

**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.

**Solution.** From the table we see that the first power of 3 which is congruent to 1 modulo 31 is  $3^{30}$ , and so 3 is a primitive root modulo 31. The order of  $3^k$  is  $30/(k, 30)$  which equals 30 when  $k = 1, 7, 11, 13, 17, 19, 23, 29$ . This gives primitive roots 3, 17, 13, 24, 22, 12, 11, 21. As a check, note that we have found 8 primitive roots and  $\phi(30) = \phi(2)\phi(3)\phi(5) = 8$ .

(b). Find all primitive roots modulo 62.

We just look at each primitive root modulo 31 and if it is even we add on 31. This gives primitive roots modulo 62: 3, 17, 13, 55, 53, 43, 11, 21.

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

**Solution.** Since  $19 \equiv 3^4 \pmod{31}$  and  $10 \equiv 3^{14} \pmod{31}$ , we are trying to solve  $3^{4x} \equiv 3^{14} \pmod{31}$ . This is equivalent to  $4x \equiv 14 \pmod{30}$  and dividing by 2, this is equivalent to  $2x \equiv 7 \pmod{15}$ . The inverse of 2 modulo 15 is 8, and so we get  $x \equiv 56 \equiv 11 \pmod{15}$ . The solutions are those  $x$  of the form  $11 + 15y$ .

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

**Solution.** Choose  $a$  with order  $M$  modulo  $m$ , and let  $N = \text{ord}_m(b)$ . We claim that there exists an element of order  $[M, N]$ . Indeed, set  $k = (M, N)$ . Then  $c = b^k$  has order  $L = N/(k, N) = N/(M, N)$ . Now  $(L, M) = 1$  and we will show that  $ac$  has order  $ML$ . Once we have shown this then since  $ML = MN/(M, N) = [M, N]$ , this proves the claim. To show that  $ac$  has order  $ML$ , let  $J = \text{ord}_m(ac)$ . Then since  $(ac)^{LM} \equiv (a^M)^L (c^L)^M \equiv 1$ , we have  $J | LM$ . But  $1 \equiv ((ac)^J)^L \equiv a^{LJ} (c^L)^J \equiv a^{LJ}$  so  $M | LJ$ . Since  $(M, L) = 1$  this implies  $M | J$ . Similarly  $1 \equiv ((ac)^J)^M \equiv (a^M)^J c^{JM} \equiv c^{JM}$  so similarly  $L | JM$  so  $L | J$ . Hence  $[L, M] | J$  and  $[L, M] = J$ .

Now since  $M$  is the maximal order and we have obtained an element of order  $[M, N]$  we see that  $[M, N] = M$  which implies  $N | M$ .

4. Show that if  $(m, n) = 1$  and  $(x, mn) = 1$  then  $\text{ord}_{mn}(x) = [\text{ord}_m(x), \text{ord}_n(x)]$ .

**Solution.** Let  $o_d$  denote the order of  $x$  modulo  $d$ . Then  $x^{o_{mn}} \equiv 1 \pmod{mn}$  implies  $x^{o_{mn}} \equiv 1 \pmod{m}$  which implies  $o_m | o_{mn}$ . Similarly  $o_n | o_{mn}$ . But this implies  $[o_m, o_n] | o_{mn}$ . Conversely

$$x^{[o_m, o_n]} = (x^{o_m})^{[o_m, o_n]/o_m} \equiv 1 \pmod{m}, \quad x^{[o_m, o_n]} = (x^{o_n})^{[o_m, o_n]/o_n} \equiv 1 \pmod{n}$$

and so by the Chinese Remainder Theorem,  $x^{[o_m, o_n]} \equiv 1 \pmod{mn}$  and so  $o_{mn} | [o_m, o_n]$ . Hence  $o_{mn} = [o_m, o_n]$ .

5. (a). By calculating a Legendre symbol, show that 3 is a quadratic non-residue modulo 257.

**Solution.**

$$\left(\frac{3}{257}\right) = (-1)^{2 \cdot 256/8} \left(\frac{257}{3}\right) = \left(\frac{2}{3}\right) = -1$$

so 3 is 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

**Solution.** First we factorize  $257 - 1 = 256 = 2^8 = 2^8 s$  where  $s = 1$ . By working the standard algorithm below we get  $x \equiv 241 \cdot 64 \cdot 136 \cdot 2 \pmod{257}$ .

$i$	$x_i$	$b_i$	$\text{ord}_{257}(b_i)$
0	2	2	16
1	$136 \cdot 2$	$249 \cdot 2 \equiv 241$	4
2	$64 \cdot 136 \cdot 2$	$241 \cdot 241 \equiv 256$	2
3	$241 \cdot 64 \cdot 136 \cdot 2$	$256 \cdot 256 \equiv 1$	1

Here is an explanation of the algorithm. We are trying to solve

$$x^2 \equiv 2 \pmod{257}.$$

If we set  $x_0 = 2$  then this solves

$$x_0^2 \equiv 2 \cdot 2 \pmod{257}.$$

We want to find  $2^{-1/2} \pmod{257}$ . (This is convenient notation although one should bear in mind that there are two square roots of  $2^{-1}$  so it is not well defined. We don't care which one we find so we will use this notation.) Then  $x = 2^{-1/2} \cdot 2$  is clearly the solution. We try to find  $2^{-1/2}$  by finding  $2^{-1}$  and taking a square root. We cannot do this exactly, but we can do it approximately from the table. Since  $2^8 = 256 \equiv -1 \pmod{257}$ , we see that 2 has order 16 modulo 257. An approximate inverse of 2 is thus any other element of order 16. We find one in the table, it is 249. The table also gives us a square root of 249, this is 136. We have

$$2^{-1} \approx 249, \quad 2^{-1/2} \approx 136.$$

We set

$$x_1 \equiv 136 \cdot 2.$$

Then

$$x_1^2 \equiv 249 \cdot 2 \cdot 2 \equiv 241 \cdot 2 \pmod{257}.$$

To find the real solution we thus want to now multiply  $x_1$  by  $241^{-1/2}$ . We have gained because 241 has order 4 modulo 257 which is a smaller than the order of the previous error 2 which had order 16. The next step is of course to find an approximate value for  $241^{-1/2}$ . An approximate value of  $241^{-1}$  is given by any element of order 4, and 241 itself will work. Then our approximate value of  $241^{-1/2}$  is 64, and our new estimate for  $x$  is

$$x_2 \equiv 64 \cdot x_1.$$

This satisfies

$$x_2^2 \equiv 241 \cdot 241 \cdot 2 \equiv 256 \cdot 2 \equiv -2.$$

The final step is to multiply  $x_2$  by a square root of  $-1$ , and there is one in the table, namely 241.