MATH 301: Problem Set 6

1. Recall that a number a is said to have an inverse modulo m if $ax \equiv 1 \pmod{m}$ has a solution.

   (a) If p is prime, prove that every nonzero element modulo p has an inverse.

   (b) Write down the inverse for each nonzero element of $\mathbb{Z}/7\mathbb{Z}$. For example, the inverse of 2 modulo 7 is 4, since $2 \cdot 4 \equiv 1 \pmod{7}$

2. Sometimes it turns out that an element of $\mathbb{Z}/m\mathbb{Z}$ is its *own* inverse. For example, $2 \cdot 2 \equiv 1 \pmod{3}$, so 2 is its own inverse modulo 3.

   (a) If p is an odd prime, prove that exactly 2 elements of $\mathbb{Z}/p\mathbb{Z}$ are their own inverses. Which elements exactly?

   (b) Does your proof in part (a) still work if the modulus is composite? If not, where does it fail?

3. (Discussion) If you tried to google the topic of lecture 10, "Sun Tzu's remainder theorem", you may end up with very few results. This is because the theorem almost universally goes by the name "Chinese remainder theorem".

   (a) What are some reasons to keep the current name? What are some reasons to name the theorem after its creator? Discuss with your group.

   (b) Which name do you prefer, and what reason(s) from your group did you find most convincing? There's no right answer but it's a good discussion to have, and absolutely part of doing mathematics!

4. When a large amount of several hundred marbles is divided into groups of 2, 3, 4, 5, or 6, there is one marble left over each time. However, when the marbles are divided into groups of 7, there are none left over. How many marbles are there?

5. (★) Here is a useful divisibility rule for 7: given a number, take the last digit, multiply it by 5, then add the result to the original number with its last digit removed. If this number is divisible by 7, then so is the original number. This trick is especially useful for 3 digit numbers.

   For example, 329 is divisibly by 7 because $9 \cdot 5 = 45$ and $32 + 45 = 77$, which a multiple of 7.

   Why does this divisibility rule work?

6. An element $a \in \mathbb{Z}/m\mathbb{Z}$ is called a **square** if $x^2 \equiv a \pmod{m}$ has a solution. How many elements of $\mathbb{Z}/104\mathbb{Z}$ are squares? [Hint: $104 = 8 \cdot 13$ and Sun Tzu's theorem]