2.8.9

21.01.20

Voici à titre d'exemple l'évaluation de a^{35}.

— On écrit l'exposant n comme une somme de puissance de 2. Ici, $35 = 32 + 2 + 1$;

— on calcule ensuite les puissances paires de a : $a^2 = a \cdot a$, $a^4 = a^2 \cdot a^2$, $a^8 = a^4 \cdot a^4$, $a^{16} = a^8 \cdot a^8$, $a^{32} = a^{16} \cdot a^{16}$.

— on multiplie pour terminer les « bons » carrés : $a^{35} = a^{32} \cdot a^2 \cdot a^1$;
Le nombre de multiplications nécessaires est dans ce cas de 7, au lieu de 34.

2.8.9

21.01.20

Voici à titre d'exemple l'évaluation de a^{35}.

— On écrit l'exposant n comme une somme de puissance de 2. Ici, $35 = 32 + 2 + 1$;

— on calcule ensuite les puissances paires de a : $a^2 = a \cdot a$, $a^4 = a^2 \cdot a^2$, $a^8 = a^4 \cdot a^4$, $a^{16} = a^8 \cdot a^8$, $a^{32} = a^{16} \cdot a^{16}$.

— on multiplie pour terminer les « bons » carrés : $a^{35} = a^{32} \cdot a^2 \cdot a^1$;
Le nombre de multiplications nécessaires est dans ce cas de 7, au lieu de 34.

10

2^6	2^5	2^4	2^3	2^2	2^1	2^0
0	1	0	0	0	1	1

$35 = 32 + 2 + 1$

$35 = 100011$

$a^{35} = \underbrace{a \cdot a \cdot a \cdot \_\_ \_ \cdot a}_{35\times}$

34 multiplications

$a^{35} = a^{32} \cdot a^2 \cdot a$

$a^2 = a \cdot a$

$a^4 = a^2 \cdot a^2$

$a^8 = a^4 \cdot a^4$

$a^{16} = a^8 \cdot a^8$

$a^{32} = a^{16} \cdot a^{16}$

(2)
(1)
(1)
(1)
(1)
(1)

7 multiplications

a) Combien de multiplications nécessite cet algorithme pour calculer chacune des puissances suivantes : a^{10}, a^{61}, a^{1000} ?

- $10 = 8 + 2$

$a^{10} = a^8 \cdot a^2$ (1)

$a^2 = a \cdot a$ (1)

$a^4 = a^2 \cdot a^2$ (1)

$a^8 = a^4 \cdot a^4$ (1)

4 multiplications

$61_{10} = 111101_2$

- $61 = 32 + 16 + 8 + 4 + 1$

$a^{61} = a^{32} \cdot a^{16} \cdot a^8 \cdot a^4 \cdot a^1$ (4)

9 multiplications

a^{1000} 14 multiplications

b) Calculer $835^{25} \pmod{1073}$, en 6 multiplications.

$25 = 16 + 8 + 1$

$835^{25} = 835^{16} \cdot 835^{8} \cdot 835$ (2)

$835^{2} \equiv 848 \pmod{1073}$ (1)

$835^{4} \equiv 848^{2} \equiv 194 \pmod{1073}$ (1)

$835^{8} \equiv 194^{2} \equiv 81 \pmod{1073}$ (1)

$835^{16} \equiv 81^{2} \equiv 123 \pmod{1073}$ (1)

6 multiplications

$835^{25} \equiv (123 \cdot 81) \cdot 835$ (1) $\pmod{1073}$

$\equiv 306 \cdot 835$ (1) $\pmod{1073}$

$\equiv 136 \pmod{1073}$

Fonction indicatrice d'Euler

On dit que deux nombres a et b sont premiers entre eux si $pgdc(a,b) = 1$.
Par exemple 21 et 38 sont premiers entre eux.

La fonction indicatrice d'Euler, notée φ, est l'application qui, à tout entier naturel n non nul, associe le nombre des entiers naturels inférieurs à n et relativement premiers à n.

$\varphi(12) = 4$

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

$pgdc(5,4) = 1$

2.8.16 Calculer $\varphi(n)$ dans les cas suivants :

a) $n = 4$, $n = 8$, $n = 16$, $n = 32$;

$\varphi(2) = 1$
$\varphi(3) = 2$
$\varphi(5) = 4$

$\varphi(2^2) = 2 = 2^1 \cdot 1$
$\varphi(2^3) = 4 = 2^2 \cdot 1$
$\varphi(2^4) = 8 = 2^3 \cdot 1$
$\varphi(2^5) = 16 = 2^4 \cdot 1$

$\varphi(p) = p - 1$ pour p premier

$\varphi(p^r) =$

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

$\varphi(2^4) = 2^4 - 2^3 = 2^3 \cdot (2-1)$

$\varphi(p^r) = p^{r-1} \cdot (p-1)$

Autre exemple

$\varphi(3^4) = \varphi(81) = 81 - 3^3 = 81 - 27 = 3^4 - 3^3 = 3^3(3-1) = 3^3 \cdot 2 = 54$

1	11	21	31	41	51	61	71	81
2	12	22	32	42	52	62	72	
3	13	23	33	43	53	63	73	
4	14	24	34	44	54	64	74	
5	15	25	35	45	55	65	75	
6	16	26	36	46	56	66	76	
7	17	27	37	47	57	67	77	
8	18	28	38	48	58	68	78	
9	19	29	39	49	59	69	79	
10	20	30	40	50	60	70	80	

$$\varphi(81) = 3^4 - 3^3 = 3^3(3-1) = 54$$

$$\varphi(p^r) = p^{r-1} \cdot (p-1)$$

Propriétés de φ

1) $\varphi(p) = p - 1$, p premier

2) $\varphi(p^r) = p^{r-1} \cdot (p-1)$, p premier

3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, si $pgdc(a, b) = 1$

2.8.16

2.8.11

2.8.12

2.8.10