Le modulo

Trouver l'inverse modulaire

Prenons l'exemple de $9\mod80$

On peut écrire 9 et 80 dans le tableau suivant

R	9 (u)	80 (v)	Q
9	1	0	
80	0	1	

Ensuite on peut effectuer la division euclidienne des deux dernières lignes soit $9 \div 80$ et mettre le reste dans la première colonne et le quotient dans la dernière

R	9 (u)	80 (v)	Q
9	1	0	
80	0	1	
9			0

Maintenant on va multiplier chaque avant-dernière case moins chaque dernière case des deux dernières colonnes avec le quotient que l'on a trouvé

R	9 (u)	80 (v)	Q
9	1	0	
80	0	1	
9	$1-0*0=1$	$0-1*0=0$	0

Enfin on peut recommencer de nouveau depuis l'étape 2 jusqu'a arriver à un reste qui vaut 1. Si il n'y a pas de 1 et que l'on passe directement à 0, alors il n'y a pas d'inverse modulaire.

R	9 (u)	80 (v)	Q
9	1	0	
80	0	1	
9	$1-0*0=1$	$0-1*0=0$	0

R	9 (u)	80 (v)	Q
8	-8	1	8
1	$1-(-8)*1=9$	$0-1*1=-1$	1

Maintenant on peut prendre le résultat de la colonne u et :

- si celui-ci est plus grand que 80 on fait $80 - u$
- si celui-ci est plus petit que 0 on fait $80 + u$
- si celui-ci est entre les deux on le garde tel quel

Donc ici 9 est plus grand que 0 et plus petit que 80 donc le résultat est **9**

Faire le modulo d'un exposant négatif

Pour faire le $(690^{-6}) \mod 11$ on commence par faire l'inverse modulaire de 690 ce qui nous donne 7

Ensuite on fait $7^6 \mod 11$ ce qui nous donne donc 4 et c'est notre réponse finale.

Revision #1
Created 27 April 2023 04:28:56 by SnowCode
Updated 24 May 2023 11:07:21 by SnowCode