

Μήκος λέξης: 64 bit

$n$  με  $u$ -ψηφία ( $b$ -αριθ.)

$$n = \underbrace{(b-1)(b-1)\dots(b-1)}_{u\text{-ψηφία}} = b^u - 1$$

$$\lceil \log_b n \rceil + 1 \geq u \quad \leadsto \quad \log_b n = \frac{\log_2 n}{\log_2 b}$$

$o(\log n)$

Πρόσθεση:

$$\begin{array}{r} 53 \\ + 35 \\ \hline 88 \end{array} + \begin{array}{r} 5 \cdot 10^1 + 3 \cdot 10^0 \\ 3 \cdot 10^1 + 5 \cdot 10^0 \\ \hline 8 \cdot 10^1 + 8 \cdot 10^0 \end{array}$$

Πρόσθεση: Πρόσθεση 3 ψηφίων με  $b$ -αριθό αριθμούς

$\Rightarrow$  2 ψηφία περίσσια.

Ανάλυση:

$$\begin{array}{r} b-1 \\ b-1 \\ + b-1 \\ \hline 3b-3 \leq b^2-1 \quad \dots \end{array}$$

$$\begin{array}{r} 110101 \\ + 100011 \\ \hline 1011000 \end{array}$$

$\leadsto$

$$\begin{array}{r} 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 \\ \hline 2 \cdot 2^1 + 0 \cdot 2^0 \end{array}$$

Απάντηση :  ~~$O(\log n)$  αν η είσοδος υπάρχει  
σε αυτό το  $n$ .~~

$O(n)$

αν η είσοδος  $S_k$   
πάρει  $n$  (n times)

• (70) & (1) analysis

$$\begin{array}{r} 43 \\ \times 10 \\ \hline 130 \end{array}$$

$$1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$\begin{array}{r} 1101 \\ \times \quad 10 \\ \hline 11010 \end{array}$$

$$\begin{array}{r|l} 135 & 10 \\ \hline 5 & 13 \end{array}$$

$$\begin{array}{r|l} 1101 & 10 \\ \hline 1 & 110 \end{array}$$

$$\begin{array}{r} 13 \\ \times 11 \\ \hline 13 \\ + 13 \\ \hline 143 \end{array}$$

$$\begin{array}{r} 13 \\ \times 1 \cdot 20^1 + 1 \cdot 20^0 \\ \hline 13 \\ + 130 \\ \hline 143 \end{array}$$

At no / m x, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000

$$\underbrace{O(n) + \dots + O(n)}_{n \text{ terms}} = O(n^2)$$

$$\downarrow$$

$$O(n^{1.59})$$

No) / nro)      Pinno      App) m:

$1 \cdot 2^0$     1 1    13     $2^0 \cdot 13$

$1 \cdot 2^1$     5    26     $2^1 \cdot 13$

$0 \cdot 2^2$     ~~2~~    ~~52~~     $2^2 \cdot 13$

$1 \cdot 2^3$     1    104     $2^3 \cdot 13$

---

143

$$X \cdot Y = \begin{cases} 2 \cdot (X \cdot \lfloor Y/2 \rfloor) & \text{if } Y \text{ is even} \\ X + 2 \cdot (X \cdot \lfloor Y/2 \rfloor) & \text{if } Y \text{ is odd} \end{cases}$$

multiply (X, Y):

Inputs: Assume  $X, Y \geq 0$  (n bit)

Base case:  $\emptyset$   $X \cdot Y$

if  $Y = 0$ , return 0

$Z = \text{multiply}(X, \lfloor Y/2 \rfloor)$

if  $Y$  is even

return  $2 \cdot Z$  (recursion + shift)

else

return  $X + 2 \cdot Z$  (recursion + shift)

Analysis:

$O(n)$  - worst case  
analysis

$O(n)$  (if we use shift  
analysis)

$O(n^2)$

$O(n)$

• Dimensions:

$$\begin{array}{c|c} 13 & 5 \\ \hline 2 & 2 \end{array}$$

$$\begin{array}{c|c} 13/2 & 5 \\ \hline 1 & 1 \\ \cdot & \cdot \\ 2 & 2 \\ 11 & + \\ & 1 \\ 2 & 11 \\ & 3 \end{array}$$

