1

What are all the primitive roots modulo 13?

The primitive roots are 2, 6, 7, and 11.

We can find this by checking their orders and making sure they are equal to phi(13) = 12.

This is #1 of the pre-class activity. -Nick

There are better ways to code this, but I liked that I could fit it on one line

We see that only 2, 6, 7, and 11 have an order of 12.

- Miah :)

Find a primitive root modulo 18.

phi(18) = 6 so for a candidate primitive root, r, we must check $r^{(6/2)}=r^3$ and $r^{(6/3)}=r^2$ and if neither equals 1 then r is a primitive root.

A primitive root must be relatively prime to the modulus (18) so 0, 1, 2, 3, 4 cannot work.

The first potential candidate is 5.

$5^3 \equiv -1 \pmod{18}$ and $5^2 \equiv 7 \pmod{18}$

Neither power yielded 1 so 5 is a primitive root modulo 18.

-Nick

3

a. If a^i=a^j (mod n), then (without loss of generality, assume i>j), a^(i-j)*a^j = a^j -> a^(i-j)=1 (mod n) (because a is relatively prime to n to define order).

This means order of a, which is k, divides i-j.

b. Since i-j is not divisible by k for i, j between 0 and k-1, those a^i, a^j's will be all different.

Theorem 1: If g is a primitive root modulo n, then any integer relatively prime to n is congruent to g^i modulo n for some i. Conversely, if g is an integer for which any integer relatively prime to n is congruent to g^i for some i, then g is a primitive root.

proof: Suppose g is a primitive root. Then g has order $\phi(n)$. Using the above problem, this says that $g^0, g^1, \ldots, g^{\phi(n)-1}$ are all different modulo n. Also note that g^i are all relatively prime to n if g is. But there are only $\phi(n)$ residue classes which are relatively prime to n, so the powers of g must cover all these residue classes.

Suppose now that g is an integer such that every integer relatively prime to n is congruent to g^i for some i. Suppose the order of g is k. Then, from the above problem, there are k different integers modulo n which are of the form g^i. All of these g^i's are relatively prime to n. But there are $\phi(n)$ integers modulo n which are relatively prime to n. Therefore, $k = \phi(n0$ and g is a primitive root.

$\square$

4

phi(10) =4 and those numbers are 1,3,7,9

so the power 1 through 4 of 3 and 7 should result in the classes of 1,3,7,9 in some order. We see that

3^1 == 3
3^2 == 9
3^3 == 7
3^4 == 1

7^1 == 7
7^2 == 9
7^3 == 3
7^4 == 1

and so 3 and 7 can be expressed in terms of each other

Cian

5

a. $2^{10}=1$ and no smaller power of 2 equals 1.

b. order of $2^4=5$ because $(2^4)^5=2^{(20)}=1$

order of $2^7=10$ because $(2^7)^i = 2^{(7*i)}$ becomes 1 only if $7*i$ has a 10 factor, and that's only when $i=10$

Similar to 2^7 reasoning: order of $2^9=10$

c. For 2^k to be a primitive root, there should be no "piece of 10" inside 10, so no common factor between k and 10. Those k's are 1, 3, 7, 9. (This is seen in problem 4.)

6

This is problem 6 in pre-class.

7

a. If a=x^2, then a^((p-1)/2)=x^(p-1)=1 (mod p) by Fermat's Little Theorem. (Oops.. this doesn't require the primitive root actually. You can do it with that too. Let a=g^(2k) then.)

b. If a is non-residue, then a=g^(2k+1). So a^((p-1)/2) = g^(p-1)k *g^((p-1)/2). Then (g^(p-1))^k=1 by FLT so that part goes away.

But the second piece, g^((p-1)/2) does not equal 1 because order of g is p-1 and (p-1)/2<p-1.

c. Let x=a^(p-1)/2. Then x^2=1 because a^(p-1)=1. So x=+-1 because those are the only solutions for x^2=1 mod p.

Also check if x^2=2, x^2=3 and x^2=13 have solutions. (Do as many as possible as time permits.)

5^((101 - 1) / 2) = 5^50 = 1 mod 101. So x^2 = 5 mod 101 has two solutions. - Miah

7^(101-1)/2 is congruent to -1 mod 101 so there is no solution to x^2 == 7 mod 101. CIAN

I'm looking for a square root calculator modulo n online, but that doesn't seem to exist. Sigh...

Another way: 2 is a primitive root, so it cannot be a square (problem 1).

2^50 = -1 (mod 101) so x^2 = 2 has no solution mod 101. -nick

13^50=1(mod 101), so x^2=13(mod 101) has 2 solutions -Maggie

3?

3^50 = -1 mod 101. No solution

Last page