Homework Set 1

Arnav Patri

September 8, 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) $(80E)_{16} = (1000\,0000\,1110)_2$
    b) $(135AB)_{16} = (0001\,0011\,0101\,1010\,1011)_2$
    c) $(ABBA)_{16} = (1010\,1011\,1011\,1010)_2$
    d) $(DEFACED)_{16} = (1101\,1110\,1111\,1010\,1100\,1110\,1101)_2$

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

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

21.

a)
```
        1 1 1
    ¹ 1 0 0 0 1 1 1
   + 1 1 1 0 1 1 1
   ―――――――――――――――
   1 0 1 1 1 1 1 0
```

```
              1 0 0 0 1 1 1
          ×   1 1 1 0 1 1 1
          ―――――――――――――――――
                10 10 10  10 1
   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
      ―――――――――――――――――――――――――――
      1 0 0 0 0 1 0 0 0 0  0 0 0 1
```

b)
```
        1 1 1 1  1 1 1
    ¹    1 1 1 0 1 1 1 1
      + 1 0 1 1 1 1 0 1
   ―――――――――――――――――――
   1   1 0 1 0 1 1 0 0
```

```
                       1 1 1 0 1 1 1 1
                   ×   1 0 1 1 1 1 0 1
                   ―――――――――――――――――――
                        11 11 10 10  1
   1  1 10 11  100 100 100 100  1 1 1 0 1 1 1 1
                       1 1   1 0 1 1 11
                     1 1 1   0 1 1 1 1
                   1 1 1 0   1 1 1 1
                 1 1 1 0 1   1 1 1
             + 1 1 1  0 1 1 1  1
   ―――――――――――――――――――――――――――――――――――
   1 0 1 1 0 0 0 0  0 1 1 1 0 0 1 1
```

1

c)

23.

a)
$$\begin{array}{r} \overset{1}{}\overset{1\,1}{7}63 \\ +147 \\ \hline 1132 \end{array}$$

b)
$$\begin{array}{r} 6001 \\ +272 \\ \hline 6273 \end{array}$$

c)
$$\begin{array}{r} \overset{1\,1\,1}{1111} \\ +777 \\ \hline 2110 \end{array}$$

d)
$$\begin{array}{r} 54321 \\ +3456 \\ \hline 57777 \end{array}$$

$$\begin{array}{r} 763 \\ \times 147 \\ \hline \overset{1\,1}{{}^2\,6\,645} \\ {}^1 3\,7\,14 \\ +7\,6\,3 \\ \hline 144\,305 \end{array}$$

$$\begin{array}{r} 6001 \\ \times 272 \\ \hline {}^11\,4002 \\ 5\,2007 \\ +14\,002 \\ \hline 21\,34272 \end{array}$$

$$\begin{array}{r} \overset{1\,1\,1}{1111} \\ \times 777 \\ \hline 7777 \\ 7777 \\ +7\,777 \\ \hline 1\,10\,7667 \end{array}$$

$$\begin{array}{r} 54321 \\ \times 3456 \\ \hline \overset{2}{{}^{1\,1}4}\,\overset{1\,1}{1}\,2346 \\ 33\,6025 \\ 261\,504 \\ +205\,163 \\ \hline 2373\,26216 \end{array}$$

4.3   Primes and Greatest Common Divisors

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

1.

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

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

21 is composite