Licence MHT 633

Cryptologie

Corrigé de la feuille d'exercices n° 1.

Arithmétique

1 Tout nombre rationnel est le quotient de deux nombres entiers premiers entre eux. Soit donc $a = p/q$ avec $(p, q) = 1$. Si $18a$ est entier c'est que q divise $18p$. Par le Lemme de Gauss:

Lemme 1 *a, b, c étant des nombres entiers, si a divise bc et si a est premier avec b alors a divise c.*

comme $(p, q) = 1$ on peut conclure que q divise 18. De même q divise 25. Finalement, si q divise 18 et 25 alors q divise leur pgcd qui vaut 1, donc $q = 1$, ce qui prouve que a est entier.

2 Rappelons la démonstration classique du fait qu'il y a une infinité de nombres premiers: si $p_1, \ldots, p_n$ sont premiers alors $N = p_1 \ldots p_n + 1$ est un entier au moins égal à 2, n'est divisible par aucun des p_i, donc possède un diviseur premier qui n'est pas dans l'ensemble $\{p_1, \ldots, p_n\}$.

Supposons maintenant qu'en outre $p_i \equiv -1 \mod 4$ pour tout $i = 1, \ldots, n$. Notons qu'ils sont nécessairement impairs. L'idée est de construire un N qui soit premier aux p_i et qui vérifie également $N \equiv -1 \mod 4$. En effet N possède alors au moins un diviseur premier égal à -1 mod 4 (sinon tous ses diviseurs premiers seraient égaux à $1 \mod 4$ et donc leur produit aussi). On a $p_1 \ldots p_n \equiv (-1)^n \mod 4$ donc on peut prendre:

$$N = \begin{cases} p_1 \ldots p_n + 2 & \text{si } n \text{ est pair} \\ p_1 \ldots p_n + 4 & \text{si } n \text{ est impair} \end{cases}$$

Remarquons qu'on utilise ici fondamentalement le fait que les congruences modulo un entier se multiplient!

3 Comme $n^2 - 1 = (n-1)(n+1)$, il est nécessaire que $n - 1 = \pm 1$ ou $n + 1 = \pm 1$ ce qui conduit aux cas à examiner: $n = 0, 2, -2$. Dans ces cas $n^2 - 1$ vaut respectivement $1, 3, 3$. Rappelons que le nombre 1 n'est pas premier..

4 Si $4p+7q = pq$ alors p divise $7q$ et q divise $4p$. Ca nous arrangerait que p et q soient premiers entre eux pour conclure que p divise 4 et q divise 7 par le lemme de Gauss. On se ramène à ce cas en posant $(p, q) = d$ et $p = dp'$, $q = dq'$ avec $(p', q') = 1$. La condition $4p + 7q = pq$ devient $4p' + 7q' = p'q'd$ et le même raisonnement montre que p' divise 4 et q' divise 7. Il reste à examiner tous les cas.

5 Soit a et b des entiers distincts.

(a) $a^2 - b^2 = (a - b)(a + b)$

(b) $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$

(c) $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$

(d) $a^{2n+1} + b^{2n+1} = (a+b)(a^{n-1} - a^{n-2}b + \cdots + b^{n-1})$ (on a remplacé b par $-b$ dans la formule précédence).

(e) On applique successivement (a) (b) (c):

$$\begin{aligned}5^{10}-2^{10} &= (5^5-2^5)(5^5+2^5)\\ &= (5-2)(5^4+2\cdot 5^3+2^2\cdot 5^2+2^3\cdot 5+2^4)(5^5+2^5)\\ &= (5-2)(5^4+2\cdot 5^3+2^2\cdot 5^2+2^3\cdot 5+2^4)(5+2)(5^4-2\cdot 5^3+2^2\cdot 5^2-2^3\cdot 5+2^4)\\ &= 3\cdot 1031\cdot 7\cdot 451\\ &= 3\cdot 1031\cdot 7\cdot 11\cdot 41\end{aligned}$$

6

1. Vous verrez plus tard des critères d'irréductibilité plus efficaces que de vérifier qu'aucun nombre premier plus petit que $\sqrt{N}$ ne divise N.

2. On factorise en utilisant les identités de l'ex 5:

$$\begin{aligned}2^{32}-1 &= (2^{16}-1)(2^{16}+1)\\ &= (2^8-1)(2^8+1)(2^{16}+1)\\ &= (2^4-1)(2^4+1)(2^8+1)(2^{16}+1)\\ &= (2^4-1)(2^4+1)(2^8+1)(2^{16}+1)\\ &= (2^2-1)(2^2+1)(2^4+1)(2^8+1)(2^{16}+1)\\ &= (2-1)(2+1)(2^2+1)(2^4+1)(2^8+1)(2^{16}+1)\\ &= 1\cdot 3\cdot 5\cdot 17\cdot 257\cdot 65537\end{aligned}$$

3. Si $k=2^n b$ avec b impair, alors l'identité $y^b+1=(y+1)(y^{b-1}-y^{b-2}+\cdots+1)$ montre que $2^{2^n}+1$ divise 2^k+1. Si $b\neq 1$ c'est un diviseur non trivial.

