math 228

Assignment 2, due Thursday May 17, 2007

Question 1. [Exercises 2.1, # 12]

Which of the following congruences have solutions:

(a) $x^2 \equiv 1 \pmod 3$ (b) $x^2 \equiv 2 \pmod 7$ (c) $x^2 \equiv 3 \pmod{11}$

Question 2. [Exercises 2.1, # 32]

Let a, b, n be integers with $n > 0$. If (a, n) does not divide b, prove that the congruence $ax \equiv b \pmod n$ has no solution.

Question 3. [Exercises 2.2, # 8].

(a) Solve the equation $x^2 + x = 0$ in $\mathbb{Z}_5$.

(b) Solve the equation $x^2 + x = 0$ in $\mathbb{Z}_6$.

(c) If p is prime, prove that the only solutions of $x^2 + x = 0$ in $\mathbb{Z}_p$ are 0 and $p - 1$.

Question 4. [Exercises 2.2, # 10].

(a) Find all a in $\mathbb{Z}_5$ for which the equation $ax = 1$ has a solution. Then do the same thing for

(b) $\mathbb{Z}_4$ (c) $\mathbb{Z}_3$ (d) $\mathbb{Z}_6$

Question 5. [Exercises 2.3, # 2].

How many solutions does the equation $6x = 4$ have in

(a) $\mathbb{Z}_7$? (b) $\mathbb{Z}_8$? (c) $\mathbb{Z}_9$? (d) $\mathbb{Z}_{10}$?

Question 6. [Exercises 2.3, # 4].

If n is composite, prove that there exist $a, b \in \mathbb{Z}_n$ such that $a \neq 0$ and $b \neq 0$ but $ab = 0$.

Question 7. [Exercises 2.3, # 6].

Let a and n be integers with $n > 1$. Prove that $(a, n) = 1$ in $\mathbb{Z}$ if and only if the equation $[\,a\,]\,x = [\,1\,]$ in $\mathbb{Z}_n$ has a solution.

Question 8. [Exercises 2.3, # 12].

Let a, b, n be integers with $n > 1$. Describe the solutions in $\mathbb{Z}$ of the congruence $ax \equiv b \pmod n$.