HW 4 Baby Step-Giant Step Problem

William Gasarch

July 19, 2014

Many people got Problem 7 on HW4 wrong. Some got it right but didn't show work. Some were very sloppy. This document shows what I wanted you to do. I will actually do problem 4,5,6 also since they give the tables needed. I did NOT use a calculator so you'll also see some tricks that I used to avoid long calculations.

I assume that the prior problems were done and that $g = 6$.

PROBLEM 4: Let $p = 59$ and g be as in the last problem. Compute the following mod p. $g^1, g^2, g^3, g^4, g^5, g^6, g^7, g^8$. Put them in a table and sort the table on the second coordinate (note that we are going to do the Baby Step/Giant Step).

SOLUTION TO PROBLEM 4 (AND I INCLUDE MY TRICKS FOR EASIER CALCULATION) I ALSO INCLUDE g^0. $=$ MEANS $\equiv \pmod{59}$.

BEFORE DOING THIS I COMPUTE SOME MULTIPLES OF 59 THAT I MAY USE

$59 \times 2 = 118$

$59 \times 3 = 177$

I USE TWO TRICKS: (1) IF A NUMBER IS BIG, LIKE 47, I MAY INSTEAD USE ITS NEGATIVE (2) IF A NUMBER HAS MANY FACTORS I MAY TRY TO REARRANGE THEM TO GET A NUMBER JUST A BIT BIGGER THAN 59 AND HENCE SMALL FOR US.

i	6^i
0	$6^0 = 1$
1	$6^1 = 6$
2	$6^2 = 36$
3	$6^3 = 36 \times 6 = 36 \times 2 \times 3 = 72 \times 3 = 13 \times 3 = 39$
4	$6^4 = 39 \times 6 = 39 \times 2 \times 3 = 78 \times 3 = 19 \times 3 = 57$
5	$6^5 = 57 \times 6 = (-2) \times 6 = -12 = 59 - 12 = 47$
6	$6^6 = 47 \times 6 = (-12) \times 6 = -(12 \times 6) = -72 = 118 - 72 = 46$
7	$6^7 = 46 \times 6 = (2 \times 23 \times 2 \times 3) = (23 \times 3) \times 4 = 69 \times 4 = 10 \times 4 = 40$
8	$6^8 = 40 \times 6 = (2 \times 2 \times 2 \times 5 \times 2 \times 3) = (2 \times 2 \times 3 \times 5 \times 2 \times 2) = 60 \times 4 = 4$

NOW WE SORT ON THE SECOND COMPONENT

i	6^i
0	$6^0 = 1$
8	$6^8 = 4$
1	$6^1 = 6$
2	$6^2 = 36$
3	$6^3 = 39$
7	$6^7 = 40$
6	$6^6 = 46$
5	$6^5 = 47$
4	$6^4 = 57$

PROBLEM 5: Let $p = 59$ and g be as in the last problem. Find g^{-1}.

SOLUTION TO PROBLEM 5.

We need a number a such that $6a \equiv 1 \pmod{59}$. It is easy to see that $a = 10$ works. So $g^{-1} = 10$.

PROBLEMS 6: Let $p = 59$ and g be as in the last problem. Compute the following mod p. $g^{-8\times1}, g^{-8\times2}, g^{-8\times3}, g^{-8\times4}, g^{-8\times5}, g^{-8\times6}, g^{-8\times7}, g^{-8\times8}$

Put them in a nice table (no need to sort).

SOLUTION TO PROBLEM 6 (WITH MY SHORTCUTS)

First note that since $6^{-1} = 10$ we really want 10^0, $10^{-8\times1}$, etc. Let us FIRST get 10 to powers of 2, then we can get the rest easily.

THIS IS NOT THE ANSWER, IT WILL HELP US GET THE ANSWER:

i	10^{2^i}
0	$10^{2^0} = 10^1 = 10$
1	$10^{2^1} = 10^2 = 100 = 41$
2	$10^{2^2} = (10^{2^1})^2 = (41)^2 = (-18)^2 = 18^2 = 3^4 \times 2^2 = 81 \times 4 = 22 \times 4 = 88 = 29$
3	$10^{2^3} = (10^{2^2})^2 = 29^2 = (-30)^2 = 30^2 = (2 \times 3 \times 5 \times 2 \times 3 \times 5) = 60 \times 15 = 15$
4	$10^{2^4} = (10^{2^3})^2 = 15^2 = (3 \times 5 \times 3 \times 5) = (5 \times 5 \times 3 \times 3) = 75 \times 3 = 16 \times 3 = 48$
5	$10^{2^5} = (10^{2^4})^2 = 48^2 = (-11)^2 = 121 = 121 - 118 = 3$
6	$10^{2^6} = (10^{2^5})^2 = 3^2 = 9$

