Catargiu Georgiana-Ecaterina
932/1

Assignment 1

· nr. matricol : 2491

a). $n = 931$

S0 : $n-1 = 2^s \cdot t \Rightarrow 931 = 2 \cdot 465$

$\Rightarrow \begin{cases} s = 1 \\ t = 465 \end{cases}$

S1 : we choose an a, $1 < a < 931$.

$a = 2 \rightarrow$ then 2^{465} (modulo 931)

· since $s = 1 \Rightarrow$ the seq. 2^{465} (modulo 931) has one single element

$2^{465} = x$ modulo 931 - we need to find the x so we perform the Repeated Squaring Modular Exp. algorithm from Course 2.

① first we write 465 as a sum of powers of 2: $465 = 2^8 + 2^7 + 2^6 + 2^4 + 2^0$ and then put and compute modulo 931

$2^{2^0} = 2^1 = 2$ modulo 931

$2^{2^1} = 2^{2^0} \cdot 2^{2^0} = 2 \cdot 2 = 2^2 = 4$ modulo 931

$2^{2^2} = 2^{2^1} \cdot 2^{2^1} = 2^2 \cdot 2^2 = 4^2 = 16$ modulo 931

$2^{2^3} = 2^{2^2} \cdot 2^{2^2} = 2^4 \cdot 2^4 = 16^2 = 256$ modulo 931

$2^{2^4} = 2^{2^3} \cdot 2^{2^3} = 256^2 = 366$ modulo 931

$2^{2^5} = 2^{2^4} \cdot 2^{2^4} = 366^2 = 823$ modulo 931

$2^{2^6} = 2^{2^5} \cdot 2^{2^5} = 823^2 = 492$ modulo 931

$2^{2^7} = 2^{2^6} \cdot 2^{2^6} = 492^2 = 4$ modulo 931

$2^{2^8} = 2^{2^7} \cdot 2^{2^7} = 4^2 = 16$ modulo 931

$465 = 2^8 + 2^7 + 2^6 + 2^4 + 2^0$

$\Rightarrow 2^{465} = 2^{(2^8+2^7+2^6+2^4+2^0)} = 2^{2^8} \cdot 2^{2^7} \cdot 2^{2^6} \cdot 2^{2^4} \cdot 2^{2^0}$

$= 16 \cdot 4 \cdot 492 \cdot 366 \cdot 2 = 449 \mod 931$

$\rightarrow$ The seq. is [449] $\Rightarrow$ 931 is composite for sure.

b). $n = 2269$

S_0 : $n-1 = 2^s t \Rightarrow 2268 = 2^2 \cdot 567$

$\rightarrow \begin{cases} s = 2 \\ t = 567 \end{cases}$

I. $a=2$

S_1 : we choose an a, $1 < a < 2269$, $a = 2$

$s = 2 \Rightarrow 2^{2^0 \cdot 567}, 2^{2^1 \cdot 567}, 2^{2^2 \cdot 567} \mod 2269$

$2^{567} = x$ modulo 2268 $\rightarrow$ we try to find the x with repeatedly squaring modular exp.

$\hookrightarrow$ as before, we write 567 as powers of 2

$567 = 2^9 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0$

$2^{2^0} = 2^1 = 2$ modulo 2269

$2^{2^1} = 2^{2^0} \cdot 2^{2^0} = 2^2 = 4$ modulo 2269

$2^{2^2} = 2^{2^1} \cdot 2^{2^1} = 4^2 = 16$ modulo 2269

$2^{2^3} = 2^{2^2} \cdot 2^{2^2} = 16^2 = 256$ modulo 2269

$2^{2^4} = 2^{2^3} \cdot 2^{2^3} = 256^2 = 2004$ modulo 2269

$2^{2^5} = 2^{2^4} \cdot 2^{2^4} = 2004^2 = 2155$ modulo 2269

$2^{2^6} = 2^{2^5} \cdot 2^{2^5} = 2155^2 = 1651$ modulo 2269

$2^{2^7} = 2^{2^6} \cdot 2^{2^6} = 1651^2 = 732$ modulo 2269

$2^{2^8} = 2^{2^7} \cdot 2^{2^7} = 732^2 = 340$ modulo 2269

$2^{2^9} = 2^{2^8} \cdot 2^{2^8} = 340^2 = 2150$ modulo 2269

$567 = 2^9 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0$

$\hookrightarrow 2^{567} = 2^{(2^9 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0)}$

$= 2^{2^9} \cdot 2^{2^5} \cdot 2^{2^4} \cdot 2^{2^2} \cdot 2^{2^1} \cdot 2^{2^0}$

