NUMBER THEORY I
SPRING 2018

ASSIGNMENT 13.3
DUE APRIL 25

Exercise 1. Let p an odd prime, $p \nmid a$ and suppose that $\left(\frac{a}{p}\right) = 1$. Show that the algorithm we gave for finding square roots of $a \pmod{p^m}$ can be written in the form

$$r_{m+1} \equiv \frac{1}{2}\left(r_m + \frac{a}{r_m}\right) \pmod{p^{m+1}},$$

where the fractions are simply a notational device to indicate taking the inverse $\pmod{p^m}$ of the element in the denominator. Show that, up to the fact that we are performing modular arithmetic, *this is the same recursion given by Newton's method from calculus for approximating* $\sqrt{a}$.

Exercise 2. Show that $\left(\frac{2}{7}\right) = 1$ and find the square roots of $2 \pmod{7^m}$ for $1 \leq m \leq 5$, using either the algorithm discussed in class, or its reformulation given above.