

Homework Set 1

Arnav Patri

May 18, 2023

4 Number Theory and Cryptography

4.2 Integer Representations and Algorithms

1–11 odd, 21, 23

1. a) $231 = (11100111)_2$

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

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

21.

a)

$$\begin{array}{r} 100\overset{1}{0}\overset{1}{1}\overset{1}{1} \\ + 11110111 \\ \hline 10111110 \end{array}$$

b) $(1110\ 1111)_2 = 239$, $(1011\ 1101)_2 = 189$

$$239 + 189 = 428 = (1\ 1010\ 1100)_2$$

$$239 \times 189 = 45,171 = (1011\ 0000\ 0111\ 0011)_2$$

[illegible]

$$\begin{aligned}
\text{c) } (10\ 1010\ 1010)_2 &= 682, \\
(1\ 1111\ 0000)_2 &= 496 \\
682 + 496 &= 1,178 = (100\ 1001\ 1010)_2 \\
682 \times 496 &= 338,272 \\
&= (101\ 0010\ 1001\ 0110\ 0000)_2
\end{aligned}$$

$$\begin{aligned}
\text{d) } (10\ 0000\ 0001)_2 &= 513, \\
(11\ 1111\ 1111)_2 &= 1,023 \\
513 + 1,023 &= 1,536 = (110\ 0000\ 0000)_2 \\
513 \times 1,023 &= 524,799 \\
&= (1000\ 0000\ 0001\ 1111\ 1111)_2
\end{aligned}$$

23.

$$\begin{array}{r}
\begin{array}{r}
\overset{1}{1}\overset{1}{7}63 \\
+ 147 \\
\hline
1\ 1\ 3\ 2
\end{array} \\
\begin{array}{r}
\overset{7}{7}63 \\
\times 147 \\
\hline
\overset{1}{2}\overset{1}{6}\overset{1}{6}45 \\
\overset{1}{3}\overset{7}{7}14 \\
+ \overset{7}{7}63 \\
\hline
1\ 4\ 4\ 3\ 0\ 5
\end{array}
\end{array}$$

$$\begin{array}{r}
\text{b) } \begin{array}{r}
6001 \\
+ 272 \\
\hline
6273
\end{array} \\
\begin{array}{r}
001 \\
\times 272 \\
\hline
1\ 1\ 4\ 0\ 0\ 2 \\
5\ 2\ 0\ 0\ 7 \\
+ 14\ 0\ 0\ 2 \\
\hline
21\ 3\ 4\ 2\ 7\ 2
\end{array}
\end{array}$$

$$\begin{array}{r}
\text{c) } \begin{array}{r}
\overset{1}{1}\overset{1}{1}\overset{1}{1} \\
+ 777 \\
\hline
2110
\end{array} \\
\begin{array}{r}
\overset{1}{1}\overset{1}{1}\overset{1}{1} \\
\times 777 \\
\hline
7777 \\
7777 \\
+ 7777 \\
\hline
1\ 1\ 0\ 7\ 6\ 6\ 7
\end{array}
\end{array}$$

$$\begin{array}{r}
\text{d) } \begin{array}{r}
5\ 4\ 3\ 2\ 1 \\
+ 3456 \\
\hline
5\ 7\ 7\ 7\ 7
\end{array} \\
\begin{array}{r}
5\ 4\ 3\ 2\ 1 \\
\times 3456 \\
\hline
\overset{2}{1}\overset{1}{4}\overset{1}{1}\overset{1}{2}\overset{1}{3}\overset{1}{4}\overset{1}{6} \\
3\ 3\ 6\ 0\ 2\ 5 \\
2\ 6\ 1\ 5\ 0\ 4 \\
+ 2\ 0\ 5\ 1\ 6\ 3 \\
\hline
2\ 3\ 7\ 3\ 2\ 6\ 2\ 1\ 6
\end{array}
\end{array}$$

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 $\therefore \not\parallel 2$
- $29 = 10(3) - 1 \therefore \not\parallel 3$
- $29 = 6(5) - 1 \therefore \not\parallel 5 \therefore$ prime

c) $\sqrt{71} \approx 8.426$

- Odd $\therefore \not\parallel 2$
- $7 + 1 = 8 = 3(3) - 1 \therefore \not\parallel 3$
- $71 = 5(14) + 1 \therefore \not\parallel 5$
- $71 = 7(10) + 1 \therefore \not\parallel 7 \therefore$ prime

d) $\sqrt{97} \approx 9.849$

- Odd $\therefore \not\parallel 2$
- $97 = 3(32) + 1 \therefore \not\parallel 3$
- $97 = 5(19) + 2 \therefore \not\parallel 5$
- $97 = 7(14) - 1 \therefore \not\parallel 7 \therefore$ 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) $14 = 7 \times 2, 15 = 3 \times 5, 21 = 3 \times 7 \therefore$ 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, 7, 19, 21, 27, 33, 51

