Solutions of Exercises

1. Fundamentals

1. $X = \{(-1,0),(-1,1),(0,0),(0,1),(1,0),(1,1)\}$, $|X| = 6$, $Y = \{1,2,3,4,5,6\}$. 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 $f : X \to \mathbb{N}$, which shows that X is countable. Note that there are many other injective maps.
   (a) Let $X = \mathbb{Z}$ and $k \in \mathbb{Z}$. Set
   $$f(k) = \begin{cases} 2k+1 & \text{for } k \geq 0 \\ -2k & \text{for } k < 0 \end{cases}.$$
   f maps the non-negative integers to odd natural numbers and the negative numbers to even natural numbers. f is a bijection.
   (b) Let $X = \mathbb{Z}^2$. Define the Heavyside function $H : \mathbb{R} \to \{0,1\}$ by
   $$H(x) = \begin{cases} 1 & \text{for } x \geq 0 \\ 0 & \text{for } x < 0 \end{cases}.$$
   Let $(k_1,k_2) \in \mathbb{Z}^2$. Then set
   $$f(k_1,k_2) = 2^{k_1}3^{k_2}5^{H(k_1)}7^{H(k_2)}.$$
   The map f is injective and so $\mathbb{Z}^2$ is countable.
   (c) Let $X = \mathbb{Q}$ and $\frac{p}{q} \in \mathbb{Q}$, where $p \in \mathbb{Z}$, $q \in \mathbb{N}$ and $q \nmid p$. Set
   $$f\left(\frac{p}{q}\right) = 2^p 3^q 5^{H(p)}.$$
   f is injective and hence $\mathbb{Q}$ is countable.

4. If f is injective, then $|im(f)| = |X| = |Y|$ and $im(f) = Y$. Hence f is surjective.
   If f is surjective, then $|im(f)| = |Y| = |X|$. Hence f must be injective.
5. (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 $x \in f^{-1}(f(A))$. Now assume that 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 $x \in A$. Hence $f^{-1}(f(A)) \subset A$.
6. $\mathbb{Z}_{26} = \{\overline{0}, \overline{1}, \ldots, \overline{25}\}$. The standard representatives of the given integers modulo 26 are 14, 22, 25, 15, 25 and 9, respectively.
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 denote the equivalence class of x by $[x]$. We have $[0] = [-2] = \mathbb{Z}$ and $[\frac{4}{3}] = \frac{4}{3} + \mathbb{Z}$. The map $f : [0, 1[\to \mathbb{R}/\sim$ with $f(x) = [x]$ is a bijection.
8. $f(x_0, x_1, x_2) = x_0x_1x_2 + x_0x_1 + x_1x_2 + x_2 + 1$. $\deg(f) = 3$.

```
sage: from sage.crypto.boolean_function import BooleanFunction
sage: B= BooleanFunction([1,1,1,0,0,0,1,1])
sage: B.algebraic_normal_form()
x0*x1*x2 + x0*x1 + x1*x2 + x2 + 1
```

9. $f_1 = O(n^3)$, 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.
   $f_7 = O(\ln(n)^2 n) = \tilde{O}(n)$, polynomial.
10. The exponent is significantly reduced by the cubic root. $f(n)$ is sub-exponential, but grows faster than any polynomial.

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

    For $n = 128,\ 1024,\ 2048$ this gives 14.5, 29.1 and 36.6 effective key bits, respectively.
11. The number of ones (or zeros) in a uniform random byte follows a binomial distribution with $n = 8$ and $p = \frac{1}{2}$. We have $\binom{8}{4} = 70$ 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 $E[X_i] = p$, we obtain $E[Y] = np$. The Bernoulli tries are independent, and from $V[X_i] = p(1-p)$ we conclude 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.
    $E[X + Y] = 7$, $E[X - Y] = 0$, $V[X + Y] = V[X - Y] = \frac{35}{6}$. The standard deviation of $X + Y$ and $X - Y$ is $\sqrt{\frac{35}{6}} \approx 2.4$.

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. Hence it is not a random bit generator. Furthermore, it is 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. We compute a collision $x_k = x_{2k}$ using Floyd's algorithm.

```
sage: def f(x):
          return(x*x+1)
      x=mod(1,56807)
      y=mod(1,56807)
      x=f(x)
      y=f(f(y))
      k=1

      while x!=y:
          x=f(x)
          y=f(f(y))
          k=k+1
      print "k␣=",k,"␣x␣=",x
k = 184  x = 22604
```

Hence $k = 184$. The least period divides 184.

```
sage: x0 = mod(22604,56807)
      x = f(x0)
      k=1
      while x!=x0:
          x = f(x)
          k=k+1
      print k
46
```

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 samples such that a collision occurs with a probability of at least 50%.