

MA 341
e-TH ROOTS (MOD m)

We have learned how to take the e -th power of a number ($\text{mod } m$). I.e. how to compute

$$a^e \pmod{m}$$

This can be done using the method of successive squaring, which is very efficient.

Here we address the issue of whether or not one can go the other way, i.e. compute an e -th root ($\text{mod } m$). We first note that when a is an integer, and $e > 1$, then $a^{(1/e)}$ is NOT an integer, so we can't just take e -roots as we do in the real numbers.

Rather we ask if we are given b , can we solve:

$$x^e \equiv b \pmod{m}$$

In particular if $a^e \equiv b \pmod{m}$ can we get $x \equiv a \pmod{m}$ back as a solution ?

In general the equation $x^e \equiv b \pmod{m}$ can have no solutions, one solution, or more than one solution.

Examples:

- a) $x^2 \equiv -1 \pmod{3}$ has no solutions.
- b) If p, q distinct primes we saw $x^2 \equiv 1 \pmod{pq}$ has 4 solutions.

Here we are interested in a special case where there is **exactly one solution**.

Proposition: If $(b, m) = 1$ and $(e, \phi(m)) = 1$ then

$$x^e \equiv b \pmod{m}$$

has exactly one solution ($\text{mod } m$).

Proof: We first show there is a solution and give a formula to find it. Since $(e, \phi(m)) = 1$ we can find integers u, v satisfying

$$eu + \phi(m)v = 1$$

Reducing this equality ($\text{mod } \phi(m)$) gives $eu \equiv 1 \pmod{\phi(m)}$. Let $d \equiv u \pmod{\phi(m)}$.

We claim $x \equiv b^d \pmod{m}$ is a solution to $x^e \equiv b \pmod{m}$.

Since $(b, m) = 1$, by Euler's theorem we know $b^{\phi(m)} \equiv 1 \pmod{m}$. Since $de \equiv ed \equiv 1 \pmod{\phi(m)}$, we we can write $de = 1 + \phi(m) \cdot k$ for some integer k . But then we have

$$(b^d)^e \equiv b^{de} \equiv b^{1+\phi(m) \cdot k} \equiv b \cdot (b^{\phi(m)})^k \equiv b \cdot 1 \equiv b \pmod{m}$$

So indeed $b^d \pmod{m}$ is a solution.

We can see this is the only solution by using $eu + \phi(m)v = 1$. Suppose x satisfies $x^e \equiv b \pmod{m}$. Then:

$$x \equiv x^{(eu+\phi(m)v)} \equiv x^{(eu)}x^{\phi(m)v} \equiv (x^e)^u \equiv b^u \pmod{m}$$

Note we used Euler's theorem $x^{\phi(m)} \equiv 1 \pmod{\phi(m)}$. So $x \equiv b^u \equiv b^d \pmod{m}$ since $u \equiv d \pmod{m}$ Hence $b^d \pmod{m}$ is the only solution.

SEE REVERSE FOR SOME COMMENTS ON THE ABOVE

Note that if we are given (m, e) then it is computationally easy to compute

$$a^e \pmod{m}$$

However If $a^e \equiv b \pmod{m}$ and we only know b and m and NOT a , then in order to solve

$$x^e \equiv b \pmod{m}$$

we need to find d satisfying $ed \equiv 1 \pmod{\phi(m)}$. But this involves first finding $\phi(m)$. In order to find $\phi(m)$ we need to FIRST FACTOR m into a product of prime numbers. Since factoring a large number m is extremely difficult it is computationally very difficult to find d even if we know (m, e) .

Using the above facts leads to public key cryptography and unbreakable codes. This is the theory of how to send secret messages to anyone, even someone you have never met, i.e. via email, such that no one will be able to decipher the message if it is intercepted.

We will learn about more about cryptography in Chapter 9 of our book.