Homework Set Five (graded)

Due Thursday, June 2.

Question 1. Solve

$$x^{131} \equiv 758 \pmod{1073}.$$

(Hint: Need $\phi(n)$.)

Question 2. Use the (proof of the) Chinese Remainder Theorem to find an integer that leaves a remainder of 9 when it is divided by either 10 or 11, but that is divisible by 13.

Question 3.

(a) Prove that if $f\colon \mathbb{Z} \to \mathbb{C}$ is multiplicative (that is, $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$) then $F(m) := \sum_{d|m} f(d)$ is also multiplicative.

(b) Consider $F(m) := \sum_{d|m} \phi(d)$, where ϕ is the Euler function. Prove that $F(m) = m$.

Question 4. Let k be a field and $f \in k[x]$ an irreducible polynomial. We define an equivalence relation $\sim$ on $k[x]$ by $g \sim h$ if $f \mid g-h$. For $g \in k[x]$, let $\overline{g} = \{h \in k[x] \mid g \sim h\}$ be the equivalence class of g. Defining $\overline{g} + \overline{h} := \overline{g+h}$ and $\overline{g} \cdot \overline{h} = \overline{g \cdot h}$, one can show that the set of equivalence classes $K := k[x]/\sim$ is a (commutative) ring.
Consider the field $\mathbb{F}_3$ and the irreducible polynomial $f = x^2 + x - 1 \in \mathbb{F}_3[x]$. Let $k = \mathbb{F}_3[x]/\sim$, where if $g, h \in \mathbb{F}_3[x]$ we have $g \sim h$ when $f \mid g - h$.

(a) Prove that if $\overline{g} \in K \setminus \{\overline{0}\}$ then there exists $\overline{h} \in K$ such that $\overline{g}\overline{h} = \overline{1}$. (Since K is a commutative ring, this implies that it is in fact a field.) Hint: Euclidean Algorithm.

(b) In the special case that $k = \mathbb{F}_3$, give a complete multiplication table for the multiplicative group $k^\times$. Is $k^\times$ cyclic? Explain/justify your answer.

Question 5. Suppose $p > 2$ is prime such that $p \equiv 1 \pmod 8$.

(a) Show $x^4 \equiv -1 \pmod p$ has a solution.

(b) Show that a solution to the previous part satisfies $(x + x^{-1})^2 \equiv 2 \pmod p$.

(c) Use the previous parts to prove $\left(\frac{2}{p}\right) = 1$.