Review for Midterms Exam 2.

Exercise.
In a certain school, each class has 30 seats. There are 7\(^9\) students in that school. They fill each class with students till there are no seats left, and then they start filling a new class. How many students are there in the last, not full class?

Solution.
30 = 2 \cdot 3 \cdot 5, so \(\varphi(30) = 1 \cdot 2 \cdot 4 = 8\). Therefore 7\(^8\) \equiv 1 \pmod{30}, and so 7\(^9\) \equiv 7 \pmod{30}. There are 7 students in the last class.

Exercise.
Find the last digit of 3\(^{39}\).

Solution.
10 = 2 \cdot 5, so \(\varphi(10) = 1 \cdot 4 = 4\). Therefore 3\(^4\) \equiv 1 \pmod{10}, and so 3\(^{39}\) = (3\(^4\))^9 \cdot 3^3 \equiv 1 \cdot 27 \equiv 7 \pmod{10}. The last digit is 7.

Exercise.
Say if the following maps are homomorphisms:

- \(f : \mathbb{Z}_4 \to \mathbb{Z}_4, f(x) = x^4\).
- \(f : \mathbb{Z}_4 \to \mathbb{Z}_4, f(x) = x^2\).
- \(f : \mathbb{Z}_5 \to \mathbb{Z}_5, f(x) = x^5\).

Solution.
The function \(f : \mathbb{Z}_4 \to \mathbb{Z}_4, f(x) = x^4\) is not a homomorphism. Take for example \(f([1] + [1]) = f([2]) = [2]^4 = [16] = [0], f([1]) + f([1]) = [1] + [1] = [2] \neq [0].\)
The function \( f : \mathbb{Z}_4 \to \mathbb{Z}_4 \), \( f(x) = x^2 \) is not a homomorphism either. Take for example \( f([1] + [1]) = f([2]) = [2]^2 = [4] = [0] \), \( f([1]) + f([1]) = [1] + [1] = [2] \neq [0] \).

The function \( f : \mathbb{Z}_5 \to \mathbb{Z}_5 \), \( f(x) = x^5 \) is a homomorphism. In general, for prime \( p \), \( x^p = x \) for any \( x \in \mathbb{Z}_p \), so the function \( f(x) = x^p \) is actually the identity function \( f(x) = x \). The identity function is a homomorphism.

**Exercise.**

Let \( f : F \to F \), \( f(x) = x^2 \). Prove that \( f \) is a homomorphism if and only if \( \text{char}(F) = 2 \) (i.e. \( 1_F + 1_F = 0_F \)).

**Proof.**

\( \Rightarrow \)

If \( f \) is a homomorphism then \( f(1+1) = f(1) + f(1) \). Now, \( f(1+1) = (1+1)(1+1) = 1 + 1 + 1 + 1 \) and \( f(1) + f(1) = 1 \cdot 1 + 1 \cdot 1 = 1 + 1 \). So \( 1 + 1 + 1 + 1 = 1 + 1 \). Subtract \( 1 + 1 \) form both sides, and get \( 1 + 1 = 0 \).

\( \Leftarrow \)

Assume \( 1 + 1 = 0 \). Let \( a, b \in F \). We need to show that \( f(a + b) = f(a) + f(b) \) and \( f(ab) = f(a)f(b) \).

\[ f(ab) = (ab)^2. \]

Since \( F \) is commutative, \( (ab)^2 = a^2b^2 = f(a)f(b) \).

\[ f(a+b) = (a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2. \]

Since \( F \) is commutative, \( ab + ba = ab + ab = (1+1)ab = 0 \cdot ab = 0 \). So \( a^2 + ab + ba + b^2 = a^2 + b^2 = f(a) + f(b) \).

**Exercise.**

Solve the system

\[ x \equiv 3 \pmod{15} \]
\[ x \equiv 6 \pmod{7} \]

**Solution.**

\[ x = 3 + 15t \]
\[ 3 + 15t \equiv 6 \pmod{7} \]
\[ 3 + t \equiv 6 \pmod{7} \]
\[ t \equiv 3 \pmod{7} \]
\[ t = 3 + 7r \]
\[ x = 3 + 15(3 + 7r) = 48 + 105r \]