CS 280 - Homework 4
Due: At the prelim on Thursday, October 9

1. Let a, b, and c be positive integers with a and b being coprime.

i. Prove that $a \mid bc \implies a \mid c$.
ii. Prove that $a \mid c \wedge b \mid c \implies ab \mid c$.
iii. Prove that $a^{-1} \equiv s \pmod{b}$ if $as + bt = 1$.

2.

i. Use the matrix layout algorithm shown in class to find $\gcd(7245, 4784)$, and express it in the form $7245s + 4784t$.
ii. If it exists, give the value of the multiplicative inverse of 91 modulo 237.

3. Prove that for any integers a and b, $ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$.

4. Let p be prime. Prove that $(p-1)! \equiv -1 \pmod{p}$.

5. Solve each of the following for x.

i. $432x \equiv 2 \pmod{91}$
ii. $23x \equiv 16 \pmod{107}$
iii. $3x \equiv 1 \pmod{5}$ with $2x \equiv 6 \pmod{8}$

6. A hoard of gold pieces "comes into the possession of" a band of 15 pirates. When they come to divide up the coins, they find that 3 are left over. Their discussion of what to do with these extra coins becomes animated, and by the time some semblance of order returns, there remain only 7 pirates capable of making an effective claim on the hoard. When however the hoard is divided between these seven it is found that 2 pieces are left over. There ensues an unfortunate repetition of the earlier disagreement, but this does at least have the consequence that the 4 pirates who remain are able to divide up the hoard evenly between them. What is the minimum number of gold pieces that could have been in the hoard? (from Humphreys and Prest, "Numbers, groups and codes", CUP 1989)