NOW the calculations will be much easier. I write each power I want as a sum of powers of 2 and then use the above. Here is the real answer:

i	$10^{8\times i}$
0	$10^{8\times0} = 10^0 = 1$
1	$10^{8\times1} = 15$
2	$10^{8\times2} = 48$
3	$10^{8\times3} = 10^{16} \times 10^8 = 48 \times 15 = (12 \times 4 \times 15) = 12 \times 60 = 12$
4	$10^{8\times4} = 3$
5	$10^{8\times5} = 10^{32} \times 10^8 = 3 \times 15 = 45$
6	$10^{8\times6} = 10^{32} \times 10^{16} = 3 \times 48 = 3 \times -11 = -33 = 59 - 33 = 26$
7	$10^{8\times7} = 10^{32} \times 10^{16} \times 10^8 = 3 \times 48 \times 15 = 48 \times 45 = (-11) \times (-14) = 11 \times 7 \times 2 = 77 \times 2 = 18 \times 2 =$
8	$10^{8\times8} = 9$

PROBLEM 7: Let $p = 59$ and g be as in the last problem. USING the Baby-step Giant-step method (and show ALL work) find the discrete log of 10, 11, and 12. (Use $m = 8$ as the tables are already geared towards that.)

SOLUTION TO PROBLEM 7.

We'll just do the $DL(11)$ and $DL(12)$ cases.

FINDING DL OF 11 RECALL: For $q = 0$ to 8 we need to see if there is a value $0 \leq r \leq 8$ such that $11 = 6^{8q+r}$. We rewrite this as $11 \times 10^{8q} = 6^r$. SO, we need to see if 11×10^{8q} is on the first table (second column). If so we can find the r.

We do the calculation 11×10^{8q} easily since we already know all of the 10^{8q}.

Finding if $11 \times 10^{8q} = 6^r$ with $0 \leq r \leq 8$ is easy since we have a table of ALL numbers of the form 6^r with $0 \leq r \leq 8$. And the list is sorted so we can find it easily. And the list also stores the r values. (NOTE- for the numbers we are looking at the sorting is not really needed. For a computer working with much bigger numbers, it is.)

$q = 0$. Is $11 \times 10^{8\times 0} = 11 \times 10^0 = 11$ on the first table? NO it is not- note that there is a 6 and a 36 adjacent, so NO 11.

$q = 1$. Is $11 \times 10^{8\times 1} = 11 \times 15 = 47$ on the first table? YES it is! Note that $6^5 = 47$, so $r = 5$. Hence we can take $q = 1$ and $r = 5$. Hence the DL of 11 is $8 \times 1 + 5 = 13$.

HENCE THE ANSWER IS 11. LIZ THE TA: NOTE THAT HERE IS THE ANSWER: 11

(Some students do not clearly mark the answer. The above sentence makes it clear what the answer is. Only use if your TA is named Liz.)

FINDING DL OF 12 RECALL: For $q = 0$ to 8 we need to see if there is a value $0 \leq r \leq 8$ such that $12 = 6^{8q+r}$. We rewrite this as $12 \times 10^{8q} = 6^r$. SO, we need to see if 12×10^{8q} is on the first table (second column). If so we can find the r.

We do the calculation 12×10^{8q} easily since we already know all of the 10^{8q}.

Finding if $12 \times 10^{8q} = 6^r$ with $0 \leq r \leq 8$ is easy since we have a table of ALL numbers of the form 6^r with $0 \leq r \leq 8$. And the list is sorted so we can find it easily. And the list also stores the r values. (NOTE- for the numbers we are looking at the sorting is not really needed. For a computer working with much bigger numbers, it is.)

$q = 0$. Is $12 \times 10^{8\times 0} = 12 \times 10^0 = 12$ on the first table? NO it is not- note that there is a 6 and a 36 adjacent, so NO 12.

$q = 1$. Is $12 \times 10^{8\times 1} = 12 \times 15 = 3$ on the first table? NO it is not- note that ther is a 1 and a 4 adjacent, so NO 3.

$q = 2$. Is $12 \times 10^{8\times 2} = 12 \times 48 = 12 \times 45$ on the first table? NO it is not- note that ther is a 40 and a 46 adjacent so NO 45.

$q = 3$. Is $12 \times 10^{8\times 3} = 12 \times 48 = 12 \times 45$ on the first table? NO it is not- note that ther is a 40 and a 46 adjacent so NO 45.

$q = 4$. Is $12 \times 10^{8\times 4} = 12 \times 3 = 36$ on the first table? YES- we see that $6^2 = 36$. So we can take $q = 4$ and $r = 2$ and get that the DL of 12 is $8 \times 4 + 2 = 34$.

LIZ- THE DL OF 12 IS 34.