4. (a) $641=2^9+2^7+1$ donc $2^7\cdot 5=2^7(2^2+1)=2^9+2^7=641-1=-1 \mod 641$.

   (b) En effet $5^4=625=-16 \mod 641$.

   Comme $32=4\cdot 7+4$, on a

$$\begin{aligned}2^{32}+1 &= (2^7)^5\cdot(-5^4)+1 \mod 641\\ &= -(2^7\cdot 5)^4+1 \mod 641\\ &= -(-1)^4+1=0 \mod 641\end{aligned}$$

   donc 641 divise $2^{32}+1$.

7 Comme $10^k=0 \mod 4$ pour $k\geq 2$, un nombre N d'écriture décimale $a_n\ldots a_1a_0$ est égal à $a_1a_0 \mod 4$.

8 L'algorithme d'Euclide appliqué à un couple de nombres entiers (a,b) calcule le pgcd de a et b. On effectue les divisions euclidiennes successives en posant $r_0=a$, $r_1=b$:

$$\begin{aligned}r_0 &= r_1q_1+r_2\\ r_1 &= r_2q_2+r_3\\ &\cdots\\ r_{i-1} &= r_iq_i+r_{i+1}\\ &\cdots\end{aligned}$$

et le pgcd de a et b est le dernier reste non nul. Une relation de Bezout est une équation de la forme $d = au + bv$ où $d = (a, b)$. Rappelons que a est inversible modulo b, c'est-à-dire $a \in (\mathbb{Z}/b\mathbb{Z})^*$ si et seulement si $(a, b) = 1$. Une relation de Bezout $au + bv = 1$ montre que $au = 1 \mod b$ et donc $a^{-1} = u$ dans $(\mathbb{Z}/b\mathbb{Z})^*$. De même $b^{-1} = v \mod a$.

On peut extraire une relation de Bezout de l'algorithme d'Euclide en "remontant" les équations données par les divisions euclidiennes successives mais il est plus efficace d'appliquer l'algorithme dit d'Euclide étendu: celui-ci calcule en même temps que la suite des q_i et des r_i, deux suites u_i et v_i vérifiant les relations de récurrence:

$$u_{i+1} = u_{i-1} - q_i u_i$$
$$v_{i+1} = v_{i-1} - q_i v_i$$

et les conditions initiales:

$$\begin{pmatrix} u_0 & v_0 \\ u_1 & v_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Le dernier couple (u_i, v_i) calculé donne une relation de Bezout entre a et b. L'intérêt de cette algorithme réside dans le fait que son exécution ne nécessite pas de garder en mémoire tous les (q_i, r_i, u_i, v_i) mais seulement les deux précédents.

Exemple: $a = 34$, $b = 21$.

i	r_i	q_i	u_i	v_i
0	34		1	0
1	21	1	0	1
2	13	1	1	−1
3	8	1	−1	2
4	5	1	2	−3
5	3	1	−3	5
6	2	1	5	−8
7	1	2	−8	13
8	0			

On trouve la relation de Bezout $(-8) \cdot 34 + 13 \cdot 21 = 1$; 34 est inversible modulo 21 avec $34^{-1} = -8 \mod 21$; 21 est inversible modulo 34 avec $21^{-1} = 13 \mod 34$.

Preuve de l'algorithme d'Euclide étendu: on peut exprimer la division euclidienne de r_{i-1} par r_i par la relation matricielle:

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}$$

ce qui conduit par itération à:

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}.$$

En posant

$$\begin{pmatrix} u_i & v_i \\ s_i & t_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} u_0 & v_0 \\ u_1 & v_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

on a

$$\begin{pmatrix} u_i & v_i \\ s_i & t_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} u_{i-1} & v_{i-1} \\ s_{i-1} & t_{i-1} \end{pmatrix}.$$

On obtient alors les relations

$$\begin{cases} s_{i-1} & = u_i \\ t_{i-1} & = v_i \\ u_{i+1} & = u_{i-1} - q_i u_i \\ v_{i+1} & = v_{i-1} - q_i v_i \end{cases}$$

À la dernière étape, on a avec $d = (a, b)$:

$$\begin{pmatrix} r_t \\ d \end{pmatrix} = \begin{pmatrix} u_t & v_t \\ u_{t+1} & v_{t+1} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

d'où la relation de Bezout $d = u_{t+1}a + v_{t+1}b$.

