Problem 3.5

(a) You start with one robot. Each moment this robot can either self-destruct, do nothing, make one copy of itself, or make two copies of itself, each with equal probability. What is the probability that you eventually end up with no robots?

Solution Let p denote the probability that eventually there are no robots left and for a robot X write A_X for the event $\{X$ and all its descendants are destroyed eventually$\}$. Let X be the name of our original robot. Using the law of total probability we condition on what happens at the first step:

$$\begin{aligned} p =& \mathbb{P}(A) \\ =& \mathbb{P}(A \mid X \text{ destroys itself}) \mathbb{P}(X \text{ destroys itself}) \\ &+ \mathbb{P}(A \mid X \text{ stays put}) \mathbb{P}(X \text{ stays put}) \\ &+ \mathbb{P}(A \mid X\text{makes a copy } Y) \mathbb{P}(X \text{ makes a copy } Y) \\ &+ \mathbb{P}(A \mid X \text{ makes two copies } X, Y) \mathbb{P}(X \text{ makes two copies } X, Y) \\ &= \frac{1}{4} + \frac{1}{4}p + \frac{1}{4}p^2 + \frac{1}{4}p^3 \\ &= \frac{1+p+p^2+p^3}{4}, \end{aligned}$$

where we used that once created, the robots Y, Z operate independently of each other and X. The cubic equation

$$p = \frac{1+p+p^2+p^3}{4}$$

has three solutions $1, \sqrt{2}-1$ and $-\sqrt{2}-1$. This tells us that p must be 1 or $\sqrt{2}-1$. To argue that p cannot be 1 we note that the expected number of robots after n steps is exatly $(3/2)^n > 1$, which would contradict $p = 1$. Therefore $p = \sqrt{2}-1$.

(b) You start with 0 coins and each turn you receive a number of coins equal to the roll of the die with sides numbered (1, 2, 2, 2, 2, 3). What is the probability that you eventually have n coins?

Solution Let X denote the sequence of dice rolls $X_1, X_2, \ldots$ that we observe. Denote the event that the cumulative sum of dicerolls in X hits n at some step. Our aim is to calculate $a_n := \mathbb{P}(A_{X,n})$. Conditioning on the first diceroll X_1 and applying the law of total probability we obtain

$$\begin{aligned} \mathbb{P}(A_{X,n}) =& \mathbb{P}(A_{X,n} \mid X_1 = 1) \mathbb{P}(X_1 = 1) \\ &+ \mathbb{P}(A_{X,n} \mid X_1 = 2) \mathbb{P}(X_1 = 2) \\ &+ \mathbb{P}(A_{X,n} \mid X_1 = 3) \mathbb{P}(X_1 = 3). \end{aligned}$$

Since the dicerolls are independent, above is equal to

$$= \frac{1}{6}\mathbb{P}(A_{Y,n-1}) + \frac{4}{6}\mathbb{P}(A_{Y,n-2}) + \frac{1}{6}\mathbb{P}(A_{Y,n-3}).$$

Let Y be the sequence of dicerolls $X_2, X_3, \ldots$ and note that $a_m = \mathbb{P}(A_{X,m}) = \mathbb{P}(A_{Y,m})$ for all m because X_1 is independent of $X_2, X_3 \ldots$. Therefore, in terms of a_n the above can be written as

$$a_n = \frac{1}{6}a_{n-1} + \frac{2}{3}a_{n-2} + \frac{1}{6}a_{n-3}.$$

The characteristic equation of this recurrence relation reads

$$\lambda^3 - \frac{1}{6}\lambda^2 - \frac{2}{3}\lambda^2 - \frac{1}{6} = 0$$

and has solutions $1, -1/2$ and $-1/3$. This suggests the form

$$a_n = C_1 + C_2\left(-\frac{1}{2}\right)^n + C_3\left(-\frac{1}{3}\right)^n$$

for unknown constants C_1, C_2, C_3 and all integers $n \geq 0$. To figure out the constants we look at the initial conditions:

$$\begin{aligned} a_0 &= 1 = C_1 + C_2 + C_3 \\ a_1 &= \frac{1}{6} = C_1 - \frac{C_2}{2} - \frac{C_3}{3} \\ a_2 &= \frac{25}{36} = C_1 + \frac{C_2}{4} + \frac{C_3}{9}. \end{aligned}$$

Solving the above system of equations for C_1, C_2 and C_3 we arrive at our answer

$$a_n = \frac{1}{2} + \left(-\frac{1}{2}\right)^n - \frac{1}{2}\left(-\frac{1}{3}\right)^n.$$

Problem 4.4

Let a be a positive integer such that $7|a-2$ and $7^k|a^6-1$ for some positive integer k. Show that $7^k|(a+1)^6-1$.

