

## Résolution de la congruence $x^e \equiv b \pmod{n}$ .

Un jour un correspondant m'a demandé si je connaissais une résolution de la congruence  $x^e \equiv b \pmod{n}$ ,  $x, e, b, n \in \mathbb{N}$  et  $\text{PGCD}(b, n) = 1$ .

Je savais que dans la base  $b$  l'inverse de  $e$  est symétrique par rapport à  $(n-1)/2$  soit  $n-1-e-2$  la solution est donnée par  $b^{n-1-(2+e)} \equiv x \pmod{n}$  quand  $n$  est premier et  $\text{PGCD}(e, p-1) = 1$

Soit la congruence  $x^{29} \equiv 61 \pmod{101}$ , l'exposant  $z = 100 - 31 = 69$ . donne la solution.

$$x \equiv 61^{69} \equiv 11 \pmod{101} \Leftrightarrow 11^{29} \equiv 61 \pmod{101}.$$

La congruence initiale et la congruence solution sont liés par leurs indices par la congruence linéaire :  $69 \times 29 \equiv 1 \pmod{100}$  et par 11 et 61 qui sont permutés.

L'identité de Bézout garantissant  $\text{PGCD}(e, \varphi(n)) = 1$  s'écrit :

$$(1) 29 \times 69 - 100 \times 20 = 1$$

Un algorithme non polynomial de DAYAN donne la solution de (1). Le premier membre de (1) est une congruence linéaire, elle permet de calculer l'exposant solution :  $29 \times z \equiv 1 \pmod{100}$ . Elle est résolue par la congruence donnant l'inverse de 29 :  $29^{99} \equiv 69 \pmod{100}$ , toujours à cause de la symétrie des indices inverses dans la base 29.

Résumé : La congruence  $x^e \equiv b \pmod{p}$  quand  $p$  est premier et  $\text{PGCD}(e, p-1) = 1$  est résolue par un indice  $z$  tel que la congruence  $b^z \equiv x \pmod{p}$ . L'exposant  $z$  est obtenu soit par l'identité de Bézout  $e \times z - (p-1) \times k = 1$  ou par  $e^{(p-2)} \equiv z \pmod{p-1}$  dont l'algorithme programmé est très performant.

La résolution de la congruence  $x^e \equiv b \pmod{n}$  est-elle isomorphe à celle de l'identité de Bézout dans tous les cas ?

Ecrivons la congruence dans le système des indices  $\text{ind}(x)$ .  $e \equiv \text{ind}(b) \pmod{\varphi(n)}$  dans la base  $b$   $\text{ind}(b) = 1$  et  $\text{ind}(x) = z$  ; Il vient  $z \times e \equiv 1 \pmod{\varphi(N)}$  soit une identité de Bézout  $z \times e - \varphi(N) \times k = 1$  avec  $\text{PGCD}(e, \varphi(n)) = 1$ .

A : Que se passe-t-il si  $n$  est composé ?

Soit  $x^{101} \equiv 5463 \pmod{10573}$  avec  $10573 = 97 \times 109$  et  $\varphi(10573) = 96 \times 108 = 10368$ . L'identité de Bézout correspondante  $101 \times 2669 - 10368 \times 26 = 1$  donne l'exposant, ainsi que la congruence  $101^{10367} \equiv 2669 \pmod{10368}$ .

$$5463^{2669} \equiv 11 \pmod{10573} \Leftrightarrow 11^{101} \equiv 5463 \pmod{10573}$$
$$2669 \times 101 - 10368 \times 26 = 1$$

Résumé : La congruence  $x^e \equiv b \pmod{p}$  quand  $p$  est composé et  $\text{PGCD}(e, \varphi(p)) = 1$  est résolue par un indice  $z$  tel que  $b^z \equiv x \pmod{p}$ . L'identité de Bézout associée :  $e \times z - \varphi(p) \times k = 1$  fournit la solution. Comme  $e \times z \equiv 1 \pmod{\varphi(p)}$ , la congruence  $e^{(\varphi(p)-1)} \equiv z \pmod{\varphi(p)}$  donne aussi la solution.

B : Que se passe-t-il si  $\text{PGCD}(e, \varphi(n)) = e$  ?

Alors l'identité de Bézout est impossible. Pour la rétablir il faut obtenir un nombre  $d$  premier avec  $e$  :  $d = \varphi(n) / e^i$ .

