Loyola University Chicago **Quiz 5**
Math 201, Spring 2010

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

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

Problem 1. (5 pts) Solve the simultaneous congruences

$$\begin{aligned} 4x &\equiv 3 \pmod 7 \\ 7x &\equiv 47 \pmod{23} \end{aligned}$$

Solution: in $\mathbb{Z}_7$, $[4]^{-1} = 2$ *so* $4x \equiv 3$ *(mod* 7*) can be rewritten as* $2\,4x \equiv 2\,3$, *so* $x \equiv 6$ *(mod* 7*). Hence* $x = 7k + 6$, *plug this into the second equation, get* $7(7k + 6) \equiv 47$, $49k + 42 \equiv 47$, *so* $3k \equiv 5$ *(mod* 23*). Change to a Diohpantine equation* $3k + 23l = 5$. *Check gcd*$(3, 23) = 1|5$, *so solutions exist. Guess that* $3\,8 + 23(-1) = 1$ *so* $3\,40 + 23(-5) = 5$. *Hence,* $k = 40$ *is one solution, which gives one solution* $x = 7\;40 + 6 = 286$ *to the simultaneous congruences. Then all solutions are* $x \equiv 286$ *(mod* 161*), where* $161 = 7\,23$, *which simplifies to*

$$x \equiv 125 \quad (mod\ 161).$$

Problem 2. (4 pts) State the Little Fermat's Theorem and use it to show that $15^{110} - 1$ is divisible by 11.

Solution: for any prime p *and integer* a *such that* $p \not| a$, $a^{p-1} \equiv 1$ *(mod* p*). Here, take* $p = 11$, $a = 15$, *check that* $11 \not| 15$, *get that* $15^{10} \equiv 1$ *(mod* 11*). Hence* $\left(15^{10}\right)^{11} \equiv 1$ *(mod* 11*) as well, which is what needed to be shown.*

Problem 3. (5 pts) Find the inverse of $[17]$ in $\mathbb{Z}_{53}$.
For full credit, your answer should have the form $[m]$, where m is an integer between 0 and 52.

Solution: need to solve $17x \equiv 1 \pmod{53}$, so $17x + 53y = 1$. Extended Euclidean Algorithm gives $x = 25$, so the answer is $[25]$.

Problem 4. (6 pts) The Chinese Remainder Theorem says the following: If $\gcd(m_1, m_2) = 1$, then, for any $a_1, a_2 \in \mathbb{Z}$, the simultaneous congruences $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$ have a solution, and if $x = x_0$ is one solution than the complete solution is $x \equiv x_0 \pmod{m_1 m_2}$. Use this result to prove the following:

- If $\gcd(m_1, m_2) = 1$ then
$$x \equiv a \pmod{m_1 m_2} \iff \begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases}$$

Solution: see textbook.