MATH 104B, PRACTICE MIDTERM 1, WINTER 2003.

k	1	2	3	4	5	6	7	8	9	10
$3^k \pmod{31}$	3	9	27	19	26	16	17	20	29	25

k	11	12	13	14	15	16	17	18	19	20
$3^k \pmod{31}$	13	8	24	10	30	28	22	4	12	5

k	21	22	23	24	25	26	27	28	29	30
$3^k \pmod{31}$	15	14	11	2	6	18	23	7	21	1

1. (a). Find all primitive roots modulo 31.
(b). Find all primitive roots modulo 62.

2. Find all solutions x to $19^x \equiv 10 \pmod{31}$.

3. Let M be the maximum possible value of $\mathrm{ord}_m(a)$, where the maximum is taken over all elements a with $(a, m) = 1$. Show that if $(b, m) = 1$ then $\mathrm{ord}_m(b) | M$.

4. Show that If $(a, m) = (b, m) = 1$, there exists c with $\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$.

5. (a). By calculating a Legendre symbol, show that 3 is a quadratic non-residue modulo 257.
(b). Use table below to solve $x^2 \equiv 2 \pmod{257}$. You may leave the answer as a product.

k	1	2	4	8	16	32	64	128	256
$3^k \pmod{257}$	3	9	81	136	249	64	241	256	1