MTH 236, Spring 2024 - Homework 12

Due on April 19th at 11:59pm on gradescope

1. The factor group $\mathbb{Z}/m\mathbb{Z}$ can be turned into a ring for any integer $m > 0$ by defining the product $(a \bmod m)(b \bmod m) = ab \bmod m$. The resulting ring is isomorphic to the ring $\mathbb{Z}_m$. From now on, let us identify $\mathbb{Z}_m$ with $\mathbb{Z}/m\mathbb{Z}$ for all positive integers m. (This just means we think of the elements of $\mathbb{Z}_m$ as equivalence classes mod m.)

   Suppose that r and s are relatively prime. Define a map $\phi : \mathbb{Z}_{rs} \longrightarrow \mathbb{Z}_r \times Z_s$ by $\phi(n) = (n \bmod r, n \bmod s)$ where n is an element of $\mathbb{Z}_{rs}$ (o,r equivalently, an integer mod rs).

   (a) Check that ϕ is well defined. That is, check that if $n \equiv n' \bmod rs$, then $\phi(n) = \phi(n')$.

   (b) Check that ϕ is a ring homomorphism.

   (c) Prove that ϕ is a ring isomorphism. [Hint: Either prove that ϕ is onto and use a counting argument to show it's one-to-one, or prove that ϕ is one-to-one and use a counting argument to show that ϕ is onto. You will need to use the fact that r and s are relatively prime here.]

2. The purpose of this problem is to prove Wilson's theorem:

   Wilson's theorem: *Let $n \geq 2$ be an integer. Then $(n-1)! \equiv -1 \pmod{n}$ if and only if n is prime.*

   (a) Show that if n is not prime, then n has a divisor a with the properties that $n > a > 1$ and a divides $(n-1)!$. Suppose that $(n-1)! \equiv -1 \pmod{n}$, and come up with a contradiction. [Hint: Force a to divide 1.] This proves one direction of Wilson's theorem.

   (b) Show that if p is prime, then 1 and -1 are the only elements of $\mathbb{Z}_p$ that are their own multiplicative inverses. [**Hint:** Consider the equation $x^2 - 1 = 0$.]

   (c) Use part (b) to show that, if p is prime, then

   $$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}.$$

   Conclude that if p is prime, then $(p-1)! \equiv -1 \pmod{p}$, proving the other direction of Wilson's theorem.

   (d) Use Wilson's theorem to find $28! \pmod{31}$, and justify your answer. Your answer should be a number in $\{0, 1, \ldots, 30\}$.

3. (a) Find $3^{2015} \pmod{17}$ and justify your answer. Your answer should be a number in $\{0, 1, \ldots, 16\}$.

   (b) Find $3^{2015} \pmod{16}$ and justify your answer. Your answer should be a number in $\{0, 1, \ldots, 15\}$.

4. (a) Prove that $n^{31} \equiv n \pmod{2046}$ for all integers n. [Hint: $2046 = 2 \cdot 3 \cdot 11 \cdot 31$.]

   (b) Improve on the number 2046 appearing in part (a). That is, find an integer m that is larger than 2046 such that $n^{31} \equiv n \pmod{m}$, and briefly justify your answer.

5. p 209 Exercises 1, 4, 8, 9