Calcul dans les anneaux et corps finis. .

Michaël Quisquater (Maître de Conférences, UVSQ)

Inverse d'une classe de congruence dans $\mathbb{Z}_n^*$

Les classes inversibles de $\mathbb{Z}_n$ possèdent la caractérisation suivante :

Théorème

Soit n un naturel supérieur ou égal à 2. $[a + n\mathbb{Z}]$ *(avec* $a \in \mathbb{Z}$*) est inversible pour la multiplication modulo n si et seulement si* $pgcd(a, n) = 1$.

Calcul de l'inverse dans $\mathbb{Z}_n^*$

Calculer l'inverse d'une classe de congruence $[a + n\mathbb{Z}]$ revient calculer $b \in \mathbb{Z}$ tel que

$$[a + n\mathbb{Z}] \cdot [b + n\mathbb{Z}] = [1 + n\mathbb{Z}] .$$

ou encore

$$n \cdot k + a \cdot b = 1 ,$$

pour un certain $k \in \mathbb{Z}$.

$\Rightarrow$ relation de Bezout.

Calcul de l'inverse dans $\mathbb{Z}_n^*$

Donnons à présent un exemple de calcul d'inverse d'une classe de congruence.

Cherchons l'inverse de la classe $\overline{3} \in \mathbb{Z}_{40}$.

La classe $\overline{3}$ est inversible. En effet, $pgcd(3, 40) = 1$ (voir ci-dessous)

Calculons un représentant de la classe inverse de $\overline{3}$. Pour ce faire, calculons les coefficients de Bezout $a, b \in \mathbb{N}$ tels que $40 \cdot a + 3 \cdot b = 1$.

L'algorithme d'Euclide étendu donne les valeurs suivantes :

Calcul de l'inverse d'une classe de congruence (suite)

k	0	1	2	3
r_k	40	3	1	0
q_k	-	13	3	-
x_k	1	0	1	-
y_k	0	1	-13	-

Nous déduisons que $a = 1$ et $b = -13$.

On vérifie que l'on a bien $40 \cdot 1 + 3 \cdot (-13) = 1$.

Un représentant de la classe inverse de $\overline{3}$ est donc -13.

Le représentant minimal de la classe $\overline{-13}$ de $\mathbb{Z}_{40}$ est 27. En effet, $[-13 + 40\mathbb{Z}] = [27 + 40\mathbb{Z}]$. Par conséquent,

$$\overline{3}^{-1} = \overline{-13} = \overline{27}\,.$$

Calcul d'inverse dans $(\mathbb{F}_p[X]/(P(X))^*$

Le calcul de l'inverse d'une classe inversible $[S(X) + (P(X))]$ avec $(pgcd(S(X), P(X)) = 1)$ se fait de la façon similaire à celle dans les entiers.

Il suffit de calculer le coefficient $B(X)$ de Bezout de l'équation :

$$A(X) \cdot P(X) + B(X) \cdot S(X) = 1\,.$$

Calcul d'inverse dans $\mathbb{F}_{p^n}$

Remarques :

- Ce coefficient se trouve via l'algorithme d'Euclide étendu sur les polynômes.
- Le dernier reste non-nul de la séquence de division Euclidienne peut ne pas être 1 mais une valeur non-nulle de $\mathbb{F}_p$. Dans ce cas, il faut multiplier l'ensemble de l'équation par l'inverse de ce nombre pour retomber sur la forme canonique.
- Si $P(X)$ est un polynôme irréductible de $\mathbb{F}_p[X]$ de degré n alors toute classe $[S(X) + (P(X))]$ non-nulle est inversible et $\mathbb{F}_p[X]/(P(X)) \cong \mathbb{F}_{p^n}$.

Existence de racine carrée : introduction

Soit p un nombre premier impair.

Un problème très important est la résolution de l'équation :

$$x^2 \equiv a \bmod p\,.$$

Cette équation n'a pas toujours de solution dans $\mathbb{Z}_p^*$ et quand elle a une solution x_0, elle en a deux i.e. $(x_0, -x_0)$.

Existence de racine carrée : introduction

- Supposons que a ne soit pas un multiple de p. a est dit résidu quadratique modulo p si l'équation précédente possède une (et donc deux) solution et non-résidu quadratique modulo p sinon.
- L'existence de la solution de cette équation dépend de la valeur du symbole de Legendre de a.

