Homework 5
(Cyclic U_n, powers modulo n, and quadratic residues.)
Due Monday, November 4 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet**.

(1) Recall that an element $[a] \in U_n$ is a primitive root if and only if $a^{\phi(n)/q} \not\equiv 1 \pmod{n}$ for each prime q dividing $\phi(n)$.

(a) If $[g]$ is a primitive root modulo 37, which of the classes $[g^2], [g^3], [g^4], \ldots, [g^8]$ are primitive roots modulo 37?

$[g^5]$ and $[g^7]$ are primitive roots, and none of the others are. We have that

$$(g^2)^{36/2} = g^{36} \equiv_{37} 1$$
$$(g^3)^{36/3} = g^{36} \equiv_{37} 1$$
$$(g^4)^{36/2} = (g^{36})^2 \equiv_{37} 1^2 = 1$$
$$(g^6)^{36/2} = (g^{36})^3 \equiv_{37} 1^3 = 1$$
$$(g^8)^{36/2} = (g^{36})^4 \equiv_{37} 1^4 = 1$$

but

$$(g^5)^{36/2} = (g^4)^{36/2} g^{36/2} \equiv_{37} g^{36/2} \not\equiv_{37} 1$$
$$(g^5)^{36/3} = (g^3)^{36/3} (g^2)^{36/3} \equiv_{37} g^{24} \not\equiv_{37} 1$$

and

$$(g^7)^{36/2} = (g^6)^{36/2} g^{36/2} \equiv_{37} g^{36/2} \not\equiv_{37} 1$$
$$(g^7)^{36/3} = (g^6)^{36/3} (g)^{36/3} = (g^{36})^2 g^{36/3} \equiv_{37} g^{36/3} \not\equiv_{37} 1$$

(b) Find all values n, where $6 \leq n \leq 16$, for which [3] is a primitive root modulo n.

First, note that for $6 \leq n \leq 16$, the group U_n is cyclic only for $n = 6, 7, 9, 10, 11, 13, 14$. From these, we know that [3] is only a unit mod n for $n = 7, 10, 11, 13, 14$.

- Since $\phi(7) = 6$ and

$$3^2 \equiv_7 2$$
$$3^3 \equiv_7 6$$

[3] is a primitive root mod 7.

- Since $\phi(10) = 4$ and

$$3^2 \equiv_{10} -1$$

[3] is a primitive root mod 10.

- Since $\phi(11) = 10$ and
$$3^2 \equiv_{11} -2$$
$$3^5 \equiv_{11} 3(-2)^2 = 3 \cdot 4 \equiv_{11} 1$$
[3] is not a primitive root mod 10.
- Since $\phi(13) = 12$ and
$$3^2 \equiv_{13} -4$$
$$3^3 \equiv_{13} 3(-4) = -12 \equiv_{13} 1$$
[3] is not a primitive root mod 13.
- Since $\phi(14) = 6$ and
$$3^2 \equiv_{14} -5$$
$$3^3 \equiv_{14} 3(-5) = -15 \equiv_{14} -1$$
[3] is a primitive root mod 14.

(2) Read the proof of Theorem 6.10 on p.107 of the text. Then prove the following statement:
If $e \geq 3$, then $U_{2^e} = \{[\pm 3^i] \mid 0 \leq i < 2^{e-2}\}$.

Lemma 1. $2^{n+2} || 3^{2^n} - 1$ for all $n \geq 1$.

Proof of Lemma. We induct on n. When $n = 1$, we have that $2^3 || 9 - 1$. Suppose $2^{n+2} || 3^{2^n} - 1$ for some $n \geq 1$. Then
$$3^{2^{n+1}} - 1 = (3^{2^n})^2 - 1 = (3^{2^n} - 1)(3^{2^n} + 1).$$
Since $2^{n+2} || 3^{2^n} - 1$ and $2 || 3^{2^n} + 1$ (since 3 to an even power is also a power of 9, so $3^{2^n} \equiv_4 1$), we have that $2^{n+3} || 3^{2^{n+1}} - 1$ as desired. □

To prove the theorem, carefully imitate the proof of Theorem 6.10.

(3) For each of the following, find all of the solutions x satisfying the congruence.

(a) $x^5 \equiv 2 \pmod{37}$ (Hint: 2 is a primitive root modulo 37.)
Since [2] is a primitive root mod 37, we have that for each solution x, $[x] = [2^i]$ for some i. So we can rewrite the given congruence as
$$(2^i)^5 \equiv_{37} 2^1.$$
Since [2] is a primitive root, it has order $\phi(37) = 36$ and so the congruence above has a solution i if and only if
$$5i \equiv_{36} 1.$$
Since $\gcd(5, 37) = 1 \mid 1$, we have exactly 1 solution. By inspection, we see that $i \equiv_7 29$. So $[x] = [2^29]$ is the only solution.

(b) $x^2 \equiv 5 \pmod{88}$ This congruence has a solution if and only if the system
$$x^2 \equiv 5 \pmod{8}$$
$$x^2 \equiv 5 \pmod{11}$$
has a solution. However, $x^2 \equiv 5 \pmod{8}$ has no solution.

(4) Consider the set of quadratic residues mod 30, Q_{30}.

(a) For each $[a] \in Q_{30}$, how many elements $[t] \in U_{30}$ are such that $t^2 \equiv a \pmod{30}$?
Since $30 = 2 \cdot 3 \cdot 5$ and $30 \equiv 2 \pmod 4$, there are $2^{3-1} = 4$ such elements.

(b) Use your result from part (a) to find all elements in Q_{30} without squaring every element in U_{30}. We know, then, that there are $\phi(30)/4 = 8/4 = 2$ elements. Squaring the first two elements in U_{30} yields

$$1^2 \equiv 1$$

$$7^2 \equiv 19$$

So $Q_{30} = \{[1], [19]\}$.

(a) Show that $(p-b)^2 \equiv b^2 \pmod p$.
We have that $(p-b)^2 = p^2 - 2pb + b^2 \equiv b^2 \pmod p$.

(b) Let p be an odd prime. Show that there are exactly $(p-1)/2$ quadratic residues modulo p and exactly $(p-1)/2$ nonresidues modulo p. Note that $U_p = \{1, 2, 3, \ldots, p-3, p-2, p-1\}$. Since p is prime, Q_p has $\phi(p)/N = (p-1)/2$ elements. Since U_p has $p-1$ elements, $(p-1)/2$ are in Q_p, while the other $(p-1)/2$ are not.

Fun problem (will not be graded): A number a is called a cubic residue modulo p if it is congruent to a cube modulo p.

(1) Make a list of the cubic residues modulo 5, 7, and 11.

(2) If p is prime and $p \equiv 2 \pmod 3$, make a conjecture about which classes are cubic residues modulo p. Prove your conjecture.