3. a) $4^{10} = 1,048,576$

b) $5^{10} = 9,765,625$

7. $26^3 = 17,576$

19. a) $3^6 = 729$

b) $4^4 = 256$

c) $4^5 = 1024$

d) $2^6 = 64$

21. a) $\{56, 63, 70, 77, 84, 91, 98\}, 7$

b) $\{55, 66, 77, 88, 99\}, 5$

c) $\{77\}, 1$

27. 3^{50}

33. a) 21^8

b) $C(21, 8) = \frac{21!}{8!(21-8)!} = 203,490$

c) 5×26^7

d) $5 \times C(26, 7) = 5 \times \frac{26!}{7!(26-7)!} = 3,289,000$

e) $26^8 - 21^8$

f) $8 \times 5 \times 21^7$

g) $26^7 - 21^7$

h) $26^6 - 21^6$

55. $25 + 16 - 8 = 33$

6.3 Permutations and Combinations

1–11, 21, 29, 37, 39 odd

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

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

5. a) $P(6, 3) = \frac{6!}{(6-3)!} = 120$

b) $P(6, 5) = \frac{6!}{(6-5)!} = 720$

c) $P(8, 1) = \frac{8!}{(8-1)!} = 8$

d) $P(8, 5) = \frac{8!}{(8-5)!} = 336$

e) $P(8, 8) = \frac{8!}{(8-8)!} = 40,320$

f) $P(10, 9) = \frac{10!}{(10-9)!} = 3,628,800$

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

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

11.

$$a) C(10, 4) = \frac{10!}{4!(10-4)!} = 210$$

$$b) \sum_{i=0}^4 C(10, i) = \sum_{i=0}^4 \frac{10!}{i!(10-i)!} = 386$$

$$c) \sum_{i=4}^{10} C(10, i) = \sum_{i=4}^{10} \frac{10!}{i!(10-i)!} = 848$$

$$d) C(10, 5) = \frac{10!}{5!(10-5)!} = 252$$

21.

$$a) P(5, 5) = \frac{5!}{(5-5)!} = 120 \quad b) P(4, 4) = \frac{4!}{(4-4)!} = 24 \quad c) P(5, 5) = \frac{5!}{(5-5)!} = 120$$

$$d) P(4, 4) = \frac{4!}{(4-4)!} = 24 \quad e) P(3, 3) = \frac{3!}{(3-3)!} = 6 \quad f) 0, \text{ as repetitions are not allowed}$$

29.

$$a) C(25, 4) = \frac{25!}{4!(25-4)!} = 12,650$$

$$b) P(25, 4) = \frac{25!}{(25-4)!} = 303,600$$

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

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

6.4 Binomial Coefficients and Identities

1–9 odd

1. a)

$$(x+y)^4 = (x+y)(x+y)(x+y)(x+y)$$

- x^4 and y^4 are only possible from a single combination each, so their coefficients are 1.
- x^3y and xy^3 terms arise by selecting the same product thrice, making their coefficients $C(4, 3) = 4$.
- x^2y^2 can be obtained by selecting x and y twice each, making their coefficients $C(4, 2) = 6$.

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

b)

$$\begin{aligned} (x+y)^4 &= \binom{4}{4}x^4y^0 + \binom{4}{3}x^3y^1 + \binom{4}{2}x^2y^2 + \binom{4}{1}x^1y^3 + \binom{4}{0}x^0y^4 \\ &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \end{aligned}$$

3.

$$\begin{aligned} (x+y)^6 &= \binom{6}{6}x^6y^0 + \binom{6}{5}x^5y^1 + \binom{6}{4}x^4y^2 + \binom{6}{3}x^3y^3 + \binom{6}{2}x^2y^4 + \binom{6}{1}x^1y^5 + \binom{6}{0}x^0y^6 \\ &= x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6 \end{aligned}$$

5. $100 + 1 = 101$

7. $\binom{19}{10}(2)^{10}(-x)^9 = -94,595,072x^9$

8. $\binom{200}{101}(2x)^{101}(-3y)^{99}$

6.5 Generalized Permutations and Combinations

5, 9, 11, 33, 35

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

9. a) $C(8 + 6 - 1, 6) = \frac{13!}{6!(7)!} = 1,716$ b) $C(8 + 12 - 1, 12) = \frac{19!}{12!(7)!} = 50,388$

c) $C(8 + 24 - 1, 24) = \frac{31!}{24!(7)!} = 2,629,575$ d) $C(8 + 4 - 1, 4) = \frac{11!}{4!(7)!} = 330$

