Worksheet - Primitive Roots II

1 What is $28^{60}$ modulo 61? Prove that 28 is not a primitive root modulo 61.

2 Prove, in as efficient a manner as possible, that 2 is a primitive root modulo 61.
3 What powers of 2 will satisfy the congruence $x^3 \equiv 1 \pmod{61}$?

4 What powers of 2 will satisfy the congruence $x^5 \equiv 1 \pmod{61}$.

5 You are told that $17^3 \equiv 33 \pmod{61}$. Begin with 17, multiply 17 by each of the powers of 2 from 3, and cube the result modulo 61. List the resulting residues.

6 You are told that $22^5 \equiv 47 \pmod{61}$. Use your answers from 4 to efficiently solve the congruence $x^5 \equiv 47 \pmod{61}$. 

7 List the exponents, $E$, satisfying $2^E$ is a quadratic residue modulo 61.

8 List the exponents, $E$, satisfying $2^E$ is a cubic residue modulo 61.
When solving the congruence $x^2 \equiv 48 \pmod{61}$ using the residue solving algorithm, we begin by writing $60 = 2^k m$. and computing $r \equiv 48^{(m+1)/2} \pmod{61}$ and $n \equiv 48^m \pmod{61}$. What are the values of $k, m$ and $r, n$?

Since $n$ was not congruent to 1 modulo 61, we must let $z$ = any non-quadratic residue modulo 61. Pick a value for $z$.

Compute $c \equiv z^m \pmod{61}$. Find $k'$ so that $\text{ord}_{61}(n) = 2^{k'}$. Let $b \equiv c^{2^{k'-1}} \pmod{61}$ and set $r' \equiv br \pmod{61}$, $c' \equiv b^2 \pmod{61}$, $n' \equiv c'n \pmod{61}$.

What are the values of $z, c, b, r', n'$?

Complete the algorithm to find a solution to $x^2 \equiv 48 \pmod{61}$. Then find all solutions to $x^2 \equiv 48 \pmod{61}$.

What powers of 2 are the solutions? What power of 2 is 48? (all modulo 61, of course.)