Appendix A

Solutions of Exercises

1. Fundamentals

1. $X = \{(-1,0),(-1,1),(0,0),(0,1),(1,0),(1,1)\}$, $|X| = 6$ and $Y = \{1,2,3,4,5,6\}$. The map $f : X \to Y$ given by $f(-1,0) = 1$, $f(-1,1) = 2$, $f(0,0) = 3$, $f(0,1) = 4$, $f(1,0) = 5$ and $f(1,1) = 6$ is bijective.

2. a) f_1 is injective, $im(f_1) = \{3,5,7,\dots\}$, not surjective.
b) f_2 is not injective, since for example $f_2(-1) = f_2(1) = 2$, but surjective.
c) f_3 is bijective, $f_3^{-1} = f_3$.
d) f_4 is neither injective nor surjective.

3. We construct injective maps $f : X \to \mathbb{N}$. Note that there are many other injective maps. a) Let $X = \mathbb{Z}$. Set $f(k) = \begin{cases} 2k+1 & \text{if } k \geq 0 \\ -2k & \text{if } k < 0 \end{cases}$.
f maps nonnegative integers to even numbers and negative numbers to odd numbers. f is a bijection.
b) Let $X = \mathbb{N}^2$. Set $f(k_1,k_2) = 2^{k_1}3^{k_2}$. f is injective and hence $\mathbb{N}^2$ is countable. It follows easily that $\mathbb{Z}^2$ is also countable.
c) Let $\mathbb{Q}^+$ the set of positive rational numbers. Set $f(\frac{k_1}{k_2}) = 2^{k_1}3^{k_2}$, where $k_1,\ k_2 \in \mathbb{N}$ and $k_2 \nmid k_1$. Then f is injective and hence $\mathbb{Q}^+$ is countable. It follows easily that $\mathbb{Q}$ is also countable.

4. If f is injective, then $|im(f)| = |X| = |Y|$ and hence $im(f) = Y$, so that f is surjective.
If f is surjective, then $|im(f)| = |Y| = |X|$. Hence f must be injective.

5. $\mathbb{Z}_{26} = \{\overline{0}, \overline{1}, \dots, \overline{25}\}$. The standard representatives of the given integers modulo 26 are: 14, 22, 25, 15, 25 and 9.

6. a) If $x \in f^{-1}(B)$, then $f(x) \in B$ which shows $f(f^{-1}(B)) \subset B$. Let $y \in B$. If f is surjective, then there exists $x \in X$ such that $f(x) = y$. Furthermore, we have $x \in f^{-1}(B)$, which gives $B \subset f(f^{-1}(B))$.
b) Let $x \in A$. Then $f(x) \in f(A)$ and $x \in f^{-1}(f(A))$. If f is injective and

$x \in f^{-1}(f(A))$, then $y = f(x) \in f(A)$. Since x is the only element with $f(x) = y$, we have $x \in A$.

7. $(x, x) \in S$ since $x - x = 0 \in \mathbb{Z}$.
$(x, y) \in S$ implies $x - y \in \mathbb{Z}$. But then $y - x \in \mathbb{Z}$ and $(y, x) \in S$.
$(x, y) \in S$ and $(y, z) \in S$ yields $x-y \in \mathbb{Z}$ and $y-z \in \mathbb{Z}$. Therefore, $x-y+y-z = x - z \in \mathbb{Z}$ which implies $(x, z) \in S$.
Hence S defines an equivalence relation on $\mathbb{R}$. We have $\overline{0} = \overline{-2} = \mathbb{Z}$ and $\overline{\frac{4}{3}} = \frac{4}{3} + \mathbb{Z}$. The map $f : [0, 1[\to \mathbb{R}/\sim$ with $f(x) = \overline{x}$ is a bijection.

8. $f_1 = O(n^3)$, polynomial.
$f_2 = O(2^n)$, exponential.
$f_3 = O(n^{1/2})$, polynomial.
$f_4 = O(\frac{1}{2^{n/2-\ln(n)}})$, negligible.
$f_5 = O(1)$, polynomial.
$f_6 = O(2^{n/3})$ exponential.

9. $f(x_0, x_1, x_2) = x_0x_1x_2 + x_0x_1 + x_1x_2 + x_2 + 1$. $\deg(f) = 3$.

10. The exponent is significantly reduced by the cubic root. $f(n)$ is sub-exponential, but grows faster than any polynomial. Set $n = 2^b$ and compute the effective key length:

$$\log_2(f(2^b)) = \frac{2\ln(2^b)^{1/3}}{\ln(2)} = \frac{2\ln(2)^{1/3} \cdot b^{1/3}}{\ln(2)}$$

For $b = 128$ and $b = 1024$ this gives 12.87 and 25.74 effective key bits, respectively.

11. The number of ones (or zeros) in a uniform random byte follows a binomial distribution with $n = 8$. One has $\binom{8}{4} = 70$ and $Pr[Y = 4] = 70\left(\frac{1}{2}\right)^8 \approx 0.27$.

12. Since $Y = X_1 + \cdots + X_n$ (with $X_i = X$) and $E[X_i] = p$ one obtains $E[Y] = np$. The Bernoulli tries are independent and from $V[X_i] = p(1-p)$ one concludes that $V[Y] = np(1-p)$.

13. $Pr[X + Y \geq 10] = \frac{1}{6}$, $Pr[X + Y \geq 10 \mid X - Y = 0] = \frac{1}{3}$.
$X + Y$ and $X - Y$ are not independent.
$E[X + Y] = 7$, $E[X - Y] = 0$, $V[X + Y] = V[X - Y] = \frac{35}{6}$.

14. The output of the new generator is uniformly distributed, but the bits are not independent since after 100 bits each output bit depends on the preceding 100 bits. So it is not a Random Bit Generator. Furthermore, it is also not a pseudorandom generator (see Chapter 2) since an adversary can distinguish the output from a random sequence by XORing 100 successive bits and comparing the result with the next bit.

15. $k = 184$. The least period is 46.

16. a) The inequality $(1 - \frac{i}{n}) \leq e^{-i/n}$ and

$$\prod_{i=0}^{k-1} e^{-i/n} = e^{\sum_{i=0}^{k-1}(-i/n)} = e^{-k(k-1)/(2n)} .$$

imply that the probability that no collision occurs is less than $e^{-k(k-1)/(2n)}$. We conclude that the probability for a collision is at least

$$1 - e^{-k(k-1)/(2n)} \ .$$

b) For a probability of $\frac{1}{2}$, one obtains

$$\frac{1}{2} = e^{-k(k-1)/(2n)} \Longleftrightarrow \ln(2) = \frac{1}{2n} k(k-1) \ .$$

We approximate $k(k-1)$ by k^2 and obtain $2n\ln(2) = k^2$, so that

$$k = \sqrt{2n\ln(2)} \approx 1.2\sqrt{n} \ .$$

This is the approximate number of random values such that a collision occurs with a probability of at least $\frac{1}{2}$.