Homework 3, Mon 09-19-11
CS 2050, Intro Discrete Math for Computer Science
Due Fri 09-23-11, Note: This homework has 2 pages and 5 questions.

Problem 1: 20 Points
Use the fast modular exponentiation algorithm to compute:
(a) \(7^{644} \mod 645\).
(b) \(3^{2003} \mod 99\).
Note: Show your work, as in Rosen’s book.

Problem 2: 20 Points
What is the greatest common divisor of these pairs of integers:
(a) \(3^7 \times 5^3 \times 7^3 \) and \(2^{11} \times 3^5 \times 5^9\)
(b) \(11 \times 13 \times 17 \) and \(2^9 \times 3^7 \times 5^5\)
(c) \(23^{21} \) and \(23^{17}\)
Note: The calculations are elementary, but please give a one line explanation.

Problem 3: 20 Points
(a) Use Euclid’s algorithm to compute the gcd of 123 and 277.
(b) Use Euclid’s algorithm to compute the gcd of 9888 and 6060.
(c) Using you calculations of part (a), compute the multiplicative inverse of 123 in arithmetic \(\mod 277\). (Look also at detailed class lecture notes of 09-12-11.)
Note: Show your work.

Problem 4: 20 Points
(a) Argue that, on input any positive integer \(n\), procedure A below returns \(2^{n(n+1)}\):
procedure A\((n:\) positive integer\)
\[
P := 1 ;
\]
for \(i := 0\) to \(n\)
\[
P := P \times 4^i ;
\]
return\((P)\);
(b) Argue that, on input any even positive integer \(n\), B below returns \(\frac{1}{8}n(3n+2)\):
procedure A\((n:\) even positive integer\)
\[
S := 0 ;
\]
for \(i := \frac{n}{2} + 1\) to \(n\)
\[
S := S + i ;
\]
return\((S)\);
Problem 5: 20 Points

(a) Let \( p > 1 \) and \( q > 1 \) be prime numbers. Let \( x \) be such that

\[
\begin{align*}
    x &\equiv a \pmod{p} \quad (1) \\
    x &\equiv b \pmod{q} \quad (2)
\end{align*}
\]

Let \( p_q \) be the multiplicative inverse of \( p \) in arithmetic \( \pmod{q} \), and let \( q_p \) be the multiplicative inverse of \( q \) in arithmetic \( \pmod{p} \). That is:

\[
\begin{align*}
    p \cdot p_q &\equiv 1 \pmod{q} \\
    q \cdot q_p &\equiv 1 \pmod{p} .
\end{align*}
\]

Prove that \( x' \) below satisfies (1) and (2):

\[
x' = a \cdot q \cdot q_p + b \cdot p \cdot p_q .
\]

**Hint:** Consider the above expression \( \pmod{p} \) and \( \pmod{q} \).

You may also want to read again the passage on the Chinese Remainder Theorem.

(b) Find a positive integer \( x \) such that

\[
\begin{align*}
    x &\equiv 1 \pmod{3} \\
    x &\equiv 3 \pmod{7} .
\end{align*}
\]

(b) Find a positive integer \( x \) in the range \( 0 \leq x \leq 3 \times 7 = 21 \) such that

\[
\begin{align*}
    x &\equiv 1 \pmod{3} \\
    x &\equiv 3 \pmod{7} .
\end{align*}
\]