WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

Revision Questions

May 16, 2024

Powers Modulo m and Successive Squaring

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

Follow the following steps to compute the value of $a^k \pmod m$.

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

   $$k = \beta_0 \cdot 2^0 + \beta_1 \cdot 2^1 + \beta_2 \cdot 2^2 + \beta_3 \cdot 2^3 + \beta_4 \cdot 2^4 + \cdots + \beta_r \cdot 2^r$$

   where each u_i is either 0 or 1.

2. Perform successive squaring as follows

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

Algorithm (conti...)

Notice that it is easy to compute the above sequence of values since each number in the sequence is the square of the preceding one. Note also that the table has $r + 1$ lines, where r is the highest exponent of 2 in the binary expansion of k in Step 1.

3. Thus, $a^k \equiv A_0^{\beta_0} \cdot A_1^{\beta_1} \cdot A_2^{\beta_2} \cdot A_3^{\beta_3} \cdot \cdots \cdot A_r^{\beta_r} \pmod{m}$

   Note that all the β_i's are either 0 or 1. Thus, this number is a product of those A_i's for which β_i equals 1.

Example 1

Use successive squaring to compute $7^{35} \bmod 27$.

Solution

$$35 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

$$7^1 \equiv 7 \bmod 27$$

$$7^2 \equiv 22 \bmod 27$$

$$7^4 \equiv 25 \bmod 27$$

$$7^8 \equiv 4 \bmod 27$$

$$7^{16} \equiv 16 \bmod 27$$

$$7^{32} \equiv 13 \bmod 27$$

$$\text{Thus } 7^{35} = \left(7^1 \cdot 22^1 \cdot 25^0 \cdot 4^0 \cdot 16^0 \cdot 13^1\right) \bmod 27$$

$$= (7 \cdot 22 \cdot 13) \bmod 27$$

$$= 4 \bmod 27$$

Example 2

Compute $27^{234} \bmod 313$

Solution

$234_{10} = 11101010_2$. Now,

$$27^1 \equiv 27 \bmod 313$$
$$27^2 \equiv 103 \bmod 313$$
$$27^4 \equiv 280 \bmod 313$$
$$27^8 \equiv 150 \bmod 313$$
$$27^{16} \equiv 277 \bmod 313$$
$$27^{32} \equiv 44 \bmod 313$$
$$27^{64} \equiv 58 \bmod 313$$
$$27^{128} \equiv 234 \bmod 313$$

Thus $27^{234} \bmod 313 = (234 \times 58 \times 44 \times 150 \times 103) \bmod 313$

$$= 1 \bmod 313$$

Example 3

Compute $5^{56} (\mathrm{mod}\, 57)$ by the method of successive squaring. Is 57 prime?

Solution

$56_{10} = 111000_2$

Thus $5^1 \equiv 5 (\mathrm{mod}\, 57)$

$5^2 \equiv 25 (\mathrm{mod}\, 57)$

$5^4 \equiv 55 (\mathrm{mod}\, 57)$

$5^8 \equiv 4 (\mathrm{mod}\, 57)$

$5^{16} \equiv 16 (\mathrm{mod}\, 57)$

$5^{32} \equiv 28 (\mathrm{mod}\, 57)$

Thus $5^{56} \equiv (28 \times 16 \times 4) (\mathrm{mod}\, 57)$

$\equiv 25 (\mathrm{mod}\, 57)$

Therefore, by Fermat's little theorem, 57 is not prime.

Example 4

Compute $7^{42} (\mathrm{mod}\, 43)$ by the method of successive squaring. Is 43 prime?

Solution

$42_{10} = 101010_2$

$$7^1 \equiv 7 (\mathrm{mod}\, 43)$$
$$7^2 \equiv 6 (\mathrm{mod}\, 43)$$
$$7^4 \equiv 36 (\mathrm{mod}\, 43)$$
$$7^8 \equiv 6 (\mathrm{mod}\, 43)$$
$$7^{16} \equiv 36 (\mathrm{mod}\, 43)$$
$$7^{32} \equiv 6 (\mathrm{mod}\, 43)$$

Thus $7^{42} \equiv (6 \times 6 \times 6) (\mathrm{mod}\, 43)$

$= 1 (\mathrm{mod}\, 43)$

Thus, by Fermat's little theorem, 43 is likely to be prime.

Revision Questions 1

1. Compute $7^{8312} (\mathrm{mod}\ 8313)$ by the method of successive squaring. Is 8313 prime?
2. Compute $5^{8512} (\mathrm{mod}\ 8513)$ by the method of successive squaring. Is 8513 prime?
3. Find all incongruent solutions to each of the following congruences.

   a) $6x \equiv 3 (\mathrm{mod} 15)$
   b) $66x \equiv 100 (\mathrm{mod} 121)$
   c) $x^2 \equiv 2 \mathrm{\ mod\ } 7$
   d) $x^2 \equiv 3 \mathrm{\ mod\ } 7$

4. Determine the number of incongruent solutions for each of the following congruences.

   a) $72x \equiv 94 (\mathrm{mod}\ 200)$
   b) $4183x \equiv 5781 (\mathrm{mod}\ 15087)$
   c) $1537x \equiv 100 (\mathrm{mod}\ 6731)$

Revision Questions

5. Find the following multiplicative inverses

   a) $7^{-1} \bmod 20$

   b) $23^{-1} \bmod 715$

   c) $13^{-1} \bmod 715$

   d) $313^{-1} \bmod 715670$

6. Find $\phi(9800)$

7. Find the remainder when 7^{1002} is divided by 29.

Solution