Section 2.4

2.(d) x=1529, y=14039. Now stepping through the Euclidean algorithm,

r:=xmody=1529, x:=y=14039, y:=r=1529
r:=xmody=278, x:=y=1529, y:=r=278
r:=xmody=139, x:=y=278, y:=r=139
r:=xmody=0, x:=y=139, y:=r=0

Thus gcd(1529,14039)=139

14. (a) $5=9-3-1=3^2 - 3^1 - 3^0$
(b) $13=9+3+1=3^2 + 3^1 + 3^0$
(c) $37=27+9+1=3^3 + 3^2 + 3^0$
(d) $79=81-3+1=3^4 - 3^1 + 3^0$

24. (a) 010110
(b) 011111
(c) 111001
(d) 101101

26. Since m is positive, the first bit from the left needs to be changed from 0 to 1. Now for the remaining $n-1$ bits, for each $i=1,...,n-1,$ if bit i is 0, change it to 1 and if it is 1, change it to 0. Now add 1 to this bit string. The reasoning is as follows. Let $0a_2...a_n$ be the bitstring representation for m, where $a_i=0$ or $a_i=1$ for $i=1,...,n.$ Note that since m is positive, the leftmost bit is 0. Since $-m$ is negative the leftmost bit must be 1. Now let the remaining $n-1$ bits be $b_2...b_n$ which is the binary exapnsion of $2^{n-1}-m=1+((2^{n-1}-1)-m).$ Note that the binary expansion of $2^{n-1}-1$ is just (n-1) 1s. And the binary expansion of $((2^{n-1}-1)-m)$ involves just switching the ones and zeros in the binary expansion of m. And then we add 1 back.

Section 2.5

2.(e) The greatest common divisor of 101 and 203 is 1=203-2*101
(g) The greatest common divisor of 2002 and 2339 is 1=-819*2002+701*2339

10. Let $\gcd(a,m)=k>1$. Now assume that there exists b such that $ab\equiv 1 \bmod m.$ This implies that m divides $(ab-1)$. Let s be such that $ms=ab-1$, hence $ab-ms=1$. Now since k divides a as well as m, k must also divide $ab-ms.$ But k does not divide 1 since $k>1$ and we have a contradiction. Thus an inverse of a modulo m does not exist if $\gcd(a,m)>1$.

22. To use the Chinese Remainder Theorem, we can set this problem up as solving $x \equiv 0 \bmod 5$ and $x \equiv 1 \bmod 3$. Then using the notation from the book, $m_1 = 5$, $m_2 = 3$, $m = 15$, $M_1 = 3$, $M_2 = 5$, $a_1 = 0$, and $a_2 = 1$. Hence we solve $3y_1 \equiv 1 \bmod 5$ and $5y_2 \equiv 1 \bmod 3$, getting $y_1 = 2$ and $y_2 = 2$. There is then a unique solution modulo m given by $x = a_1M_1y_1 + a_2M_2y_2 = 10$. Hence $10 + 15n$ for any integer n satisfies the conditions.

36. First note that n=43*59=2537. Translating the letters in the word ATTACK to their numerical equivalents and grouping them into blocks of four we get

0019 1900 0210.

Encrypting each block, $19^{13} \bmod 2537=2299$, $1900^{13} \bmod 2537=1317$ and, $210^{13} \bmod 2537=2117$. Thus the encrypted message is 2299 1317 2117.

Section 2.6

4. (a)

AB=

$$\begin{vmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \\ 1 & -2 & 1 \end{vmatrix}$$

14. Let A, B be nxn diagonal matrices. Let C=AB. We want to show that C is a diagonal matrix as well. Let C(i, j) denote the entry in the i^{th} row and j^{th} column of matrix C. Now

$C(i,j)=\sum A(i,k)*B(k,j)$, where k runs from 1 to n.

Since A and B are diagonal matrices, $A(i,k)=0$ if $k\neq i$ and $B(k,j)=0$ if $k\neq j$ and so $C(i,j)=0$ if $i\neq j$. Thus C is a diagonal matrix. Since C is diagonal, we need only compute the diagonal entries. $C(i,i)=A(i,i)*B(i,i)$ for i=1,...,n.

20. (a) A^{-1}=

$$\begin{vmatrix} -0.6 & 0.4 \\ 0.2 & 0.2 \end{vmatrix}$$

(b) A^3=

$$\begin{vmatrix} 1 & 18 \\ 9 & 37 \end{vmatrix}$$

(c) $(A^{-1})^3$=

$$\begin{vmatrix} -0.296 & 0.144 \\ 0.072 & -0.008 \end{vmatrix}$$

(d) To check that $(A^{-1})^3=(A^3)^{-1}$, we compute $A^3*(A^{-1})^3$=

$$\begin{vmatrix} -0.296+18*0.072 & 0.144-18*0.008 \\ -9*0.296+37*0.072 & 9*0.144-37*0.008 \end{vmatrix}$$

=

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$$

Since inverses are unique, we have that $(A^{-1})^3=(A^3)^{-1}$.

Problem: Let A and B be the first and second matrices in problem 18, respectively, and let C and D be formed from A and B by taking each entry mod 2. Find the Boolean product of C and D.

First we form C and D. We have C=

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}$$

And D=

$$\begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{vmatrix}$$

Now C◯D=

$$\begin{vmatrix} (0\wedge 1)\vee(1\wedge 0)\vee(1\wedge 1) & (0\wedge 0)\vee(1\wedge 1)\vee(1\wedge 1) & (0\wedge 1)\vee(1\wedge 1)\vee(1\wedge 1) \\ (1\wedge 1)\vee(0\wedge 0)\vee(1\wedge 1) & (1\wedge 0)\vee(0\wedge 1)\vee(1\wedge 1) & (1\wedge 1)\vee(0\wedge 1)\vee(1\wedge 1) \\ (1\wedge 1)\vee(1\wedge 0)\vee(1\wedge 1) & (1\wedge 0)\vee(1\wedge 1)\vee(1\wedge 1) & (1\wedge 1)\vee(1\wedge 1)\vee(1\wedge 1) \end{vmatrix}$$

=

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{vmatrix}$$