Exemple :  $x^5 \equiv 111 \pmod{143}$   $\varphi(143) = 10 \times 12 = 120$  alors  $d = 120 / 5 = 24$ , l'identité de Bézout triviale est immédiate il vient :  $5 \times 5 - 1 \times 24 = 1$ , la congruence  $5^{23} \equiv 5 \pmod{24}$  confirme la solution.

$$111^5 \equiv 89 \pmod{143} \Leftrightarrow 89^5 \equiv 111 \pmod{143}$$

Résumé : La congruence  $x^e \equiv b \pmod{p}$  quand  $p$  est composé et  $\text{PGCD}(e, \varphi(p)) = e$ , nécessite d'ôter tous les facteurs  $e$  de  $\varphi(p)$  et de calculer  $d = \varphi(p) / e^i$ . L'indice  $z$ , inverse de  $e$  modulo  $d$ , est obtenu par une identité de Bézout réduite  $e \times z - d = 1$  ou par la congruence  $e^{(d-1)} \equiv z \pmod{d}$ .

C : Existe-t-il des formules de résolution simplifiées ?

1 / Avec  $e = 2$  et  $\varphi(n)$  qui est pair, il nous faut donc un nombre impair  $d = \varphi(n) / 2^i$  pour obtenir une identité de Bézout valide :  $2 \times z - d \times 1 = 1$ . Alors  $z = (d + 1) / 2$ .

Exemple :  $x^2 \equiv 35 \pmod{1261}$ ,  $1261 = 97 \times 13$ ,  $\varphi(1261) = 96 \times 12 = 1152$  et  $d = 1152 / 2^7 = 9$  alors  $z = (9 + 1) / 2 = 5$  :

$$35^5 \equiv 1225 \pmod{1261} \Leftrightarrow 1225^2 \equiv 35 \pmod{1261}$$

l'identité de Bézout devient triviale :  $5 \times 2 - 9 \times 1 = 1$

2 / Quand l'exposant  $e$  est premier le second membre de (1) donne la congruence  $\varphi(n) \times k \equiv -1 \pmod{e}$  qui permet de calculer  $k$  par :  $e - \varphi(n)^{(e-2)} \equiv k \pmod{e}$  puis d'obtenir :  $z = ((\varphi(n) \times k + 1) / e)$ .

Exemple :  $x^{197} \equiv 252 \pmod{3637}$ . De l'identité de Bézout  $197 \times z - 3636 \times k = 1$  nous tirons le calcul de l'inconnu  $k$  :  $k \equiv 197 - 3636^{195} \pmod{197} \equiv 197 - 81 \equiv 116 \pmod{197}$  alors  $z = (3636 \times 116 + 1) / e = 2141$ . On vérifie l'identité de Bézout :  $197 \times 2141 - 3636 \times 116 = 1$ .

$$x \equiv 252^{2141} \equiv 2096 \pmod{3637} \Leftrightarrow 2096^{197} \equiv 252 \pmod{3637}$$

$$2141 \times 197 - 3636 \times 116 = 1$$

Résumé : Quand l'exposant  $e$  est premier la congruence  $x^e \equiv b \pmod{n}$  est résolue, en deux temps, on calcul d'abord l'inconnu  $k \equiv e - \varphi(n)^{e-2} \pmod{e}$  puis  $z = ((\varphi(n) \times k + 1) / e)$ .

3 / Les nombres de la forme  $\varphi(n) = e \times m + 1$  avec  $e$  premier, permettent de résoudre par une formule simple la congruence  $x^e \equiv b \pmod{n}$ . L'identité de Bézout devient  $e \times z - (e m + 1) \times k = 1$ . Comme  $e$  est premier nous pouvons calculer d'abord  $k : k = e - (e m + 1)^{e-2} \equiv e - 1 \pmod{e}$  alors l'exposant  $z = [(e - 1)(e m + 1) + 1] / e = [e^2 m - e m + e - 1 + 1] / e = e m - m + 1 = m(e - 1) + 1$ .

Résumé : les nombres de la forme  $\varphi(n) = e \times m + 1$  permettent de résoudre la congruence  $x^e \equiv b \pmod{n}$  par la congruence  $b^{m(e-1)+1} \pmod{n}$  et l'identité de Bézout devient  $e \times (m(e-1) + 1) - (e m + 1)(e - 1) = 1$

Exemple :  $p = 197$ ,  $\varphi(p) = 196 = 15 \times 13 + 1$   $e = 13$ . Soit  $x^{13} \equiv 173 \pmod{197}$  alors  $z = 15 \times 12 + 1 = 181$  et la solution de la congruence initiale  $x \equiv 173^{181} \equiv 97 \pmod{197} \Leftrightarrow 97^{13} \equiv 173 \pmod{197}$ . L'identité  $13 \times 181 - 196 \times 12 = 1$ .

