

(Refer: Section 4.2 of textbook [WS], particularly page 110.) Finally, we have

$$A^{-1} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$