> Math 418 : MAPLE Solution of Assignment #6 -- *Your NAME*

Problem 5(a): Making a power table of b in (Z/mZ)^x:

The following program powtab(b,m) constructs a list whose k-th element is b^k.
If gcd(b,m) > 1, then its returns FAIL.

```
> powtab := proc(b, m) local k, g, lst;
    g := modp(b, m); lst := [b];
    if igcd(b, m) ≠ 1 then return(FAIL) fi;
    for k while g ≠ 1 do;
      g := modp(g·b, m);
      lst := [op(lst), g]; od;
    return(lst); end;
```

```
powtab := proc(b, m)                                                    (1)
    local k, g, lst;
    g := modp(b, m);
    lst := [b];
    if igcd(b, m) <> 1 then return FAIL end if;
    for k while g <> 1 do g := modp(g * b, m); lst := [op(lst), g] end do;
    return lst
end proc
```

Note: In calculating the powers b^k mod m, remember to use the recursive formula
b^k = b^(k-1)*b mod m in place of the naive method b^k mod m.

The power tables for (b,m) = (2,11), (5,123) and (3,541) are as follows:

```
> pt1 := powtab(2, 11);
```

$$pt1 := [2, 4, 8, 5, 10, 9, 7, 3, 6, 1] \quad (2)$$

```
> pt2 := powtab(5, 123);
```

$$pt2 := [5, 25, 2, 10, 50, 4, 20, 100, 8, 40, 77, 16, 80, 31, 32, 37, 62, 64, 74, 1] \quad (3)$$

```
> pt3 := powtab(3, 541);
```

$$pt3 := [3, 9, 27, 81, 243, 188, 23, 69, 207, 80, 240, 179, 537, 529, 505, 433, 217, 110, 330, 449, 265, 254, 221, 122, 366, 16, 48, 144, 432, 214, 101, 303, 368, 22, 66, 198, 53, 159, 477, 349, 506, 436, 226, 137, 411, 151, 453, 277, 290, 329, 446, 256, 227, 140, 420, 178, 534, 520, 478, 352, 515, 463, 307, 380, 58, 174, 522, 484, 370, 28, 84, 252, 215, 104, 312, 395, 103, 309, 386, 76, 228, 143, 429, 205, 74, 222, 125, 375, 43, 129, 387, 79, 237, 170, 510, 448, 262, 245, 194, 41, 123, 369, 25, 75, 225, 134, 402, 124, 372, 34, 102, 306, 377, 49, 147, 441, 241, 182, 5, 15, 45, 135, 405, 133, 399, 115, 345, 494, 400, 118, 354, 521, 481, 361, 1] \quad (4)$$

(b) Make a log table out of a given power table pt:

The procedure logtab(pt, m) returns a list of length m-1 whose k-th entry equals
DL_b(k), if k in <b> and equals 0 otherwise.

```
> logtab := proc(pt, m) local lt, k, n;
    n := nops(pt); lt := [seq(0, k = 1 ..m − 1)];
    for k to n do;
      lt := subsop(pt[k] = k, lt); od;
    return(lt); end;
```

(5)

```
logtab := proc(pt, m)                                                    (5)
    local lt, k, n;
    n := nops(pt);
    lt := [seq(0, k = 1 ..m − 1)];
    for k to n do lt := subsop(pt[k] = k, lt) end do;
    return lt
end proc
```

Note: As was stated in the problem, be sure to use the subsop command in place of a search command (or loop).

The log tables for (b,m) = (2,11), and (5,123) are as follows:

```
> logtab(pt1, 11);
```

$$[10, 1, 8, 2, 4, 9, 7, 3, 6, 5] \tag{6}$$

```
> logtab(pt2, 123);
```

[20, 3, 0, 6, 1, 0, 0, 9, 0, 4, 0, 0, 0, 0, 0, 12, 0, 0, 0, 7, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 14, 15, 0, 0, 0, 0, 16, 0, 0, 10, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 17, 0, 18, 0, 0, 0, 0, 0, 0, 0, 0, 0, 19, 0, 0, 11, 0, 0, 13, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] **(7)**

(c) The discrete log function:

```
> DL := (y, b, m) → logtab(powtab(b, m), m)[y];
```

$$DL := (y, b, m) \rightarrow logtab(powtab(b, m), m)_y \tag{8}$$

The discrete log DL_7(17) in F_71 is 49 because

```
> DL(17, 7, 71);
```

$$49 \tag{9}$$

This is correct because 7^49 = 17 mod 71:

```
> Power(7, 49) mod 71;
```

$$17 \tag{10}$$

Similarly, the discrete log DL_2(33) in (Z/17389Z)^x is 12460 because

```
> DL(33, 2, 17389);
```

$$12460 \tag{11}$$

This is correct because 2^12460 = 33 mod 17389:

```
> Power(2, 12460) mod 17389;
```

$$33 \tag{12}$$

Remarks: 1) Note that the last discrete log computation took several seconds (whereas the computation of the check was instantaneous):

```
> settime := time( ) : DL(33, 2, 17389); time( ) − settime;
```

$$12460$$
$$4.914 \tag{13}$$

Thus, this took 4.9 secs. That this took some time is understandable because the DL program has to construct two tables of length > 15,000.

2) If we compute DL(3,4,123), then we obtain:

```
> DL(3, 4, 123);
```

$$0 \tag{14}$$

This means that 4 is not congruent to a power of 3 mod 123. This is also evident from the computation of part (b).