NT & ECC
MAT4930 5662

HW-4

Prof. JLF King
Touch: 2Jul2018

All four HW problems were emailed out; I have typeset the 4th-problem, here, to make it easier to read. I suggest that you staple this sheet as first page of your soln to problem 4.4.

Essays should abide by the CHECKLIST on

http://www.math.ufl.edu/~squash/teaching.html

It will help me if you write your ordinal, LARGE, in the upper-RH corner of the first page of your WU, and your name below or next to it. Ta.

4.4: We work modulo $M := 191$, which is prime. Its multiplicative-group, Γ, has $\varphi(191)=190$ elements. This Γ is cyclic, and $G := 19$ is a generator, i.e $\text{Ord}_\Gamma(G) = 190$.

Use BSGS ("Baby-Step Giant-Step") to compute the unique exponent E in $[0 \,..\, 190)$ for which

$$19^E \equiv_M 23\,.$$

a Draw a large circle-picture and label the entries of the bottom-right patch by $G^0 \equiv 1$, $G^1 \equiv 19$, $G^2 \equiv 170$, ... up to $G^{12} \equiv ??$, putting in the actual values. [*Optional:* Produce a sorted version of this list, for binary searching.]

b Draw in the other patches; how many are there? By how much does our last patch overlap our initial patch?

c What is the value of the multiplier, call it U, which carries us back to the previous patch? Now use BSGS to compute the above E. Which patch was it in?

d Use repeated-squaring to check that your value for E is correct.