AM_10700-Quiz 2 Instructor: PaoLien Lai
Nov. 11, 2013 14:10 pm ~ 15:30 pm Closed book, no calculators

---

Student name:______________________________

Student number: ______________________________

There are 8 questions and 100 marks total.

1. (10 points) Find each of these values.
   a) $(-133 \mathbf{~mod~} 23 + 261 \mathbf{~mod~} 23) \mathbf{~mod~} 23$ **b)** $(457 \mathbf{~mod~} 23 \cdot 182 \mathbf{~mod~} 23) \mathbf{~mod~} 23$
2. (10 points) If the product of two integers is $2^7 3^8 5^2 7^{11}$ and their greatest common divisor is $2^3 3^4 5$, what is their least common multiple?
3. (15 points) Solve each of the following congruences.
   a) $34x \equiv 77 \pmod{89}$ **b)** $144x \equiv 4 \pmod{233}$ **c)** $200x \equiv 13 \pmod{1001}$
4. (15 points) Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences
   $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$, and $x \equiv 1 \pmod{11}$.
5. (20 points)
   a) Use Fermat's little theorem to compute 3^{302} **mod** 5, 3^{302} **mod** 7, and 3^{302} **mod** 11.
   b) Use your results from part (a) and the Chinese remainder theorem to find 3^{302} **mod** 385. (Note that $385 = 5 \cdot 7 \cdot 11$.)
6. (10 points) What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4x_n + 3) \mathbf{~mod~} 7$ with seed $x_0 = 3$?
7. (10 points) Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
   a) $f(p) = (p + 15) \mathbf{~mod~} 26$ **b)** $f(p) = (-7p + 2) \mathbf{~mod~} 26$
8. (10 points) Decrypt these messages encrypted using the shift cipher $f(p) = (p + 13) \mathbf{~mod~} 26$.
   a) CEBBOXNOB XYGA **b)** LO WI PBSOXNB