Homework Set 1

Arnav Patri

September 4, 2022

4 Number Theory and Cryptography

4.2 Integer Representations and Algorithms

1–11 odd, 21, 23

1. a) $231 = (1110\,0111)_2$ b) $4532 = (1\,0001\,1011\,0100)_2$
   c) $97644 = (1\,0111\,1101\,0110\,1100)_2$

3. a) $(1\,1111)_2 = 37$ b) $(10\,0000\,0001)_2 = 513$
   c) $(1\,0101\,0101)_2 = 215$ d) $(110\,1001\,0001\,0000)_2 = 26896$

5. a) $(572)_8 = 378$ b) $(1604)_8 = 900$
   c) $(432)_8 = 275$ d) $(2417)_8 = 1295$

7. a) $(80\text{E})_{16} = (1000\,0000\,1110)_2$
   b) $(135\text{AB})_{16} = (0001\,0011\,0101\,1010\,1011)_2$
   c) $(\text{ABBA})_{16} = (1010\,1011\,1011\,1010)_2$
   d) $(\text{DEFACED})_{16} = (1101\,1110\,1111\,1010\,1100\,1110\,1101)_2$

9. $(\text{ABCDEF})_{16} = (1010\,1011\,1100\,1101\,1110\,1111)_2$

11. $(1011\,0111\,1011)_2 = (\text{B7B})_{16}$

21. a)

$$\begin{array}{r}
{\scriptstyle 1\;1\;1} \\
{\scriptstyle 1}\;1\,0\,0\;0\,1\,1\,1 \\
+\,1\,1\,1\;0\,1\,1\,1 \\
\hline
1\,0\,1\,1\;1\,1\,1\,0
\end{array}$$

$$\begin{array}{r}
1\;0\;0\;\;0\,1\,1\,1 \\
\times\,1\;1\;1\;\;0\,1\,1\,1 \\
\hline
{\scriptstyle 10\;10\;10\;\;10\;1} \\
{\scriptstyle 1\;1\;\;1\;1\;10\;11\;\;11}\;1\;0\;0\;\;0\,1\,1\,1 \\
1\;0\;0\;0\;\;1\,1\,1 \\
1\;\;0\;0\;0\;1\;\;1\,1 \\
1\,0\;0\;\;0\;1\;1\;1 \\
1\,0\,0\;0\;\;1\;1\;1 \\
+\;\;1\,0\,0\,0\;1\;\;1\;1 \\
\hline
1\,0\;0\,0\,0\;1\;\;0\;0\;0\;0\;\;0\,0\,0\,1
\end{array}$$

b)

$$\begin{array}{r}
{\scriptstyle 1\;1\;1\;1\;\;1\;1\;1} \\
{\scriptstyle 1}\quad 1\,1\,1\,0\;1\,1\,1\,1 \\
+\,1\,0\,1\,1\;1\,1\,0\,1 \\
\hline
1\quad 1\,0\,1\,0\;1\,1\,0\,0
\end{array}$$

$$\begin{array}{r}
1\;1\;1\;0\;\;1\,1\,1\,1 \\
\times\,1\;0\;1\;1\;\;1\,1\,0\,1 \\
\hline
{\scriptstyle 11\;11\;10\;10\;\;1} \\
{\scriptstyle 1\;\;1\;10\;11\;\;100\;100\;100\;100}\quad 1\;1\;1\;0\;\;1\,1\,1\,1 \\
1\;\;\;1\quad 1\;0\;1\;1\;\;1\,1 \\
1\;\;\;1\;\;\;1\quad 0\;1\;1\;1\;\;1 \\
1\;\;\;1\;\;\;1\;\;\;0\quad 1\;1\;1\;1 \\
1\;\;\;1\;\;\;1\;\;\;0\;\;\;1\quad 1\;1\;1 \\
+\,1\,1\,1\;\;\;0\;\;\;1\;\;\;1\;\;\;1\quad 1 \\
\hline
1\,0\,1\,1\;\;\;0\;\;\;0\;\;\;0\;\;\;0\quad 0\;1\;1\;1\;\;0\,0\,1\,1
\end{array}$$

c)

23.

a) $\begin{array}{r} {}^{1}\overset{1}{7}\overset{1}{6}3 \\ +147 \\ \hline 1132 \end{array}$
$\begin{array}{r} 763 \\ \times 147 \\ \hline {}^{2}\overset{1}{6}\,\overset{1}{6}45 \\ {}^{1}3714 \\ +763 \\ \hline 144305 \end{array}$

b) $\begin{array}{r} 6001 \\ +\ \ 272 \\ \hline 6273 \end{array}$
$\begin{array}{r} 6001 \\ \times\ \ 272 \\ \hline {}^{1}\quad 14002 \\ 52007 \\ +14002 \\ \hline 2134272 \end{array}$

c) $\begin{array}{r} \overset{1}{1}\overset{1}{1}\overset{1}{1}1 \\ +\ \ 777 \\ \hline 2110 \end{array}$
$\begin{array}{r} \overset{1}{1}\overset{1}{1}\overset{1}{1}1 \\ \times\ \ 777 \\ \hline 7777 \\ 7777 \\ +7777 \\ \hline 1107667 \end{array}$

d) $\begin{array}{r} 54321 \\ +3456 \\ \hline 57777 \end{array}$
$\begin{array}{r} 54321 \\ \times 3456 \\ \hline {}^{1\,1}\overset{2}{4}1\overset{1}{2}\overset{1}{3}46 \\ 336025 \\ 261504 \\ +205163 \\ \hline 237326216 \end{array}$

4.3 Primes and Greatest Common Divisors

1, 3, 5, 15, 17 (19 extra credit)

1. a) $\sqrt{21} \approx 4.583 > 2, 3$

   - ends in 1 $\therefore$ not divisible by 2
   - $2 + 1 = 3, 3 \bmod 3 = 0$ $\therefore$ divisible by 3

   21 is composite

   b)