$X = q \cdot \gamma + v$

•  $X$  dimensions:  $\left[ \frac{X}{2} \right] = \frac{X}{2} = q' \cdot \gamma + v' \quad \text{2}$

$$X = \underbrace{2q'}_q \cdot \gamma + \underbrace{2v'}_v$$

•  $X$  ny,  $v_0$ :  $\left\lfloor \frac{X}{2} \right\rfloor = \frac{X-1}{2} = e_1' \cdot \gamma + v_1' \cdot 2$

$\cdot 2 \rightarrow X-1 = 2e_1' \cdot \gamma + 2v_1'$

$X = \underbrace{2e_1'}_q \cdot \gamma + \underbrace{2v_1' + 1}_r$

divide(x, y):

Inputs: Arbitrary  $x, y \geq 1$  ( $n$  bit)

Outputs: Finding  $q$  and remainder  $r$  so  $x = qy + r$

if  $x = 0$  return  $(0, 0) \rightsquigarrow O(1)$

$(q', r') = \text{divide}(\lfloor x/2 \rfloor, y)$

$q = 2q', r = 2r' \rightsquigarrow O(n)$

if  $x \geq y$  then  $q = q' + 1 \rightsquigarrow O(1)$

$r = r' + 1 \rightsquigarrow O(n)$



if  $r \geq y \rightarrow O(n)$

$q = q + 1, r = r - y \rightarrow O(n)$

return  $(q, r)$ .

Complexity:  $O(n)$  and  $O(n)$  in time

$O(n)$

$O(n^2)$

Algorithm:

$$\begin{array}{r}
 \begin{array}{ccc} 0 & 1 & \\ 1 & \cancel{1} & 0 \end{array} \quad \sim 13 \\
 - \begin{array}{ccc} 1 & 0 & 1 \end{array} \quad \sim 11 \\
 \hline
 \begin{array}{ccc} \cancel{0} & 0 & 1 \end{array} \quad \sim 2
 \end{array}$$

$$\begin{array}{r}
 \begin{array}{ccccccc} 0 & 1 & & & & & \\ \cancel{1} & \cancel{1} & \cancel{1} & 0 & 0 & 1 & 1 \end{array} \quad \sim 115 \\
 - \begin{array}{ccccccc} & & & 1 & 1 & 0 & 1 \end{array} \quad \sim 26 \\
 \hline
 \begin{array}{ccccccc} 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array} \quad \sim 109
 \end{array}$$

$$O(n)$$

## Arithmetische Funktionen:

Modular Erweitern:  $x, y$  paarweise teilerfremd,  $x > y$

z.B.  $\mu(x, y) = \mu(x \bmod y, y)$

Anst.

Ausw. u.d.o.

$$\mu(x, y) = \mu(x - y, y)$$

noch teilerfremd

$$\begin{array}{l} b \mid x \\ b \mid y \end{array} \Rightarrow b \mid x - y$$

$$\dots \Rightarrow \mu(x, y) \leq \mu(x - y, y)$$

$$\left. \begin{array}{l} b \mid x-y \\ b \mid y \end{array} \right\} \Rightarrow b \mid x \quad \dots \Rightarrow \gcd(x-y, y) \leq \gcd(x, y)$$

Euclid (a, b)

Inputs: Arguments a, b,  $a \geq b \geq 0$  (n bit)

Output:  $\gcd(a, b)$

if  $b = 0$

return a

else

return Euclid(b,  $a \bmod b$ ).

Lemma:  $a \geq b \Rightarrow a \bmod b < \frac{a}{2}$

Proof:

•  $b \leq a/2$ :

$$a \bmod b < b \leq a/2$$

•  $b > a/2$

$$a \bmod b = a - b < a - \frac{a}{2}$$

$$= \frac{a}{2}$$

Exemple

$2 \cdot n$

αναίρεση αριθμών

//

$O(n)$

\*

$O(n^2)$

(για διάγνωση)

//

$O(n^3)$