$= 2150 \cdot 2155 \cdot 2004 \cdot 16 \cdot 4 \cdot 2 = -1 \mod 2269$

$2^{567} = \qquad = 2^{434} = -1 \mod 2269$

$2^{2 \cdot 567} = 2^{2 \cdot 567} \cdot 2^{2 \cdot 567} = (-1) \cdot (-1) = 1 \mod 2269$

The resulting seq: $[-1, 1]$ => 2269 is prime (probably)

II. $a = 3$ => $3^{567}, 3^{2 \cdot 567}, 3^{3 \cdot 567} \mod 2269$

$3^{567} = x \mod 2269$ -> by repeatedly squaring modular exp.

$567 = 2^9 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0$

$3^{2^0} = 3^1 = 3 \mod 2269$

$3^{2^1} = 3^{2^0} \cdot 3^{2^0} = 3^2 = 9$ modulo 2269

$3^{2^2} = 3^{2^1} \cdot 3^{2^1} = 9^2 = 81$ modulo 2269

$3^{2^3} = 3^{2^2} \cdot 3^{2^2} = 81^2 = 2023$ modulo 2269

$3^{2^4} = 3^{2^3} \cdot 3^{2^3} = 2023^2 = 1522$ modulo 2269

$3^{2^5} = 3^{2^4} \cdot 3^{2^4} = 1522^2 = 2104$ modulo 2269

$3^{2^6} = 3^{2^5} \cdot 3^{2^5} = 2104^2 = 2256$ modulo 2269

$3^{2^7} = 3^{2^6} \cdot 3^{2^6} = 2256^2 = 169$ modulo 2269

$3^{2^8} = 3^{2^7} \cdot 3^{2^7} = 169^2 = 1333$ modulo 2269

$3^{2^9} = 3^{2^8} \cdot 3^{2^8} = 1333^2 = 262$ modulo 2269

$\hookrightarrow 3^{567} = 3^{(2^9 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0)} = 3^{2^9} \cdot 3^{2^5} \cdot 3^{2^4} \cdot 3^{2^2} \cdot 3^{2^1} \cdot 3^{2^0}$

$= 262 \cdot 2104 \cdot 1522 \cdot 81 \cdot 9 \cdot 3 = -1 \mod 2269$

$3^{567} = \qquad = -1 \mod 2269$

$3^{2 \cdot 567} = 2^{567} \cdot 2^{567} = (-1)^2 = 1 \mod 2269$

The seq: $[-1, 1]$ => 2269 is probably prime

III. $a=5$ $\rightarrow$ we choose $a=5$ $\Rightarrow$ $5^{567} = x$ modulo 2269

$\Rightarrow$ we again do squaring modular exponentiation

$567 = 2^9 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0$

$5^{2^0} = 5^1 = 5$ modulo 2269

$5^{2^1} = 5^{2^0} \cdot 5^{2^0} = 5 \cdot 5 = 5^2 = 25$ modulo 2269

$5^{2^2} = 5^{2^1} \cdot 5^{2^1} = 25^2 = 625$ modulo 2269

$5^{2^3} = 5^{2^2} \cdot 5^{2^2} = 625^2 = 357$ modulo 2269

$5^{2^4} = 5^{2^3} \cdot 5^{2^3} = 357^2 = 385$ modulo 2269

$5^{2^5} = 5^{2^4} \cdot 5^{2^4} = 385^2 = 740$ modulo 2269

$5^{2^6} = 5^{2^5} \cdot 5^{2^5} = 740^2 = 771$ modulo 2269

$5^{2^7} = 5^{2^6} \cdot 5^{2^6} = 771^2 = 2232$ modulo 2269

$5^{2^8} = 5^{2^7} \cdot 5^{2^7} = 2232^2 = 1369$ modulo 2269

$5^{2^9} = 5^{2^8} \cdot 5^{2^8} = 1369^2 = 2236$ modulo 2269

$\hookrightarrow 5^{567} = 5^{(2^9 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0)} =$

$= 5^{2^9} \cdot 5^{2^5} \cdot 5^{2^4} \cdot 5^{2^2} \cdot 5^{2^1} \cdot 5^{2^0} =$

$= 2236 \cdot 740 \cdot 385 \cdot 625 \cdot 25 \cdot 5 = -1$ modulo 2269

$2^{567} = -1$ modulo 2269

$2^{2 \cdot 567} = 2^{567} \cdot 2^{567} = (-1)^2 = 1$ modulo 2269

The resulting seq : $[-1, 1]$ $\Rightarrow$ 2269 is probably prime