Caractère "carré" modulo p d'un nombre : symbole de Legendre

Soit p un premier impair et a un entier. Le symbole de Legendre, noté $\left(\frac{a}{p}\right)$, est défini par :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \text{ est un multiple de } p \\ 1 & \text{si } a \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } a \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

On peut facilement montrer que :

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p\,.$$

Caractère "carré" modulo p d'un nombre : symbole de Legendre

Soit p un premier impair et a un entier. Le symbole de Legendre, noté $\left(\frac{a}{p}\right)$, possède les propriétés suivantes :

1. $\left(\frac{a}{p}\right)$ ne dépend que de la classe de congruence modulo p de a.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. si b n'est pas un multiple de p, $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.
4. $\left(\frac{1}{p}\right) = 1$ et $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
5. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
6. (réciprocité quadratique) : si p et q sont des premiers impairs, $\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$.

Calcul d'inverse
Existence de racine carrée
Théorème des restes chinois
Librairies des grands nombres.
Symbole de Legendre
Symbole de Jacobi

Caractère "carré" modulo p d'un nombre : symbole de Legendre

Soit a et b des naturels impairs, alors :

$$(-1)^{(a^2-1)/8} = \begin{cases} 1 & \text{si } a \equiv \pm 1 \bmod 8 \\ -1 & \text{si } a \equiv \pm 3 \bmod 8 \end{cases}$$

$$(-1)^{(a-1)(b-1)/4} = \begin{cases} -1 & \text{si } a \equiv b \equiv 3 \bmod 4 \\ 1 & \text{sinon} \end{cases}$$

Application au calcul du symbole de Legendre

Exemple :

Soit $a = 2025$ et $p = 211$. Comme p est premier, calculer $\left(\frac{2025}{211}\right)$ a un sens.

Réduction : Comme $2025 = 9 \cdot 211 + 126$, $\left(\frac{2025}{211}\right) = \left(\frac{126}{211}\right)$.
Factorisation : Aussi, $126 = 2 \cdot 3^2 \cdot 7$. Donc,

$$\left(\frac{126}{211}\right) = \left(\frac{2}{211}\right) \cdot \left(\frac{7}{211}\right) = (-1)^{(211^2-1)/8} \cdot \left(\frac{7}{211}\right).$$

Aussi, $(-1)^{(211^2-1)/8} = -1$ car $211 = 3 \bmod 8$.
Réciprocité : Comme 7 et 211 sont des premiers impairs, on peut utiliser la réciprocité quadratique pour calculer $\left(\frac{7}{211}\right)$:

$$\left(\frac{7}{211}\right) = (-1) \cdot \left(\frac{211}{7}\right) = (-1) \cdot \left(\frac{1}{7}\right) = -1.$$

Application au calcul du symbole de Legendre (suite)

Conclusion : $\left(\frac{2025}{211}\right) = (-1) \cdot (-1) = 1$. Par conséquent, 2025 est un résidu quadratique modulo 211.

Remarque :

Il a fallu factoriser 126 ce qui peut s'avérer compliqué pour de plus grands nombres $\Rightarrow$ Symbole de Jacobi.

Symbole de Jacobi

L'idée est de généraliser le symbole de Legendre aux nombres impairs tout en conservant certaines propriétés de celui-ci.

Soit $n > 1$ un naturel impair et a un entier. Considérons la factorisation de $n = \prod_{i \in I} p_i^{\alpha_i}$ avec $\alpha_i \in \mathbb{N}_0$ pour $i \in I$.

Le **symbole de Jacobi**, noté $\left(\frac{a}{n}\right)$, est défini par :

$$\left(\frac{a}{n}\right) = \prod_{i \in I} \left(\frac{a}{p_i}\right)^{\alpha_i}.$$

Remarque : notons que $\left(\frac{a}{n}\right) = 1$ pour n composé n'implique pas que a soit résidu quadratique modulo n. En effet, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ alors qu'il n'existe pas de nombre $x \in \mathbb{Z}$ tel que $x^2 = 2 \bmod 15$.