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

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

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

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

5 Induction and Recursion

5.1 Mathematical Induction

5, 7, 9, 11, 13, 15, 17

5. Let

$$P(n) \implies \sum_{i=0}^n (2i + 1)^2 = \frac{(n + 1)(2n + 1)(2n + 3)}{3}$$

Let $n = 0$:

$$\sum_{i=0}^0 (2i + 1)^2 = \frac{(0 + 1)(0 + 1)(0 + 3)}{3}$$

$$(0 + 1)^2 = \frac{3}{3}$$

$$1 = 1 \implies P(0)$$

Assume that $P(k)$ is true for an arbitrary fixed integer $k > 0$:

$$\begin{aligned}
P(k) &\implies \sum_{i=0}^k (2i+1)^2 = \frac{(k+1)(2k+1)(2k+3)}{3} \\
&\sum_{i=0}^{k+1} (2i+1)^2 = \frac{(k+1)(2k+1)(2k+3)}{3} + (2k+3)^2 \\
&= (2k+3) \left(\frac{(k+1)(2k+1)}{3} + 2k+3 \right) \\
&= (2k+3) \left(\frac{2k^2 + k + 2k + 1 + 6k + 9}{3} \right) \\
&= \frac{(2k+3)(2k^2 + 9k + 10)}{3} = \frac{2k+3}{3} \frac{(2k+5)(k+2)}{3} \\
&= \frac{((k+1)+2)(2(k+1)+1)(2(k+1)+3)}{3} \implies P(k+1)
\end{aligned}$$

By mathematical induction, $P(n)$ is true for all integers $n \geq 0$.

7. Let

$$P(n) \implies \sum_{i=0}^n [3 \times 5^i] = \frac{3(5^{n+1} - 1)}{4}$$

Let $n = 0$:

$$\begin{aligned}
\sum_{i=0}^0 [3 \times 5^i] &= \frac{3(5^{0+1} - 1)}{4} \\
3 \times 5^0 &= \frac{3(4)}{4} \\
3 &= 3 \implies P(0)
\end{aligned}$$

Assume that $P(k)$ is true for an arbitrary fixed integer $k > 0$:

$$\begin{aligned}
P(k) &\implies \sum_{i=0}^k [3 \times 5^i] = \frac{3(5^{k+1} - 1)}{4} \\
&\sum_{i=0}^{k+1} [3 \times 5^i] = \frac{3(5^{k+1} - 1)}{4} + (3 \times 5^{k+1}) = \frac{3(5^{k+1}(1+4) - 1)}{4} \\
&= \frac{3(5^{k+2} - 1)}{4} = \frac{3(5^{(k+1)+1} - 1)}{4} \implies P(k+1)
\end{aligned}$$

By mathematical induction, $P(n)$ is true for all integers $n \geq 0$.

9. a)

$$\sum_{i=1}^n 2i = 2 \times \frac{n(n+1)}{2} = n(n+1)$$

b) Let

$$P(n) \implies \sum_{i=1}^n 2i = n(n+1)$$

Let $n = 1$:

$$\begin{aligned} \sum_{i=1}^1 2i &= 1(1+1) \\ 2 &= 2 = 2 \end{aligned}$$

Assume that $P(k)$ is true for an arbitrary fixed integer $k > 1$:

$$\begin{aligned} P(k) &\implies \sum_{i=1}^k 2i = k(k+1) \\ \sum_{i=1}^{k+1} 2i &= k(k+1) + 2(k+1) = k^2 + k + 2k + 1 = k^2 + 3k + 1 \\ &= (k+1)(k+2) \implies P(k+1) \end{aligned}$$

By mathematical induction, $P(n)$ is true for all integers $n \geq 1$.

11. a)

n	1	2	3
$\sum_{i=1}^n \frac{1}{2^i}$	$\frac{1}{2}$	$\frac{3}{4}$	$\frac{7}{8}$

$$\sum_{i=1}^n \frac{1}{2^i} = 1 - \frac{1}{2^n}$$

b) Let

$$P(n) \implies \sum_{i=1}^n \frac{1}{2^i} = 1 - \frac{1}{2^n}$$

Let $n = 1$:

$$\begin{aligned} \sum_{i=1}^1 \frac{1}{2^i} &= 1 - \frac{1}{2^1} \\ \frac{1}{2} &= \frac{1}{2} \implies P(1) \end{aligned}$$

Assume that $P(k)$ is true for an arbitrary fixed integer $k > 1$:

$$\begin{aligned} P(k) \implies \sum_{i=1}^k \frac{1}{2^i} &= 1 - \frac{1}{2^k} \\ \sum_{i=1}^{k+1} \frac{1}{2^i} &= 1 - \frac{1}{2^k} + \frac{1}{2^{k+1}} = 1 + \frac{1-2}{2^{k+1}} = 1 - \frac{1}{2^{k+1}} \implies P(k+1) \end{aligned}$$

By mathematical induction, $P(n)$ is true for all integers $n \geq 1$.

