1

What are all the primitive roots modulo 13?

a	1	2	3	4	5	6	7	8	9	10	11	12
order of a mod 13	1	12	3	6	4	12	12	4	3	6	12	2

2, 6, 7, and 11 are all the primitive roots modulo 13.

-Nick

2

g=2

g^0=1(mod 13)
g^1=2(mod 13)
g^4=3(mod 13)

g^2=4(mod 13)
g^9=5(mod 13)
g^5=6(mod 13)

g^11=7(mod 13)
g^3=8(mod 13)
g^8=9(mod 13)

g^10=10(mod 13),
g^7=11(mod 13),
g^6=12(mod 13)

-Maggie

3

G=2

the order of g^2 or 2^2 is 6, Which is 2's order 12 / 2

the order of g^3 or 2^3 is 4, Which is 2's order 12 / 3

In general, if g is a primitive root mod p, the order of g^l is the order of g divided by the gcd of the order of g and i

In other words, (phi(n)) / gcd{ phi(n), i }

Cian

4

Combining Maggie and Nick's work we see that the primitive roots expressed as 2^i are: 2=2^1, 6=2^5, 7=2^(11), 11=2^7.

Using Cian's work, we see that this makes sense because a primitive root will have order = phi(n) and hence gcd(phi(n),i) has to equal 1 for the order of g^i not be smaller than phi(n).

The powers i for which i is relatively prime to phi(n)=12 are 1, 5, 7, 11.

5

a=1,3,4,5,9

Even powers of the primitive root are the squares.

6

a. 5 quadratic residue, 5 non-residue (0 is not counted).

b. 6 quadratic residue, 6 non-residue.

c. (p-1)/2 quadratic residue, (p-1)/2 nonresidue.