Loyola University Chicago
Math 201, Spring 2010

Sample Quiz 4

Name (print): ______________________ **Signature:** ______________

You have 30 minutes. Show your work. Notes not allowed! Problems are on both sides of this sheet.

Problem 1. (7 pts) Find all solutions to the congruence

$$x^2 \equiv 4x \pmod{77}.$$

Solution: get $x^2 - 4x \equiv 0$ *(mod 77), so* $x(x-4) \equiv 0$ *(mod 77). Now note that* $77 = 7 \cdot 11$*, so* $x(x-4) \equiv 0$ *(mod 77), i.e.,* $77|x(x-4)$*, holds only if one of the following four cases is true:*

- $77|x$*, i.e.,* $x \equiv 0$ *(mod 77)*
- $77|x-4$*, i.e.,* $x - 4 \equiv 0$ *(mod 77), i.e.,* $x = 4$ *(mod 77)*
- $7|x$ *and* $11|x-4$*, so* $x = 7k$ *and* $7k - 4 + 11l = 0$*; solve* $7k + 11l = 4$*, get* $x = 70 + 77k$*;*
- $11|x$ *and* $7|x-4$*, so* $x = 11 + 77l$*.*

The complete solution is $x \equiv 0$ *or* $x \equiv 4$ *or* $x \equiv 11$ *or* $x \equiv 70$ *(mod 77).*

Problem 2. (3 pts) Find all solutions to

$$15x \equiv 14 \pmod{39}.$$

Solution: the congruence is equivalent to $15x + 39y = 14$ *for some* $y \in \mathbb{Z}$*. Now, gcd*$(15, 39) = 3$ *and* $3 \nmid 14$*, so there are no solutions.*

Problem 3. (5 pts) Prove that $n^{91} \equiv n^7 \pmod{91}$ for all integers n. Is $n^{91} \equiv n \pmod{91}$ for all integers n?

Solution: $91 = 7 * 13$ *and* 7, 13 *are prime (so* $gcd(7, 13) = 1$*), so the congruence* $n^{91} \equiv n^7$ *(mod* 91*) is equivalent to simultaneous congruences*

$$n^{91} \equiv n^7 \ (mod\ 7) \quad and\ n^{91} \equiv n^7 \ (mod\ 13),$$

which are the same as

$$\left(n^{13}\right)^7 \equiv n^7 \ (mod\ 7) \quad and\ \left(n^7\right)^{13} \equiv n^7 \ (mod\ 13).$$

One of the consequences of the Fermat's Little Theorem is that, for any prime p *and any* a, *we have* $a^p \equiv p$ *(mod* p*). This verifies both of the congruences above.*

Problem 4. (5 pts) The Linear Congruence Theorem says that $ax \equiv c \pmod{m}$ has a solution if and only if $\gcd(a, m)|c$, and if x_0 is one solution then $x \equiv x_0$ (mod $\frac{m}{\gcd(a,m)}$) is the complete solution. Use this result to prove the following:

- If $\gcd(m_1, m_2) = 1$, then, for any $a_1, a_2 \in \mathbb{Z}$, the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}$$

  have a solution, and if $x = x_0$ is one solution than the complete solution is $x \equiv x_0 \pmod{m_1 m_2}$.

Solution: see textbook.