Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. Multiplicative inverses in two ways. Let $m = 101$.
   (a) Use Fermat's Little Theorem and the fast power algorithm to compute the inverse of 68 in $\mathbb{Z}_m$.
   (b) Use the extended Euclidean algorithm to compute the inverse of 68 in $\mathbb{Z}_m$.
   (c) Which method is better? Are there circumstances when one method can be used, but not the other?

2. [JJJ 1.36] Compute the value of $2^{(p-1)/2} \pmod p$ for every prime p such that $3 \leq p < 20$. (You do not need to show the details of your computation.) Make a conjecture as to the possible values of $2^{(p-1)/2} \pmod p$ and prove that your conjecture is correct.

3. Let $m = 1961$. Use Fermat's Little Theorem to prove that m cannot be prime. Do not factor m.

4. Fast Power Algorithm
   (a) Implement the fast power algorithm `fast_power`(a, n, m) as a function that computes $a^n \pmod m$. A recursive implementation will probably not work due to limited stack space provided by most programming environments, so an iterative implementation is recommended. Submit your code for `fast_power`(a, n, m). Hints: make a loop that computes $\alpha \cdot (\beta)^n \pmod m$, where α and β are variables. In each iteration, your loop should decrease n by 1 (if n is odd) or cut n in half (if n is even), modifying α and β appropriately.

(b) Use your code to compute $3^n \pmod m$ where

$$n = 821036289345065157413172229675735660520083016935657878581340012427976914943991097837309645364624258053145966355116065354591033434855266678250438301548529598352882812656428385418093139636082570658299829788458938908380697891850347162793511345840677394329025453958771101783320710143255502165882660412782001229014976766842196418148035830194622969905911126993897921967321817986478442195134063060064678359754030334303960856670348374085636897270421920592695857045941303445877873776631729687290220967738719394610885925352341939128785360497722310135338307527222868644664552070651137382023448891804352986044611267798726544229245 1$$

$$m = 865115004355732551145017510126478620877543942297436341469140268739268386174658077372180608647325347798354292868567454439581756543056845714821187406006409811660901887625785757970044918073643563547474989534274434944403668015688790562183523557949513113457521773059495238938201195279925138931446812421418853371399332409100345940952416553337808100354362871109951870215818680246819107214492903711323010930843097199754799801451312671268935081309087777646976206845273438064284099734416580537135595935687371967971961207074853896477311180589401574808099181259933074341756543771264188237265473464737563681021550920284059941660272 9$$

Hint: to check your work, the answer begins "860..." and the sum of the digits is 2765.

(c) Compute $3^{m-1} \pmod m$, $4^{m-1} \pmod m$, and $5^{m-1} \pmod m$. What might these computations suggest about m?