Exemple avec  $n$  composé :  $n = 10961 = 97 \times 113$ ,  $x^{13} \equiv 6430 \pmod{10961}$ ,  $\varphi(n) = 96 \times 112 = 10752$ ,  $10751 = 13 \times 827$ , l'exposant  $z = 827 \times 12 + 1 = 9925$  alors :

$$6430^{9925} \equiv 197 \pmod{10961} \Leftrightarrow 197^{13} \equiv 6430 \pmod{10961} .$$

$$13 \times 9925 - 10752 \times 12 = 1$$

D / Si aucune méthode convient l'algorithme de Dayan Voici le programme BEZOUT

BEZOUT

```
LBL 0 : ? → N : N = 0 ⇒ GOTO 1 : ? → M :
      PRO" BZT" : if S < 0 : THEN N + S → S - (MS - 1) / N → U IFEND
      {M, S, N, U} ♦
      GOTO 0
LBL 1 : CLRTEXT
```

BZT

```
M → O : N → Q : 1 → S : 0 → T : 1 → V :
WHILE Q > 0 : O QUOTIENT Q → X : O RESTE Q → Y
S - XT → P : U - XV → R : Q → O : Y → Q : T → S : P → T : V → U : R → V
WHILEEND
```

E / Une applications : résolution de l'équation (2)  $a x^2 + b x + c \equiv 0 \pmod{p}$

Multiplions (2) par  $(4 a)$  il vient  $(2a x + b)^2 \equiv b^2 - 4 a c \equiv \Delta \pmod{p}$  soit  $r^2 \equiv \Delta \pmod{p}$  avec  $r = 2a x + b$  et  $\Delta = b^2 - 4ac$ .

Soit  $d$  impair =  $(p-1)/2$  Si  $\Delta^d \equiv 1 \pmod{p}$  on peut continuer par  $z = (d + 1) / 2$  et  $\Delta^z \equiv r_1$  Entier $[(r_1 - b) / 2a] = x_1$  et la seconde racine Entier $[(p - r_1 - b) / 2a] = x_2$ .

Exemple :  $3x^2 + 23x + 41 \equiv 0 \pmod{3637}$ . Le discriminant  $\Delta = 37$ ,  $d = 3636 / 4 = 909$ ,  $37^{909} \equiv 1 \pmod{3637}$  alors l'exposant solution  $z = (909 + 1) / 2 = 455$ .

$r_1 = 37^{455} \equiv 209 \pmod{3637}$  et  $x_1 = (209 - 23) / 6 = 31$   
 $r_2 = 3637 - 209 = 3428$  donne  $6 x_2 = 3428 - 23 \equiv 3405 \pmod{3637}$  et la seconde  
 inconnue  $x_2 \equiv 3405 \times 6^{3635} \equiv 2386 \pmod{3637}$ .

F / Application à l'algorithme de cryptographie à clef publique RSA.

On choisit deux nombres premiers  $p$  et  $q$  et on forme  $N = p \times q$  et on calcule  $\varphi(N) = (p - 1)(q - 1)$ . On choisit les clefs publiques  $s$  parmi les nombres, premiers avec  $\varphi(N)$  et l'on calcule la congruence  $s \times t \equiv 1 \pmod{\varphi(N)}$  alors l'identité de Bézout s'écrit  $s \times t - \varphi(N) \times k = 1$  elle permet de coder le message numérisé  $x_i$  :

$$x_i^t \equiv c_i \pmod{N} \Leftrightarrow c_i^s \equiv x_i \pmod{N}$$

On retrouve une solution similaire à notre congruence initiale, la différence est que dans RSA  $s$  est première avec  $\varphi(N)$  alors que dans la résolution de notre congruence initiale l'indice  $e$  peut diviser  $\varphi(N)$  et nous obliger à calculer  $d$  premier avec  $e$ .

Il faut choisir des nombres  $p$  et  $q$  assez grands pour que la mise en facteur de  $N$  soit impossible. Les clefs  $s$  doivent être premières avec  $\varphi(N)$  et avec  $\varphi(N) - 1$  en raison de C paragraphe 3.

Exemple :  $x^5 \equiv 233 \pmod{247}$ ,  $N = 247 = 13 \times 19$ ,  $\varphi(N) = 12 \times 18 = 216$ ,  $215 = 5 \times 43$  alors  $z = 4 \times 43 + 1 = 173$  et la congruence  $233^{173} \equiv 25 \pmod{247}$  donne la solution et définit l'identité de Bézout :  $5 \times 173 - 216 \times 4 = 1$ .

Dans le cas où  $e$  divise  $\varphi(N) - 1$  l'indice pour décrypter le message  $z = (e - 1)K + 1$  et  $\varphi(N) = Ke + 1 = (p - 1)(q - 1)$

On comprend pourquoi  $\varphi(N)$  doit rester secret.

G / La factorisation quadratique de  $n$  de RSA montre que  $p$  et  $q$  ne doivent pas être de même ordre de grandeur.

