Math 180B - Primitive Roots and Indices

1. Suppose $\mathbb{Z}/n\mathbb{Z}$ has a primitive root (n not necessarily prime). How many primitive roots does it have?

2. You are given the table of powers base 2, modulo 37.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^k	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36

k	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2^k	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1

Use the table to find all solutions to the following congruences.

(a) $12x \equiv 23$

(b) $5x^{23} \equiv 18$

(c) $x^{12} \equiv 11$

(d) $7x^{20} \equiv 34$

3. If r and r' are both primitive roots of the odd prime p, show that for $(a,p) = 1$,

$$ind_{r'}\ a = (ind_r\ a)(ind_{r'}\ r) \pmod{p-1}.$$

What other formula does this remind you of?

4. Given the congruence $x^3 \equiv a \pmod{p}$, where $p \geq 5$ is a prime and $(a,p) = 1$, prove the following:

(a) If $p \equiv 1 \pmod{6}$, then the congruence has either no solutions or three incongruent solutions modulo p.

(b) If $p \equiv 5 \pmod{6}$, then the congruence has a unique solution modulo p.

5. Suppose that g is a primitive root modulo p, where p is an odd prime.

(a) Let n be the order of g modulo p^2. Prove that $p - 1 \mid n$.

(b) Since g is a primitive root modulo p, we have $g^{p-1} = 1 + up$ for some $u \in \mathbb{Z}$. Suppose that $p \nmid u$. Use the binomial theorem to prove that

$$g^{t(p-1)} \equiv 1 \mod p^2 \iff p \mid t$$

(c) Explain why g is a primitive root modulo p^2.