16-Powers Modulo m and Successive Squaring

How would you compute $5^{100000000000000}$ (mod 12830603)?

12830603 = 3571 · 3593

$\emptyset$(12830603) = $\emptyset$(3571)$\emptyset$(3593) = 3570. 3592 = 12823440.

Euler's Formula

$a^{\emptyset(m)} \equiv 1 \pmod m$ for any a and m with gcd(a, m) =1

so we can use the fact that

100000000000000=7798219*12823440+6546640

to "simplify" our problem,

$$5^{100000000000000} = (\ 5^{12823440}\ )^{7798219} . 5^{6546640}$$

$$\equiv 5^{6546640} \pmod{12830603}.$$

more than 4 million digits!!!

- It is possible to use the computation of $a^k \pmod{m}$ to encode and decode messages.

Successive Square Method

$$??? \equiv 7^{327} \pmod{853}$$

Table of 2^k-powers of 7 modulo 853

$7^1 \equiv 7 \equiv 7 \pmod{853}$

$7^2 \equiv 49 \equiv 49 \pmod{853}$

$7^4 \equiv (7^2)^2 \equiv (49)^2 \equiv 2401 \equiv 695 \pmod{853}$

$7^8 \equiv (7^4)^2 \equiv (695)^2 \equiv 483025 \equiv 227 \pmod{853}$

$7^{16} \equiv (7^8)^2 \equiv (227)^2 \equiv 51529 \equiv 349 \pmod{853}$

$7^{32} \equiv (7^{16})^2 \equiv (349)^2 \equiv 121801 \equiv 675 \pmod{853}$

$7^{64} \equiv (7^{32})^2 \equiv (675)^2 \equiv 455625 \equiv 123 \pmod{853}$

$7^{128} \equiv (7^{64})^2 \equiv (123)^2 \equiv 15129 \equiv 628 \pmod{853}$

$7^{256} \equiv (7^{128})^2 \equiv (628)^2 \equiv 394384 \equiv 298 \pmod{853}$

$327 = 256 + 71$

$= 256 + 64 + 7$

$= 256 + 64 + 4 + 3$

$= 256 + 64 + 4 + 2 + 1.$

binary expansion of 327

Now we use the binary expansion of 327 to compute

$7^{327} = 7^{256+64+4+2+1}$

$= 7^{256} . 7^{64} . 7^{4} . 7^{2} . 7^{1}$

$\equiv 298 \cdot 123 \cdot 695 \cdot 49 \cdot 7 \pmod{853}$

$\equiv 828 . 695. 49 . 7 \pmod{853}$

$\equiv 538 . 49 . 7 \pmod{853}$

$\equiv 772 . 7 \pmod{853}$

$7^{327} \equiv 286 \pmod{853}$ We are done!!! ☺

You can compute it directly-

$7^{327} = 22236123868955180582 \underbrace{\ldots\ldots\ldots\ldots}_{\text{237 digits omitted}} 32584937995509879543\ 237$

$\equiv 286 \pmod{853}.$

It is completely infeasible to compute a^k exactly when k has, say, 20 digits.

Algorithm 1 (Successive Squaring to Compute $a^k \pmod{m}$).

The following steps compute the value of $a^k \pmod{m}$:

1. **Write k as a sum of powers of 2 ,**

$$k = u_o + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + \cdots + u_r \cdot 2^r,$$

where each u_i is either 0 or 1.

(This is called the binary expansion of k.)

2. **Make a table of powers of a modulo m using successive squaring.**

$$\begin{array}{llll}
a^1 & & & \equiv A_0 \pmod{m} \\
a^2 & \equiv (a^1)^2 & \equiv (A_0)^2 & \equiv A_1 \pmod{m} \\
a^4 & \equiv (a^2)^2 & \equiv (A_1)^2 & \equiv A_2 \pmod{m} \\
a^8 & \equiv (a^4)^2 & \equiv (A_2)^2 & \equiv A_3 \pmod{m} \\
 & \vdots & & \\
(a)^{2^r} & \equiv (a^{2^{r-1}})^2 & \equiv (A_{r-1})^2 & \equiv A_r \pmod{m}
\end{array}$$

Note that to compute each line of the table you only need to take the number at the end of the previous line, square it, and then reduce it modulo m. Also note that the table has r + 1 lines, where r is the highest exponent of 2 appearing in the binary expansion of k in Step 1.

3. The product

$$A_0^{u0}.A_1^{u1}.\ A_2^{u2} \ldots \quad A_r^{ur} \pmod{m}$$

will be congruent to $a^k \pmod{m}$. Note that all the u_i's are either 0 or 1, so these numbers are really the product of those A_i's for which u_i equals 1.