9 $32x + 10y = 6$ ssi $16x + 5y = 3$. Comme $(16, 5) = 1$ et que $16 - 3 \cdot 5 = 1$ on a $16^{-1} = 1 \mod 5$ et $5^{-1} = -3 \mod 16$. On a $16x = 3 \mod 5$ ssi $x = 3 \mod 5$ et $5y = 3 \mod 16$ ssi $y = -9 \mod 16$. En remplaçant $x = 3 + 5x'$ et $y = -9 + 16y'$ on trouve que $16x + 5y = 3$ ssi $x' = -y'$. finalement les solutions (x, y) sont tous les $(3 + 5q, -9 - 16q)$ avec $q \in \mathbb{Z}$.

10 On doit donc résoudre $12J + 31M = 442$. Par l'algorithme d'Euclide étendu on trouve $13 \cdot 12 - 5 \cdot 31 = 1$. Comme dans l'exercice précédent on a $J = 11 \mod 31$ et $M = 10 \mod 12$. Comme $1 \leq M \leq 12$ la seule solution est $M = 10$ et donc $J = 11$.

11

(a) $(3, 37) = 1$ donc $3 \in (\mathbb{Z}/37\mathbb{Z})^*$; une relation de Bezout $37 - 3 \cdot 12 = 1$ montre que $3^{-1} = 12 \mod 37$.

(b) $(4, 14) = 2 > 1$ donc 4 n'est pas inversible modulo 14.

12

(a) Comme $(2, 21) = 1$, 2 est inversible modulo 21. On a donc $2x = 37 \mod 21 = 16 \mod 21$ ssi $x = 8 \mod 21$.

(b) $5x = 15 \mod 25$ ssi $x = 3 \mod 5$ ssi $x = 3, 8, 13, 18, 23 \mod 25$.

(c) $3x = 7 \mod 18$ n'a pas de solution car 3 ne divise pas 7.

Tout d'abord, il faut remarquer que dans un anneau A quelconque, si a est un élément inversible de A, l'équation $ax = b$ est équivalente à $x = a^{-1}b$. Ainsi, dans le cas particulier $A = \mathbb{Z}/n\mathbb{Z}$ on a : si $(a, n) = 1$, $ax = b \mod n$ ssi $x = a^{-1}b \mod n$.

Si $(a, n) = d > 1$, on va se ramener au cas précédent en factorisant d dans a et n. Soit donc $a = da'$ et $n = dn'$. L'équation devient $da'x = b \mod dn'$. Puisque d divise $da'x$ et dn' il doit aussi diviser b. Écrivons $b = db'$; on a $da'x = db' \mod dn'$. En remontant dans $\mathbb{Z}$, on obtient $da'x = db' \mod dn'$ ssi il existe $q \in \mathbb{Z}$ tel que $da'x = db' + qdn'$ ssi il existe $q \in \mathbb{Z}$ tel que $a'x = b' + qn'$ ssi $a'x = b' \mod n'$. En résumé on voit qu'on a divisé toute l'équation par d *y compris le module* n. Comme maintenant $(a', n') = 1$, on peut résoudre comme précédemment en $x = a'^{-1}b' \mod n'$. On a alors plusieurs solutions modulo n. En effet, si α est un représentant de $a'^{-1}b' \mod n'$, les solutions modulo n sont les $\alpha + kn' \mod n$ avec $k = 0, 1, \ldots, d - 1$ et il y en a d. En résumé on a:

Lemme 2 *Résolution de* $ax = b \mod n$*:*

1. *Si* $(a, b) = 1$ *une solution unique* $x = a^{-1}b \mod n$.
2. *Si* $(a, b) = d > 1$ *et* d *ne divise pas* b*, pas de solution*

3. *Si $(a,b) = d > 1$ et d divise b il y a d solutions: avec $a = a'd$, $b = b'd$, $n = n'd$, avec $\alpha = b'a'^{-1} \mod n'$, ce sont les $x = \alpha + kn' \mod n$ avec $k \in \{0, \dots, d-1\}$.*

13 On rappelle que a est un inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $(a,n) = 1$. On a donc: $(\mathbb{Z}/4\mathbb{Z})^* = \{1,3\}$, $(\mathbb{Z}/6\mathbb{Z})^* = \{1,3,5\}$, $(\mathbb{Z}/12\mathbb{Z})^* = \{1,5,7,11\}$. Si p est premier, les inversibles de $\mathbb{Z}/p^2\mathbb{Z}$ sont les $a \mod p^2$ tels que p ne divise pas a. Il y en a donc $p^2 - p$.

14

Sur un anneau A, les transformations élémentaires suivantes conduisent à un système linéaire équivalent:

1. Échange de deux lignes
2. Multiplication d'une ligne par un élément inversible de A
3. Remplacement d'une ligne L_i par $L_i + aL_j$ avec $a \in A$.

