MATH 3375 (Theory of Cryptology) – Fall 2013

Homework Assignment 2

Due: September 26

1. From Section 1.3, do Exercises 3, 5, 7c.
2. From Section 1.4, do Exercises 3, 7
3. From Section 1.5, do Exercises 2[1], 3abd, 5
4. Let a, b, and m be positive integers.
   - (i) Prove that $ax \equiv b \pmod{m}$ has no solution if $\gcd(a, m)$ does not divide b.
   - (ii) If $\gcd(a, m) = 1$, prove that $ax \equiv b \pmod{m}$ has a solution.
   - (iii) Solve the following congruences, or explain why no solution exists:

$$\begin{aligned} 4x &\equiv 7 \pmod{26} \\ 4x &\equiv 8 \pmod{26} \\ 5x &\equiv 17 \pmod{26} \\ 5x &\equiv 23 \pmod{26} \end{aligned}$$

5. The following message was encoded with an additive cipher. Decrypt it:
   MZVYDIB DN OJ OCZ HDIY RCVO ZSZMXDNZ DN OJ OCZ WJYT

[1] Yes, I know the answer is in the back. This is an important question. AVT