Name:

Section 5.2

1. Without converting to decimal add the binary numbers: $1110101+110101$
2. Describe the method you are using to add the binary numbers above.
3. Without converting to decimal add the hexadecimal numbers: $48 F 9+D 62$
4. Describe the method you are using to add the hexadecimal numbers above.
5. Take the binary number 10010101101 and convert it to hexadecimal by:
(a) converting from binary to decimal and decimal to hexadecimal.
(b) converting directly from binary to hexadecimal.

Section 5.3
This section has two main ideas: (a) the Euclidean Algorithm (how to run it) and (b) how to use the Euclidean (what it tells you)

You will find this algorithm in pseudo code on page 249. Here is the algorithm in plain English. The input consists of two nonnegative integers $a$ and $b$ and without loss of generality, assume $a \geq b$. Apply the Quotient-Remainder Theorem (page 111) to $a$ and $b$ to obtain a remainder $r$. Now repeat with $b$ and $r$. Continue until obtaining the remainder 0 .

Here is the trace of the Euclidean Algorithm on $a=225$ and $b=84$.

| iteration | $a$ | $b$ | Quotient-Remainder Thm <br> $a=q \cdot b+r ; 0 \leq r<b$ | $r$ | comments |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 225 | 84 | $225=2 \cdot 84+57$ | 57 | $r \neq 0$ so repeat |
| 2 | 84 | 57 | $84=1 \cdot 57+27$ | 27 | $r \neq 0$ so repeat |
| 3 | 57 | 27 | $57=2 \cdot 27+3$ | 3 | $r \neq 0$ so repeat |
| 4 | 27 | 3 | $27=9 \cdot 3+0$ | 0 | $r=0$ so return previous $r$-value |

The algorithm would return the number 3

1. Apply the Euclidean Algorithm to each pair below. Show your work by including the Quotient-Remainder Thm calculation for each iteration.
(a) $m=2310, n=805$
(b) $n=18, m=305$
2. Let $a, b, q, r, d \in \mathbb{Z}^{+}$and assume $a=q \cdot b+r$. If $d$ divides $a$ and $d$ divides $b$, does that mean $d$ divides $r$ ? Explain your answer.
3. (Read carefully! This is different from \#2.) Let $a, b, q, r, d \in \mathbb{Z}^{+}$and assume $a=q \cdot b+r$. If $d$ divides $r$ and $d$ divides $b$, does that mean $d$ divides $a$ ? Explain your answer.
4. Now use your answers to $\# 2$ and $\# 3$ above to explain why the Euclidean Algorithm returns the greatest common divisor of its two inputs.
5. For 1 a and 1 b above, find the prime factorization of each integer and confirm that the Euclidean Algorithm returns the greatest common divisor of $m$ and $n$.

One of the other useful results of the Euclidean Algorithm is that the calculations used to find the GCD and be reversed to obtain the GCD of two integers in terms of a linear combination of the two integers. For example, we found that gcd $225,84=3$. By reversing the calculations, we can obtain the equation: $3=3 \cdot 225-8 \cdot 84$.

In the table below, columns 1 and 2 are copied from the table on page 1 . Column 3 is obtained by solving each equation for $r$. Column 4 is back substitutions starting at the last row and working up.

| iter- <br> ation | QR Thm <br> (copied) | Solve for $r$ | back substitute and simplify | comments |
| :---: | :---: | :---: | :---: | :--- |
| 1 | $225=2 \cdot 84+57$ | $225-2 \cdot 84=57$ | $3 \cdot(225-2 \cdot 84)-2 \cdot 84=3$ | Replace <br> $57 ;$ <br> re-group |
| 2 | $84=1 \cdot 57+27$ | $84-1 \cdot 57=27$ | $57-2 \cdot[84-1 \cdot 57$ <br> $3 \cdot 225-8 \cdot 84=3$ | Replace <br> $27 ;$ <br> re-group |
| 3 | $57=2 \cdot 27+3$ | $57-2 \cdot 27=3$ | $3 \cdot 57-2 \cdot 84=3$ | START <br> HERE <br> work up |

6. For each pair of numbers below, write their GCD as a linear combination of $m$ and $n$.
(a) $m=2310, n=805$
(b) $n=18, m=305$
