Math 30810 Honors Algebra 3
Homework 6

Andrei Jorza

Due Wednesday, October 16

Do 5.

1. Explicit Chinese Remainder Theorem.

   (a) Let m and n be coprime integers and let u and v be integers such that $mu+nv = 1$ (from Bézout's relation). Show that the system of equations

   $$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

   has the unique solution $x \equiv anv + bmu \pmod{mn}$.

   (b) Compute

   $$12^{34^{56^{78}}} \pmod{90}$$

   [Hint: Use the Chinese Remainder Theorem.] (A bit on notation: the exponent of 56 is 78, the exponent of 34 is 56^{78}, the exponent of 12 is $34^{56^{78}}$. In particular, this is NOT $((12^{34})^{56})^{78}$.)

2. Artin 2.9.5 on page 73.

3. Let p be a prime integer. Show that $(p-1)! \equiv -1 \pmod{p}$. [Hint: There are two ways to do this. Either (a) decompose the polynomial $X^{p-1} - 1 \mod p$ into linear factors or (b) interpret $(p-1)!$ as a product of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$.]

4. Artin 2.12.1 on page 74.

5. Artin 2.12.2 on page 75.

6. Let p be an odd prime and $a \in \mathbb{Z}$ a primitive root mod p.

   (a) Show that $a^{p^{n-1}}(p+1)$ is a primitive root mod p^n.

   (b) If a is also a primitive root mod p^2 show that it is a primitive root mod p^n for all n. E.g., show that 2 is a primitive root mod 3^n for all n.

7. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive root mod p. Show that a^k is also a primitive root mod p if and only if $(k, p-1) = 1$. Conclude that there are exactly $\varphi(\varphi(p-1))$ primitive roots mod p in $(\mathbb{Z}/p\mathbb{Z})^\times$.

8. Let G be a group and $g \in G$. Show that $\mathrm{ord}(g) = n$ if and only if

   (a) $g^n = e$ AND

   (b) for every prime $p \mid n$, $g^{n/p} \neq e$.