Le premier système se résoud très facilement:

$$\left\{ \begin{array}{lll} x+y & = 6 & \mod 11 \\ 2x-y & = 8 & \mod 11 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lll} y & = 6-x & \mod 11 \\ 3x-6 & = 8 & \mod 11 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lll} y & = 9 & \mod 11 \\ x & = 8 & \mod 11 \end{array} \right.$$

Dans le deuxième, on a $51 = 3 \cdot 17$. Tous les termes sont divisibles par 3 sauf $17y$. Il est donc nécessaire que 3 divise y. En posant $y = 3z$ on obtient

$$\begin{aligned} \left\{ \begin{array}{lll} 3x+17y & = 9 & \mod 51 \\ 9x+6y & = 6 & \mod 51 \end{array} \right. &\Leftrightarrow \left\{ \begin{array}{lll} x+17z & = 3 & \mod 17 \\ 3x+6z & = 2 & \mod 17 \end{array} \right. \\ &\Leftrightarrow \left\{ \begin{array}{lll} x & = 3 & \mod 17 \\ z & = 13 & \mod 17 \end{array} \right. \\ &\Leftrightarrow \left\{ \begin{array}{lll} x & = 3, 20, 37 & \mod 51 \\ y & = 39 & \mod 51 \end{array} \right. \end{aligned}$$

15 Comme $2 \in (\mathbb{Z}/5\mathbb{Z})^*$ et $3 \in (\mathbb{Z}/7\mathbb{Z})^*$, on obtient

$$\left\{ \begin{array}{lll} 2x & = 37 & \mod 5 \\ 3x & = 48 & \mod 7 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lll} 2x & = 2 & \mod 5 \\ 3x & = 6 & \mod 7 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{lll} x & = 1 & \mod 5 \\ x & = 2 & \mod 7 \end{array} \right.$$

On utilise une relation de Bezout entre 5 et 7: $3 \cdot 5 - 2 \cdot 7 = 1$ pour remarquer que

$$15 = \left\{ \begin{array}{ll} 0 & \mod 5 \\ 1 & \mod 7 \end{array} \right. \quad \text{et} \quad -14 = \left\{ \begin{array}{ll} 1 & \mod 5 \\ 0 & \mod 7 \end{array} \right.$$

On en déduit que

$$2 \cdot 15 - 14 = 16 = \left\{ \begin{array}{ll} 1 & \mod 5 \\ 2 & \mod 7 \end{array} \right.$$

Alors x vérifie le système ssi $x - 16$ est divisible par 5 et 7, ssi $x - 16$ est divisible par 35. Finalement l'ensemble des solutions est l'ensemble des $x = 16 \mod 35$.

16 Pour résoudre une équation du second degré du type $x^2 + 2bx + c = 0$ dans un anneau A, on peut faire "comme dans $\mathbb{R}$" avec le début d'une carré, soit

$$x^2 + 2bx + c = 0 \Leftrightarrow (x+b)^2 - b^2 + c = 0.$$

Il faut ensuite discuter si $b^2 - c$ est un carré dans A. Si ce n'est pas le cas il n'y a pas de solution. Si $b^2 - c = a^2$ alors

$$x^2 + bx + c = 0 \Leftrightarrow (x+b)^2 - a^2 = 0 \Leftrightarrow (x+b-a)(x+b+a) = 0.$$

Alors $x = -b + a$ ou $x = -b - a$ ou $(x + b - a, x + b + a)$ est un couple de diviseurs de zéro (attention à ne pas oublier ce dernier cas..). L'équation $ax^2 + bx + c = 0$ se ramène au cas précédent si d'une part a est un inversible de A et d'autre part si 2 est inversible dans A (car alors on peut toujours écrire $a^{-1}b = 2b'$),

(a) $x^2 + x + 7 = 0$ dans $\mathbb{Z}/13\mathbb{Z}$: $x^2 + x + 7 = (x+7)^2 - 49 + 7 = (x+7)^2 - 3 \mod 13$. On a $3 = 16 = 4^2 \mod 13$ donc on obtient $(x + 7 - 4)(x + 7 + 4) = (x + 3)(x + 11)$ soit $x = 10, 2 \mod 13$.

(b) $x^2 - 4x + 3 = 0$ dans $\mathbb{Z}/12\mathbb{Z}$: $x^2 - 4x + 3 = (x-2)^2 - 1 = (x-3)(x-1)$. Les diviseurs de zéro dans $\mathbb{Z}/12\mathbb{Z}$ sont: $\{2, 3, 4, 6\}$. Les solutions sont donc: $x = 1, 3 \mod 12$ car aucun couple de diviseur de zéro ne convient.

(c) $x^2 - 2x + 3 = 0$ dans $\mathbb{Z}/4\mathbb{Z}$: $x^2 - 2x + 3 = (x-1)^2 + 2$. Les carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont $0, 1$. Comme 2 n'est pas un carré il n'y a pas de solutions.