Symbole de Jacobi

Soit n un naturel impair et a un entier. Le symbole de Legendre, noté $\left(\frac{a}{p}\right)$, possède les propriétés suivantes :

1. $\left(\frac{a}{n}\right)$ ne dépend que de la classe de congruence modulo n de a.
2. $\left(\frac{1}{n}\right) = 1$ et $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
3. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.
4. (réciprocité quadratique) : si de plus a naturel est impair,

$$\left(\frac{a}{n}\right) = (-1)^{(a-1)(n-1)/4} \left(\frac{n}{a}\right).$$

Application au calcul du symbole de Legendre

Exemple :

Soit $a = 2025$ et $p = 211$. On souhaite calculer le symbole de Legendre $\left(\frac{2025}{211}\right)$ (p est premier).

Application au calcul du symbole de Legendre

Réduction : Comme $2025 = 9 \cdot 211 + 126$, $\left(\frac{2025}{211}\right) = \left(\frac{126}{211}\right)$.
Extraction des puissances des 2 : Aussi, $126 = 2 \cdot 63$. Donc,

$$\left(\frac{126}{211}\right) = \left(\frac{2}{211}\right) \cdot \left(\frac{63}{211}\right) = (-1)^{(211^2-1)/8} \cdot \left(\frac{63}{211}\right).$$

Aussi, $(-1)^{(211^2-1)/8} = -1$ car $211 = 3 \bmod 8$.
Réciprocité : Comme 63 et 211 sont des naturels impairs, on peut utiliser la réciprocité quadratique pour calculer $\left(\frac{63}{211}\right)$.
Aussi, $211 = 3 \bmod 4$ et $63 = 3 \bmod 4$.

$$\left(\frac{63}{211}\right) = (-1)\left(\frac{211}{63}\right).$$

Application au calcul du symbole de Legendre

Réduction : $\left(\frac{211}{63}\right) = \left(\frac{22}{63}\right)$ car $211 = 3 \cdot 63 + 22$.
Extraction des puissances des 2 : Aussi, $22 = 2 \cdot 11$. Aussi $(-1)^{(63^2-1)/8} = 1$ car $63 = -1 \bmod 8$. Donc,

$$\left(\frac{22}{63}\right) = \left(\frac{11}{63}\right)$$

Réciprocité : Comme 11 et 63 sont des naturels impairs, on peut utiliser la réciprocité quadratique pour calculer $\left(\frac{11}{63}\right)$:

$$\left(\frac{11}{63}\right) = (-1) \cdot \left(\frac{63}{11}\right) .$$

Application au calcul du symbole de Legendre

Réduction : $\left(\frac{63}{11}\right) = \left(\frac{8}{11}\right)$ car $63 = 5 \cdot 11 + 8$.
Extraction des puissances des 2 : Aussi, $8 = 2^3$. Donc,

$$\left(\frac{8}{11}\right) = (-1)^3 = -1 .$$

Conclusion :

$$\left(\frac{2025}{211}\right) = (-1) \cdot (-1) \cdot (-1) \cdot (-1) = 1 .$$

Utilisation algorithmique du théorème des restes chinois

Le théorème des restes chinois établit un isomorphisme d'anneau entre un anneau quotient et un le produit cartésien d'anneaux quotients ("plus petits").
Lorsque le théorme des restes chinois est d'application, il généralement beaucoup moins coûteux de d'abord appliquer l'isomorphisme, effectuer les opérations dans le produit cartésien d'anneaux quotients et ensuite revenir dans l'anneau quotient initial.

Exemple : Calcul du RSA. $\mathbb{Z}_{p\cdot q} \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Calculer $m^d \bmod n$ revient donc essentiellement à calculer $m^{d \bmod p-1} \bmod p$ et $m^{d \bmod q-1} \bmod q$. $\Rightarrow$ gain d'un facteur 4.

Librairies des grands nombres

En pratique, un ordinateur ne gère que des nombres de 32 ou 64 bits la plupart du temps → librairies des grands nombres

Librairies de grands nombres

- (C/C++) : `http://gmplib.org/`
- Java : BigInteger `http://java.sun.com/j2se/1.4.2/docs/api/java/math/BigInteger.html`
- Python : natif `www.python.org/`
- PHP :
  - BC Math : `http://www.php.net/manual/en/book.bc.php`
  - GMP : `http://www.php.net/manual/en/book.gmp.php`