Homework Set 1

Arnav Patri

September 15, 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)
$$\begin{array}{r} {\scriptstyle 1\ 1\ 1} \\ 1\,1\,0\,0\,0\,1\,1\,1 \\ +\,1\,1\,1\,0\,1\,1\,1 \\ \hline 1\,0\,1\,1\,1\,1\,1\,0 \end{array}$$

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

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

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

c)

23.

a)
$$\begin{array}{r} {\scriptstyle 1\ 1}\\ {\scriptstyle 1}\,763\\ +147\\ \hline 1132 \end{array}$$
$$\begin{array}{r} 763\\ \times 147\\ \hline {\scriptstyle 1\ 1}\\ {\scriptstyle 2}\,6645\\ {\scriptstyle 1}\,3714\\ +763\\ \hline 144305 \end{array}$$

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

c)
$$\begin{array}{r} {\scriptstyle 1\ 1\ 1}\\ 1111\\ +\ 777\\ \hline 2110 \end{array}$$
$$\begin{array}{r} {\scriptstyle 1\ 1\ 1}\\ 1111\\ \times\ 777\\ \hline 7777\\ 7777\\ +7777\\ \hline 1107667 \end{array}$$

d)
$$\begin{array}{r} 54321\\ +3456\\ \hline 57777 \end{array}$$
$$\begin{array}{r} 54321\\ \times 3456\\ \hline {\scriptstyle 2\ \ 1\ 1}\\ {\scriptstyle 1\ 1}\,4123\,46\\ 336025\\ 261504\\ +205163\\ \hline 237326216 \end{array}$$

4.3 Primes and Greatest Common Divisors

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

1. a) $21 = 7 \times 3 \therefore$ composite

   b) $\sqrt{29} \approx 5.385$
   - Odd $\therefore \not| \ 2$
   - $29 = 10(3) - 1 \therefore \not| \ 3$
   - $29 = 6(5) - 1 \therefore \not| \ 5 \therefore$ prime

   c) $\sqrt{71} \approx 8.426$
   - Odd $\therefore \not| \ 2$
   - $7 + 1 = 8 = 3(3) - 1 \therefore \not| \ 3$
   - $71 = 5(14) + 1 \therefore \not| \ 5$
   - $71 = 7(10) + 1 \therefore \not| \ 7 \therefore$ prime

   d) $\sqrt{97} \approx 9.849$
   - Odd $\therefore \not| \ 2$
   - $97 = 3(32) + 1 \therefore \not| \ 3$
   - $97 = 5(19) + 2 \therefore \not| \ 5$
   - $97 = 7(14) - 1 \therefore \not| \ 7 \therefore$ prime

3. a) $88 = 2^3 \times 11$ b) $126 = 2 \times 3^2 \times 7$ c) $729 = 3^6$ d) $1001 = 7 \times 11 \times 13$

   e) $1,111 = 11 \times 101$ f) $909,090 = 2 \times 3^3 \times 5 \times 13 \times 259$

5. $10! = 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 = 2^8 \times 3^4 \times 5^2 \times 7$

15. $30 = 2 \times 3 \times 5 \implies 1, 7, 11, 13, 17, 19, 23, 29$

17. a) $11, 15 = 3 \times 5, 19 \therefore$ Yes b) $14 = 7 \times 2, 15 = \mathbf{3} \times 5, 21 = \mathbf{3} \times 21 \therefore$ No

    c) $12 = 2^2 \times 3, 17, 31, 37 \therefore$ Yes d) $7, 8 = 2^3, 9 = 3^2, 11 \therefore$ Yes

6 Counting

6.1 The Basics of Counting

3.

6.3 Permutations and Combinations

1. $\{a, b, c\}, \{a, c, b\}, \{b, a, c\}, \{b, c, a\}, \{c, a, b\}, \{c, b, a\}$

3. $P(6, 6) = \dfrac{6!}{(6-6)!} = 720$

5.
   a) $P(6, 3) = \dfrac{6!}{(6-3)!} = 120$
   b) $P(6, 5) = \dfrac{6!}{(6-5)!} = 720$
   c) $P(8, 1) = \dfrac{8!}{(8-1)!} = 8$
   d) $P(8, 5) = \dfrac{8!}{(8-5)!} = 336$
   e) $P(8, 8) = \dfrac{8!}{(8-8)!} = 40,320$
   f) $P(10, 9) = \dfrac{10!}{(10-9)!} = 3,628,880$

7. $P(9, 5) = \dfrac{9!}{(9-5)!} = 15,120$

9. $P(12, 3 = \dfrac{12!}{(12-3)!} = 1,320$

11.
   a) $C(10, 4) = \dfrac{10!}{4!(10-4)!} = 210$
   b) $\displaystyle\sum_{i=0}^{4} C(10, i) = \sum_{i=0}^{4} \frac{10!}{i!(10-i)!} = 386$
   c) $\displaystyle\sum_{i=4}^{10} C(10, i) = \sum_{i=4}^{10} \frac{10!}{i!(10-i)!} = 848$
   d) $C(10, 5) = \dfrac{10!}{5!(10-5)!} = 252$

21.
   a) $P(5, 5) = \dfrac{5!}{(5-5)!} = 120$
   b) $P(4, 4) = \dfrac{4!}{(4-4)!} = 24$
   c) $P(5, 5) = \dfrac{5!}{(5-5)!} = 120$
   d) $P(4, 4) = \dfrac{4!}{(4-4)!} = 24$
   e) $P(3, 3) = \dfrac{3!}{(3-3)!} = 6$
   f) 0, as repetitions are not allowed

29.
   a) $C(25, 4) = \dfrac{25!}{4!(25-4)!} = 12,650$
   b) $P(25, 4) = \dfrac{25!}{(25-4)!} = 303,600$

37. $C(10, 2) = \frac{10!}{2!(10-2)!} = 45$

39. $\displaystyle\sum_{i=3}^{7} C(10, i) = \sum_{i=3}^{7} \frac{10!}{i!(10-i)!} = 912$

6.4 Binomial Coefficients and Identities

1.

6.5 Generalized Permutations and Combinations

5. $C(5+3-1,3) = \dfrac{(7)!}{3!(4)!} = 35$

9.

a) $C(8+6-1,6) = \dfrac{13!}{6!(7)!} = 1,716$

b) $C(8+12-1,12) = \dfrac{19!}{12!(7)!} = 50,388$

c) $C(8+24-1,24) = \dfrac{31!}{24!(7)!} = 2,629,575$

d) $C(8+4-1,4) = \dfrac{11!}{4!(7)!} = 330$

e) $\displaystyle\sum_{i=0}^{2} C(7+9-i-1,9-i) = \sum_{i=0}^{2} \frac{(15-i)!}{(9-i)!(6)!} = 9,724$

11. $C(2+8-1,8) = \dfrac{9!}{8!(1)!} = 9$

33. $\dfrac{11!}{5!2!2!1!1!} = 83,160$

35. $P(3,1) + [1 + P(3,2)] + \left[1 + 2\left(\dfrac{3!}{2!1!}\right) + P(3,3)\right] + \left[2\left(\dfrac{4!}{3!1!}\right) + \dfrac{4!}{2!1!1!}\right] + \left[\dfrac{5!}{3!1!1!}\right] = 63$

5 Induction and Recursion

5.1 Mathematical Induction

5.