Solution We will use the following three identities:

$$\begin{aligned} x^2 - y^2 &= (x-y)(x+y) \\ x^3 - y^3 &= (x-y)(x^2+xy+y^2) \\ x^3 + y^3 &= (x+y)(x^2+xy+y^2) \end{aligned}$$

for all $x, y \in \mathbb{R}$. Armed with the above we obtain

$$\begin{aligned} a^6 - 1 &= (a^3-1)(a^3+1) \\ &= (a-1)(a^2+a+1)(a+1)(a^2-a+1) \end{aligned} \tag{1}$$

as well as

$$\begin{aligned} (a+1)^6 - 1 &= ((a+1)^3-1)((a+1)^3+1) \\ &= ((a+1)-1)((a+1)^2+(a+1)+1)((a+1)+1)((a+1)^2-(a+1)+1) \\ &= a(a^2+3a+2)(a+2)(a^2+a+1). \end{aligned} \tag{2}$$

Recall that $a \equiv 2 \pmod 7$. Modular arithmetic tells us that the only term in (1) that is divisible by 7 is (a^2+a+1). Since $7^k|a^6-1$ this implies that $7^k|(a^2+a+1)$. But this term also divides $(a+1)^6-1$ by (2) and the conclusion follows.

Problem 5.2

(a) In $x^3 + px^2 + qx + r$ one zero is the sum of the two others. Find an expression for r in terms of p, q.

Solution Let $a, b, a+b$ be the roots of the polynomial. Vieta's formula tells us that

$$\begin{aligned} p &= -2(a+b) \\ q &= (a+b)^2 + ab \\ r &= -ab(a+b). \end{aligned}$$

We see that $a+b=-p/2$ and so $ab=-r/(-p/2)=2r/p$. Plugging in we obtain

$$q=\frac{p^2}{4}+\frac{2r}{p}.$$

(b) Let a, b, c be nonzero real numbers such that $a+b+c\neq 0$ and

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=\frac{1}{a+b+c}. \tag{3}$$

Prove that for all odd $n\geq 1$ it holds that

$$\frac{1}{a^n}+\frac{1}{b^n}+\frac{1}{c^n}=\frac{1}{a^n+b^a+c^n}.$$

Solution 1 Let us define $p=a+b+c$, $q=ab+ac+bc$ and $r=abc$. Rearranging (3) a bit we see it is equivalent to

$$\frac{q}{r}=\frac{1}{p}.$$

Let $P(x)$ be the third degree monic polynomial with roots a, b and c so that

$$\begin{aligned}P(x)&=(x-a)(x-b)(x-c)\\&=x^3-px^2+qx-r\\&=x^3-px^2+qx-pq.\end{aligned}$$

We can easily factor $P(x)$ to get

$$P(x)=(x^2+q)(x-p).$$

Above factorization tells us that the three roots a, b, c are $p, \sqrt{q}, -\sqrt{q}$ in some order, where $\sqrt{q}$ may be imaginary. Therefore, a^n, b^n, c^n must be $p^n, \sqrt{q}^n, -\sqrt{q}^n$ in some order, where we used that n is odd. Thus

$$\begin{aligned}\frac{1}{a^n}+\frac{1}{b^n}+\frac{1}{c^n}&=\frac{1}{p^n}+\frac{1}{\sqrt{q}^n}-\frac{1}{\sqrt{q}^n}\\&=\frac{1}{p^n}\\&=\frac{1}{p^n+\sqrt{q}^n-\sqrt{q}^n}\\&=\frac{1}{a^n+b^n+c^n},\end{aligned}$$

as required.

Solution 2 (Alayah Hines) Multiplying by $abc(a+c+b)$ in (3) we have

$$(ab+ac+bc)(a+b+c)=abc.$$

Expanding and factoring in a smart fashion we get

$$\begin{aligned}abc&=(ab+ac+bc)(b+c)+(ab+ac+bc)a\\&=(ab+ac+bc)(b+c)+a^2(b+c)+abc\\&=(b+c)(a(b+a)+c(b+a))+abc\\&=(b+c)(b+a)(a+c)+abc.\end{aligned}$$

Upon subtracting abc from both sides, we have shown that (3) is equivalent to

$$(a+b)(b+c)(a+c) = 0. \tag{4}$$

This implies in particular that one of $a = -b, b = -c, a = -c$ must hold. In either case, for odd n we will have

$$(a^n + b^n)(a^n + c^n)(b^n + c^n) = 0. \tag{5}$$

Performing the same transformations backwards we arrive at the desired expression

$$\frac{1}{a^n} + \frac{1}{b^n} + \frac{1}{c^n} = \frac{1}{a^n + b^n + c^n}. \tag{6}$$