Name: Solutions

Section 5.2

1. *Without converting to decimal* add the binary numbers: 1110101 + 110101

"carries"

$$\begin{array}{r} 1110101 \\ +\ 110101 \\ \hline 10101010 \end{array}$$

2. Describe the method you are using to add the binary numbers above.

1+1=10 (carry the 1)
1+1+1=11 (carry the 1)

3. *Without converting to decimal* add the hexadecimal numbers: 48*F*9 + *D*62

$$\begin{array}{r} 48F9 \\ D62 \\ \hline 565B \end{array}$$

work 9+2=11=B

$\underbrace{F+6}_{hex} = \underbrace{15+6=21}_{10} = \underbrace{16+5}_{10} = \underbrace{1\ 5}_{hex}$ (16, 1)

D+8+1 = 13+9 = 22 = 16+6

4. Describe the method you are using to add the hexadecimal numbers above.

Add normally, but when a sum is over 16, pull out a 16 an "carry" the "1".

5. Take the binary number 10010101101 and convert it to hexadecimal by:

(a) converting from binary to decimal and decimal to hexadecimal.

$2^{10}+2^7+2^5+2^3+2^2+1 = 1197$

$1197 = 4\cdot 16^2 + 10\cdot 16 + 13$

ANS: 4AD

(b) converting directly from binary to hexadecimal.

Use $2^4=16$. Or in binary 10000. So four consecutive bits is a # between 0 and 15

$\underbrace{100}\underbrace{1010}\underbrace{1101}$

(4) two-fifty sixes

(8+2) sixteens

(8+4+1) ones

ANS 4AD

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. $\boxed{\text{Yes}}$

Since $a = qb + r$ can be written $a - qb = r$, we know that if $d|a$ and $d|b$, then $d | a - qb$. So $d|r$.

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.

$\boxed{\text{Yes}}$

This is easier. By assumption, $d|b$ and $d|r$. So $d | qb + r$. So $d|a$.

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.

Any common divisor of a and b is a divisor of r. So the greatest common divisor of a and b is a divisor of r. This holds $\forall$ a, b, and r in every iteration. So the largest a divisor of a and b can b is the smallest positive r. From #3, we know r is a common divisor of a and b.

5. For 1a and 1b above, find the prime factorization of each integer and confirm that the Euclidean Algorithm returns the greatest common divisor of m and n.

1.a. $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$; $805 = 5 \cdot 7 \cdot 23$. So $\gcd(2310, 805) = 5 \cdot 7 = 35$ ✓

1.b $18 = 2 \cdot 3^2$, $305 = 5 \cdot 61$. So $\gcd(18, 305) = 1$ ✓

Section 5.3

This section has two main ideas: (a) the Euclidean Algorithm (how to run it)
and (b) how to use the ~~Euclidean~~ Algorithm (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 $a = q \cdot b + r$; $0 \leq r < b$	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 $\boxed{3}$.

1. Apply the Euclidean Algorithm to each pair below. Show your work by including the Quotient-Remainder Thm calculation for each iteration.

(a) $m = 2310$, $n = 805$

$2310 = 2 \cdot 805 + 700$
$805 = 1 \cdot 700 + 105$
$700 = 6 \cdot 105 + 70$
$105 = 1 \cdot 70 + 35$
$70 = 2 \cdot 35 + 0$

Return $\boxed{35}$.

This side is for #6 later

$\boxed{700} = 2310 - 2 \cdot 805$
$\boxed{105} = 805 - 1 \cdot \boxed{700}$
$\boxed{70} = 700 - 6 \cdot 105$
$35 = 105 - 1 \cdot \boxed{70} \longrightarrow 35 = 105 - (700 - 6 \cdot 105)$
$= 7 \cdot \boxed{105} - 1 \cdot 700$
$= 7(805 - 1 \cdot 700) - 1 \cdot 700$
$= 7 \cdot 805 - 8 \cdot \boxed{700}$
$= 7 \cdot 805 - 8(2310 - 2 \cdot 805)$
$= 23 \cdot 805 - 8 \cdot 2310$

(b) $n = 18$, $m = 305$

$305 = 16 \cdot 18 + 17$
$18 = 1 \cdot 17 + 1$
$17 = 17 \cdot 1 + 0$

Return $\boxed{1}$.

$\boxed{17} = 305 - 16 \cdot 18$
$1 = 18 - 1 \cdot \boxed{17} \longrightarrow 1 = 18 - 1 \cdot (305 - 16 \cdot 18)$

$\boxed{1 = 17 \cdot 18 - 305}$

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: $\boxed{3 = 3 \cdot 225 - 8 \cdot 84.}$

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.*

iteration	QR Thm (copied)	Solve for r	back substitute and simplify	comments
1	$225 = 2 \cdot 84 + 57$	$225 - 2 \cdot 84 = 57$	$3 \cdot \left(225 - 2 \cdot 84\right) - 2 \cdot 84 = 3$ $3 \cdot 225 - 8 \cdot 84 = 3$	Replace 57; re-group
2	$84 = 1 \cdot 57 + 27$	$84 - 1 \cdot 57 = 27$	$57 - 2 \cdot \boxed{84 - 1 \cdot 57} = 3$ $3 \cdot 57 - 2 \cdot 84 = 3$	Replace 27; re-group
3	$57 = 2 \cdot 27 + 3$	$57 - 2 \cdot 27 = 3$	$57 - 2 \cdot \boxed{27} = 3$	START HERE work up

6. For each pair of numbers below, write their GCD as a linear combination of m and n.

(a) $m = 2310,\ n = 805$

$35 = 23 \cdot 805 - 8 \cdot 2310$

(See R.H.S. of #1a)

(b) $n = 18,\ m = 305$

$1 = 17 \cdot 18 - 305$

(See R.H.S. of #1b)