Problem Set 3

1. **Can't we all just get along?** (5 pts)
   In an particular instance of the stable marriage problem with n men and n women, it turns out that there are exactly three distinct stable matchings, $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$. Also, each man M has a different partner in the three matchings. Therefore each man has a clear preference ordering of the three matchings (according to the ranking of his partners in his preference list). Now, suppose for man M_1, this order is $\mathcal{M}_1 > \mathcal{M}_2 > \mathcal{M}_3$. True or false: every man has the same preference ordering $\mathcal{M}_1 > \mathcal{M}_2 > \mathcal{M}_3$. Justify your answer.

2. **Squares in $\mathbb{Z}_8$** (5 pts)
   Prove that if $n \equiv 7 \pmod 8$, then n cannot be the sum of the squares of 3 integers.

3. **What's in a googolplex?** (3 pts)
   A "googolplex", the namesake of Google's "Googleplex" headquarters, is the number written as 1 followed by 10^{100} zeroes. That is, it's $10^{10^{100}}$. For a positive integer n, we define "n factorial" (written $n!$) as the product of all positive integers from 1 to n, i.e. $n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$. As you might imagine, $10^{10^{100}}!$, googleplex factorial, is a Very Large Number. Let

   $$\begin{aligned} m \;=\; & 518592598673542354244446723783888386221345346346345345 62 \\ & 434345346344209816452435913459181000751311145943572345 91 \\ & 102350982374575234234575911174490422035251174567779890 31. \end{aligned}$$

   Note that that's a single 168-digit number (it just doesn't fit onto one line). Calculate what $10^{10^{100}}!$ is congruent to, modulo m. That is, find the value of:

   $$10^{10^{100}}! \mod m$$

   Show all your work. Hint: if your answer takes more than 5-10 lines of text, you are probably doing it wrong.

4. **Modular pigeons** (2 pts)
   Let a and n be positive integers. Prove that if you write down the values of $a^0 \mod n$, $a^1 \mod n$, …, $a^n \mod n$, at least one number will appear more than once in the list.

5. **Euclid's algorithm** (4 pts)
   Find the GCD of a and b using Euclid's algorithm. Show all steps:

   (a) $a = 42$, $b = 70$
   (b) $a = 1234$, $b = 4321$

6. **Greatest Common Roots** (8 pts)
   Take two integers $a \geq 2$ and $b \geq 2$. We'll say that integer c is a common root of a and b if there exist positive integers n and m such that $a = c^m$ and $b = c^n$. Not all pairs of a and b have a common root, but if they do, we'll define their Greatest Common Root (GCR) to be, naturally, the greatest of their common roots.

   For instance, the GCR of 729 and 81 will be 9, since $9^3 = 729$ and $9^2 = 81$. While 3 is also *a* common root of 729 and 81, it's not the greatest one. On the other hand, 16 and 36 don't have a greatest common root at all, since there are no integers which are integer-power roots of both 16 and 36.

   Design an algorithm which takes two integers a and b and quickly determines their GCR if it exists, or, otherwise, detects that there's no GCR. By "quickly" we mean, in particular, that you may *not* go through a long list of integers to do trial-and-error.

   Prove that your algorithm works.