$N - 1 - \varphi(N) = pq - 1 - pq + p + q - 1 = (p - 1) + (q - 1) = S$   
 $\varphi(N) = (p - 1)(q - 1) = P$  on tire  $N - 1 - P = S$ . L'équation quadratique suivante  $x^2 - Sx + P = 0$  a pour racine  $(p - 1)$  et  $(q - 1)$ . Si le déterminant  $\Delta = \sqrt{S^2 + 4P}$  est entier alors  $p = 1 + \frac{1}{2}(S + \Delta)$  et  $q = 1 + \frac{1}{2}(S - \Delta)$ .

Exemple :  $N = 3626089$ , en 10 seconde, le programme suivant de ma calculatrice, a donné  $3626089 = 997 \times 3637$  après 207 itérations.

FACQUAD

LBL 0 : ? → N : N = 0 ⇒ GOTO 1 :

INT √ N → R : 2 → F :

1 = (N - 2 R) mod 4 ⇒ 4 → F : 2 R - F → Q

FOR Q → S TO N STEP F

N - 1 - S → P

S<sup>2</sup> - 4 P = D

```

D < 0 ⇒ NEXT
√ D → D
IF 0 = FRAC D : THEN
1 + (S + D) / 2 ♦
1 + (S - D) / 2 ♦
BREAK
IFEND
NEXT
GOTO 0
LBL 1 : CLRTEXT

```

Plus les facteurs p et q sont proches plus ce programme est performant, si N est un carré la réponse est instantanée de même que pour des nombres ayant le même nombre de chiffres ( $3637 \times 4243 = 15431791$ ).. Par contre ( $3637 \times 1236541 = 4497299617$ ) avec 551209 itérations à demandé plus de 7 heures.

C'est pourquoi les nombres premiers de RSA doivent être de taille différente pour que la factorisation soit impossible avec un ordinateur puissant. Soit  $p = x \cdot 10^{400} + a$  et  $q = y \cdot 10^{250} + b$ , le produit a 400 chiffres décimaux, la racine de  $N = p \cdot q$  a 325 chiffres et  $2R - 4$  a aussi 325 chiffres, le différentiel avec 400 donne l'indice 75 qui demande a mon programme d'effectuer  $\frac{1}{4} (z \cdot 10^{75})$  itérations. Le temps nécessaire  $t = (\frac{1}{4} (z \cdot 10^{75}) (10 / 207)) \approx 10^{74}$  secondes. Une année comporte  $3.1536000 \cdot 10^7$  secondes soit environ ( $10^{67}$ ) ans pour mettre en facteur N avec ma calculatrice ; Si un ordinateur est un milliard de fois plus rapide que ma calculatrice et le programme de factorisation un milliard de fois plus puissant que FACQUAD il lui faudra encore  $10^{49}$  ans. Ce qui est impensable ! car le soleil aura grillé la terre bien avant la fin de la mise en facteur !

H / Recherche de formule pour des nombres premiers  $p = a \times m + b$

Si  $e = 2$  et  $p = 4m + 3$ ,  $\varphi(n) = 4m + 2$ ,  $d = 2m + 1$ . Considérons la congruence  $x^2 \equiv b \pmod{4m + 3}$ , la congruence  $x^{2m+1} \equiv 1 \pmod{4m + 3}$  peut s'écrire  $x \times x^{2m} \equiv 1 \pmod{4m + 3}$   $x^{2m} \equiv b^m \pmod{4m + 3}$ . Il vient  $x \equiv b^{m(P-2)} \pmod{4m + 3}$   
Si  $e = 3$  et  $p = 9m + 4$ , alors  $z = (p - 2) m \pmod{3m + 1}$   
Si  $e = 4$  et  $p = 16m + 5$  alors  $z = (p - 2) m \pmod{4m + 1}$

Si e et  $p = e^2 m + e + 1 = e(e+1) + 1$  alors  $z = ((p - 2) m) \pmod{(e m + 1)}$

Soit  $p = 3919907 = 101 \times 197^2 + 197 + 1$ ,  $d = 197 \times 101 + 1 = 19898$ . Soit la congruence  $x^{197} \equiv 2323742 \pmod{3919907}$ , comme  $2323742^{19898} \equiv 1 \pmod{3919907}$   $z = (3919907 - 2) \times 101 \equiv 19797 \pmod{19898}$

$$2323742^{19797} \equiv 1867728 \pmod{3919907} \Leftrightarrow 1867728^{197} \equiv 2323742 \pmod{3919907}$$

$$197 \times 19797 - 19898 \times 198 = 1$$

Cette formules se limite aux nombres premiers d'une seule forme, alors que par la formule générale quand e divise  $\varphi(n) - 1$  est un polynôme linéaire :  $z = (e - 1) m + 1 = 196 \times 101 + 1 = 19797$ . Il semble illusoire de chercher d'autres formules.

Daniel Guoin