13. Let

$$P(n) \implies \sum_{i=1}^n (-1)^{i-1} i^2 = \frac{(-1)^{n-1} n(n+1)}{2}$$

Let $n = 1$:

$$\begin{aligned} \sum_{i=1}^1 (-1)^{i-1} i^2 &= \frac{(-1)^{1-1} 1(1+1)}{2} \\ 1 &= 1 \implies P(1) \end{aligned}$$

Assume that $P(k)$ is true for an arbitrary integer $k > 1$:

$$\begin{aligned} P(k) \implies \sum_{i=1}^k (-1)^{i-1} i^2 &= \frac{(-1)^{k-1} k(k+1)}{2} \\ \sum_{i=1}^{k+1} (-1)^{i-1} i^2 &= \frac{(-1)^{k-1} k(k+1)}{2} + (-1)^{k+1-1} (k+1)^2 \\ &= \frac{(-1)(-1)^k (k^2 + k) + 2(-1)^k (k^2 + 2k + 1)}{2} \\ &= \frac{(-1)^k (2k^2 + 4k + 2 - k^2 - k)}{2} = \frac{(-1)^k (k^2 + 3k + 2)}{2} \\ &= \frac{(-1)^k (k+1)(k+1)}{2} = \frac{(-1)^k (k+1)((k+1)+1)}{2} \implies P(k+1) \end{aligned}$$

By mathematical induction, $P(n)$ is true for all integers $n \geq 1$.

15. Let

$$P(n) \implies \sum_{i=1}^n i(i+1) = \frac{n(n+1)(n+2)}{3}$$

Let $n = 1$

$$\begin{aligned}\sum_{i=1}^1 i(i+1) &= \frac{1(1+1)(1+2)}{3} \\ 1(2) &= \frac{1(2)(3)}{3} \\ 2 &= 2 \implies P(1)\end{aligned}$$

Assume that $P(k)$ is true for an arbitrary fixed integer $k > 1$:

$$\begin{aligned}P(k) \implies \sum_{i=1}^k i(i+1) &= \frac{k(k+1)(k+2)}{3} \\ \sum_{i=1}^{k+1} i(i+1) &= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) = \frac{(k+3)(k+1)(k+2)}{3} \\ &= \frac{(k+1)((k+1)+1)((k+1)+2)}{3} \implies P(k+1)\end{aligned}$$

By mathematical induction, $P(n)$ is true for all integers $n \geq 1$.

17. Let

$$P(n) \implies \sum_{j=1}^n j^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

Let $n = 1$:

$$\begin{aligned}\sum_{j=1}^1 j^4 &= \frac{1(1+1)(2+1)(3+3-1)}{30} \\ 1 &= \frac{1(2)(3)(5)}{30} = \frac{30}{30} = 1 \implies P(1)\end{aligned}$$

Assume that $P(k)$ is true for an arbitrary integer $k > 1$:

$$\begin{aligned}P(k) \implies \sum_{i=1}^k j^4 &= \frac{k(k+1)(2k+1)(3k^2+3k-1)}{30} \\ \sum_{j=1}^{k+1} j^4 &= \frac{k(k+1)(2k+1)(3k^2+3k-1)}{30} + (k+1)^4 \\ &= \frac{(2k^3+3k^2+k)(3k^2+3k-1)}{30} + k^4 + 4k^3 + 6k^2 + 4k + 1 \\ &= \frac{6k^5 + 6k^4 - 2k^3 + 9k^4 + 9k^3 - 3k^2 + 3k^3 + 3k^2 - k}{30} \\ &\quad + k^4 + 4k^3 + 6k^2 + 4k + 1 \\ &= \frac{6k^5 + 45k^4 + 130k^3 + 180k^2 + 119k + 30}{30} \\ &= \frac{(k+1)((k+1)+1)(2(k+1)+1)(3(k+1)^2+3(k+1)-1)}{30} \\ &\implies P(k+1)\end{aligned}$$

By mathematical induction, $P(n)$ is true for all integers $n \geq 1$.