Math 302 Worksheet 8: Powers Modulo n

Math 302: Introduction to Proofs via Number Theory

Instructor: Professor Stephanie Treneer, Stephanie.Treneer@wwu.edu

Beginning with an integer a, consider its powers $a, a^2, a^3, \ldots$ modulo n. Look for patterns in the following tables:

Mod 3			
a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
2	1	2	1

Mod 5					
a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0
1	1	1	1	1	1
2	4	3	1	2	4
3	4	2	1	3	4
4	1	4	1	4	1

Mod 7							
a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2
4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4
6	1	6	1	6	1	6	1

Mod 11											
a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1	2	4
3	9	5	4	1	3	9	5	4	1	3	9
4	5	9	3	1	4	5	9	3	1	4	5
5	3	4	9	1	5	3	4	9	1	5	3
6	3	7	9	10	5	8	4	2	1	6	3
7	5	2	3	10	4	6	9	8	1	7	5
8	9	6	4	10	3	2	5	7	1	8	9
9	4	3	5	1	9	4	3	5	1	9	4
10	1	10	1	10	1	10	1	10	1	10	1

Problem 8.1. Explain the repetition that occurs in the rows of the tables. Why is it periodic? Is the period related to the modulus?

Problem 8.2. Make a conjecture about the values of a and k for which $a^k \equiv 1 \pmod{p}$ for p prime.

Problem 8.3. Make a table for the powers of a modulo 9. Remember that you can make the work easier by "modding as you go" (that is, reduce to the least nonnegative residue whenever you have a number larger than 8).

Mod 9									
a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
0									
1									
2									
3									
4									
5									
6									
7									
8									

Problem 8.4. Now consider whether the behavior of powers modulo primes also holds for composite moduli. Look at the mod 9 table above.

(a) Do the patterns you observed for moduli 3, 5, 7, and 11 also hold modulo 9? If not, what is different?

(b) Explain the rows of zeros you see.

(c) For which values of a and k is $a^k \equiv 1 \pmod 9$? How does the result here relate to the result for primes?