Investigations on Primitive Roots and Quadratic Residues
Pre-class, Week 9

In this pre-class, we will investigate two topics: primitive roots and quadratic residues.

Primitive roots modulo n are the elements whose orders are the maximum possible value. We know that any a relatively prime to n satisfies $a^{\phi(n)} \equiv 1 \pmod{n}$. For most a's, $\phi(n)$ is not the order, but for some select a's, it is. These a's are called the *primitive roots* modulo n.

1. What are all the primitive roots modulo 13? (Note: Use $(-a)^k \equiv (-1)^k a^k \pmod{n}$ to find the order of half of the numbers without much work.)

a	1	2	3	4	5	6	7	8	9	10	11	12
order	1	12	3	6	4	12	12	4	3	6	12	2
		☆				☆	☆				☆	

2. Pick one of your primitive roots from problem 1, call it g. Write all non-zero elements modulo 13 in terms of powers of g.

n	1	2	3	4	5	6	7	8	9	10	11	12
g^n	2	4	8	3	6	12	11	9	5	10	7	1

3. Take the same g as above. What is the order of g^2 modulo 13? What about g^3? Or more generally g^i?

order of g^2 is $\frac{12}{2} = 6$

order of g^3 is $\frac{12}{3} = 4$

order of g^i is $\frac{12}{\gcd(12,i)}$

4. Take the same g as above. Can you find all other primitive roots modulo 13 in terms of g? How many such primitive roots do you have?

$$\frac{12}{\gcd(12,i)} = 12 \text{ iff } \gcd(12,i) = 1$$

The number of primitive roots mod 13 is $\phi(12)$
$= \phi(\phi(13))$

Over →

We have tools to solve linear congruence equations, including systems, but we have yet to learn how to solve a quadratic congruence equation. One important step in working with a quadratic equation is finding a "square root" which will translate into finding for which a, $x^2 \equiv a \pmod{n}$ has a solution.

5 a. Find all a for which $x^2 \equiv a \pmod{11}$ has a solution. (Hint: It might be easier to think about this as finding the squares of all numbers modulo 11.)

X	1	2	3	4	5	6	7	8	9	10
X²% 11	1	4	9	5	3	3	5	9	4	1

b. We know that 2 is a primitive root modulo 11. We also know that any element modulo 11 can be expressed as 2^i. Express all the elements as 2^i and using your results for part a, come up with an easy test for which a's are squares.

a	1	2	3	4	5	6	7	8	9	10
2^i	2^{10}	2^1	2^8	2^2	2^4	2^9	2^7	2^3	2^6	2^5
square?	Y	N	Y	Y	Y	N	N	N	Y	N
i%2	0	1	0	0	0	1	1	1	0	1

Let p be a prime. We call the relatively prime squares modulo p *quadratic residues* modulo p. In other words, a is a quadratic residue if $\gcd(a, p) = 1$ and $x^2 \equiv a \pmod{p}$ has a solution. If $x^2 \equiv a \pmod{p}$ does not have a solution, then a is a *quadratic nonresidue.*

For example, modulo 17, 8 is a quadratic residue because $5^2 \equiv 8 \pmod{17}$ while 3 is a quadratic nonresidue since there is no x whose square is congruent to 3 modulo 17.

6 a. How many quadratic residues are there modulo 11? How many quadratic non-residues are there?

5

5

b. What about modulo 13?

6 & 6

c. Can you make a conjecture as to the number of quadratic residues and nonresidues for an odd prime?

$\frac{p-1}{2}$ & $\frac{p-1}{2}$