Proof- we compute

$$a^k = a^{(uo + u1 \cdot 2 + u2 \cdot 4 + u3 \cdot 8 + \cdot\cdot\cdot + ur \cdot 2^r)} \quad \text{(using step 1)}$$

$$a^k = (a^1)^{u0} . (a^2)^{u1} . (a^4)^{u2} \ \ldots \ (a^{2^r})^{ur}$$

$$\equiv (A_0)^{u0} (A_1)^{u1} \ldots \quad (A_r)^{ur} \pmod{m} \quad \text{(using step 2)}$$

1. Use the method of successive squaring to compute each of the following powers.

(a) 5^{13} (mod 23) **(b) 28^{749} (mod 1147)**

k/2	Q	R
13/2	6	1
6/2	3	0
3/2	1	1
1/2	0	1

(a)Answer- a = 5, k = 13, m = 23.

***step1*- *W*rite k as sum of powers of 2.**

$$k = (1101)_2$$

$$= 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0$$

$$(u_0 = 1, u_1 = 0, u_2 = 1, u_3 = 1)$$

$$= 8 + 4 + 1.$$

***step2*- Make a table of powers of 5 modulo 23 using successive squaring.**

$$5^1 \equiv 5 \equiv 5 \pmod{23}$$

$$5^2 \equiv 25 \equiv 2 \pmod{23}$$

$$5^4 \equiv (5^2)^2 \equiv (2)^2 \equiv 4 \equiv 4 \pmod{23}$$

$$5^8 \equiv (5^4)^2 \equiv (4)^2 \equiv 16 \equiv 16 \pmod{23}$$

***step3*-** $5^{13} = 5^{8+4+1}$

$$= 5^8 . 5^4 . 5^1$$

$$\equiv (16.4).5 \pmod{23} \qquad \text{(using step 2)}$$

$$\equiv 18.5 \pmod{23} \qquad (64 \equiv 18 \pmod{23})$$

$$5^{13} \equiv 21 \pmod{23} \qquad (90 \equiv 21 \pmod{23})$$

(b) **answer- a = 28, k = 749, m = 1147.**

***step1*- *W*rite k as sum of powers of 2.**

$k = (1011101101)_2$

$= 2^9 + 2^7 + 2^6 + 2^5 + 2^3 + 2^2 + 1$

$= 512 + 128 + 64 + 32 + 8 + 4 + 1$

***step2*- Make a table of**

powers of 28 modulo 1147

using successive squaring.

$28^1 \equiv 28 \equiv 28 \pmod{1147}$

$28^2 \equiv 784 \equiv 784 \pmod{1147}$

$28^4 \equiv (28^2)^2 \equiv (784)^2$

$\equiv 614656 \equiv 1011 \pmod{1147}$

K/2	Q	R
749/2	374	1
374/2	187	0
187/2	93	1
93/2	46	1
46/2	23	0
23/2	11	1
11/2	5	1
5/2	2	1
2/2	1	0
1/2	0	1

$28^{8} \equiv (28^{4})^{2} \equiv (1011)^{2} \equiv 1022121 \equiv 144 \pmod{1147}$

$28^{16} \equiv (28^{8})^{2} \equiv (144)^{2} \equiv 20736 \equiv 90 \pmod{1147}$

$28^{32} \equiv (28^{16})^{2} \equiv (90)^{2} \equiv 8100 \equiv 71 \pmod{1147}$

$28^{64} \equiv (28^{32})^{2} \equiv (71)^{2} \equiv 5041 \equiv 453 \pmod{1147}$

$28^{128} \equiv (28^{64})^{2} \equiv (453)^{2} \equiv 205209 \equiv 1043 \pmod{1147}$

$28^{256} \equiv (28^{128})^{2} \equiv (1043)^{2} \equiv 1087849 \equiv 493 \pmod{1147}$

$28^{512} \equiv (28^{256})^{2} \equiv (493)^{2} \equiv 243049 \equiv 1032 \pmod{1147}$

step3- $28^{749} = 28^{512 + 128 + 64 + 32 + 8 + 4 + 1}$

$= 28^{512} . 28^{128} . 28^{64} . 28^{32} . 28^{8} . 28^{4} . 28^{1}$

$\equiv (1032. 1043). (453. 71). (144. 1011). 28 \pmod{1147}$

$\equiv (490. 47). (1062.28) \pmod{1147}$

$\equiv 90. 1061 \pmod{1147}$

$28^{749} \equiv 289 \pmod{1147}$

≥

≥

2. The method of successive squaring described in the text allows you to compute $a^k \pmod{m}$ quite efficiently, but it does involve creating a table of powers of a modulo m.

(a) Show that the following algorithm will also compute the value of $a^k \pmod{m}$. It is a more efficient way to do successive squaring, well-suited for implementation on a computer.

(1) Set $b = 1$

(2) Loop while $k \geq 1$

(3) If k is odd, set $b = a.b \pmod{m}$

(4) Set $a = a^2 \pmod{m}$

(5) Set $k = k/2$ (round down if k is odd)

(6) End of Loop

(7) Return the value of b (which equals $a^k \pmod{m}$)

(b) Implement the above algorithm on a computer using the computer language of your choice.

(c) Use your program to compute the following quantities: (i) $2^{1000} \pmod{2379}$

(ii) $567^{1234} \pmod{4321}$ (iii) $47^{258008} \pmod{1315171}$.