Inverse modulaire

Rappel:

En arithmétique modulaire, l'inverse modulaire d'un entier relatif ***a*** pour la multiplication modulo ***n*** est un entier ***u*** satisfaisant l'équation :

$$a \times u \equiv 1 \ (mod\, n) \ avec \ PGCD(a, n) = 1$$

D'après la définition ci-dessus, ***u*** est un inverse de ***a*** modulo ***n*** s'il existe un entier ***v*** tel que

$$a \times u + n \times v = 1$$

Algorithme d'Euclide étendu appliqué rapidement:

Prenons un exemple illustratif de ma méthode, et calculons $8^{-1}\%27 = ?$:

1. $27\%8 = 3$
2. $8\%3 = 2$
3. $3\%2 = 1$

On arrête lorsqu'on arrive à « 1 ».

On va chercher combien de « 8 » il y en est caché.

"3" $= 27\%8 = -\frac{27}{8} = -3$ (c'est une valeur formelle c-à-d le coefficient multiplié par 8 est -3).

"2" $= 8\%3 = 1 - (\frac{8}{3}) * (-3) = 7$ (-3 est la valeur formelle de 3 déjà calculée et 7 est la valeur formelle de 2)

Remplaçant ces valeurs formelles dans l'équation 3 :

$-3 - (\frac{3}{2}) * 7 = -3 - 7 = -10$, en ajoutant la base 27 on obtient → -10+27=17.

(-10 = 17 dans l'anneau Z /nZ pour n=27).

Vérification : $8 \times 17 = 136 \,\%\, 27 = 1.$

Procédure :

On va nommer les opérandes par le gauche et le droit. On calcule toujours le gauche modulo le droit en commençant par la base modulo la cible (ici la base est 27 et la cible est 8).

On répète cette étape jusqu'à obtenir une valeur unitaire.

Après on commence à calculer ce que j'appelle les valeurs formelles, ceux sont les coefficients multipliés par la cible.

La conclusion de la méthode dit que si le nombre qui contient une valeur de la cible est à gauche alors sa valeur formelle est égale à ce coefficient, s'il est à droite sa valeur formelle égale au coefficient multiplié par le moins du rapport gauche/droite.

L'inverse modulaire est la différence entre la valeur formelle du gauche et la valeur formelle du droit multipliée par le rapport gauche/droit de la dernière équation.

Prenons un autre exemple illustratif, calculons $7^{-1}\%39 = ?$:

On commence par les itérations jusqu'à obtenir une valeur unitaire

1. $39\%7 = 4$
2. $7\%4 = 3$
3. $4\%3 = 1$

"4" $= 39\%7 = -\frac{39}{7} = -5$, puisque 7 est à gauche et toujours la base ne contient aucune valeur du cible alors la valeur formelle de 4 est le moins du rapport gauche/droit multiplié par 1 (car le coefficient multiplié par la cible est 1).

Remarquons qu'on ne peut pas calculer la valeur formelle de 3 avant celle de 4.

"3" $= 1 - \left(\frac{7}{4}\right) \times (-5) = 6$

Enfin, $7^{-1}\ \%39 = -5 - \left(\frac{4}{3}\right) \times 6 = -5 - 6 = -11 = 28$

Vérification :$7 \times 28 = 196\%39 = 1$!! $c.q.f.d$

Alors, allons maintenant au clavier :

```
public class My_method{
        private long a;
        private long n;
        private long b1;
        private long b2;
        public boolean hasInverse=true;
        public My_method(long a,long n)
        {
        this.a=(a>n) ? a%n:a;
        this.n=n;
        function();
        }
        public void function()
        {long x,y;
        long p=n;
                    if(n%a==1)
                    b2=n-n/a;
              else{
              b1=-n/a;
              y=a;
```

```
        a=n%a;
        n=y;
        b2=1-(n/a)*b1;
        while(n%a!=1 && n%a!=0)
        {
                y=a;
                a=n%a;
                n=y;
                x=b1-(n/a)*b2;
                b1=b2;
                b2=x;
        }
        if(n%a==0)
                hasInverse=false;
        else while(b2<0)
                b2+=p;
        }
}
public long get()
{
        return b2;
}
}
```