Section 3.6

4. Converting integers from binary to decimal notation is done by adding up appropriate powers of 2, depending on the bits in the binary representation, as in Example 1 on page 219. Specifically, \((b_n \ldots b_1 b_0)_2 = \sum_{i=0}^{n} b_i \cdot 2^i\). For example, \((1 \ 1011)_2 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 = 1 + 2 + 8 + 16 = 27\).

2. The last bit of base-2 representation of \(n\) is \((n \mod 2)\), and to get the remaining bits recurse on \((n \div 2)\). This procedure is explained in Example 5 on page 221. This way you get \((321)_{10} = (1\ 0100\ 0001)_2\), because
\[
321 \mod 2 = 1, \quad (321 - 1) \div 2 = 160
\]
\[
160 \mod 2 = 0, \quad (160 - 0) \div 2 = 80
\]
\[
80 \mod 2 = 0, \quad (80 - 0) \div 2 = 40
\]
\[
40 \mod 2 = 0, \quad (40 - 0) \div 2 = 20
\]
\[
20 \mod 2 = 0, \quad (20 - 0) \div 2 = 10
\]
\[
10 \mod 2 = 0, \quad (10 - 0) \div 2 = 5
\]
\[
5 \mod 2 = 1, \quad (5 - 1) \div 2 = 2
\]
\[
2 \mod 2 = 0, \quad (2 - 0) \div 2 = 1
\]
\[
1 \mod 2 = 1, \quad (1 - 0) \div 2 = 0, \text{ so we stop here.}
\]

Now you just need to order the bits appropriately, namely the least-significant bit was first and the most-significant one was last.

Similarly \((1023)_{10} = (11\ 1111\ 1111)_2\). You can verify that these representations are correct by checking that \(321 = 2^0 + 2^6 + 2^8\) and that \(1023 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9\).\(^1\)

12. By theorem 1 on page 219 we have that
\[
(a_k \ldots a_0)_{16} = \sum_{i=0}^{k} a_i \cdot 16^i
\]
If you denote the binary representation of hexadecimal digit \((a_i)_{16}\) as \((b_{4i+3} b_{4i+2} b_{4i+1} b_{4i})_2\), then
\[
a_i = \sum_{j=0}^{3} b_{4i+j} \cdot 2^j
\]
and therefore
\[
a_i \cdot 16^i = a_i \cdot 2^{4i} = \left(\sum_{j=0}^{3} b_{4i+j} \cdot 2^j\right) \cdot 2^{4i} = \sum_{j=0}^{3} b_{4i+j} \cdot 2^{4i+j}
\]
Consequently,
\[
(a_k \ldots a_0)_{16} = \sum_{i=0}^{k} a_i \cdot 16^i = \sum_{i=0}^{k} \sum_{j=0}^{3} b_{4i+j} \cdot 2^{4i+j}
\]
But if you denote \(4i + j\) as \(t\), this can be re-written as
\[
\sum_{t=0}^{4k+3} b_t \cdot 2^t
\]
And therefore
\[
(a_k \ldots a_0)_{16} = (b_{4k+3} \ldots b_0)_2
\]
where each block of four consecutive bits \((b_{4i+3} \ldots b_4i)_2\) is a binary representation of \((a_i)_{16}\).

\(^1\)Actually if you remember different powers of 2, and it’s very useful for a computer-science to remember powers of 2, you might notice that \(1023 + 1 = 1024 = 2^{10}\), and since \(2^{10} = (100\ 0000\ 0000)_2\), it follows that \(2^{10} - 1 = (100\ 0000\ 0000)_2 - (1)_2 = (11\ 1111\ 1111)_2\).
6.8. Now converting between hexadecimal and binary should be easy. For example, $\text{(BAD)}_{16} = (1011 1010 1101)_{2}$ because $\text{(B)}_{16} = 11 = (1011)_{2}$, $\text{(A)}_{16} = 10 = (1010)_{2}$, and $\text{(D)}_{16} = 13 = (1101)_{2}$, because $\text{(B)}_{16} = 11 = (1011)_{2}$, $\text{(A)}_{16} = 10 = (1010)_{2}$, and $\text{(D)}_{16} = 13 = (1101)_{2}$. Similarly

$(\text{BADFACE}D)_{16} = (1011 1010 1101 1111 1101 1100 1110 1101)_{2}$

Conversely, $(1111 0111)_{2} = (F7)_{16}$ because $(1111)_{2} = 15 = (F)_{16}$ and $(0111)_{2} = 7 = (7)_{16}$, etc.

If you are not sure how these conversions work, read the examples in the book, ask the TA to go over it, practice with even-numbered exercises which have the solutions at the end of the book, and come to our office hours.

20. We are to compute $11^{644}$ mod 645. To use the square-and-multiply exponentiation algorithm we need to first represent the exponent in binary. Here $644 = (10 1000 0100)_{2}$. If you use the algorithm from the slides, you start with $k = 9$ and $x = 1$, and here are each iterations of the main loop:

Since $a_{0} = 1$, $x$ becomes $(x * 11)^{2} = 121$ mod $645 = 121$

Since $a_{8} = 0$, $x$ becomes $x^{2} = 121^{2} = 14,641 = 451$ mod $645$.

Since $a_{7} = 1$, $x$ becomes $(x * 11)^{2} = (451 * 11)^{2} = (4,961)^{2} = (446)^{2} = 198,916 = 256$ mod $645$. In the middle of this transformation we used the fact that $4,961 = 446$ mod $645$.

Since $a_{6} = 0$, $x$ becomes $x^{2} = (256)^{2} = 65,536 = 391$ mod $645$.

Since $a_{5} = 0$, $x$ becomes $x^{2} = (391)^{2} = 152,881 = 16$ mod $645$.

Since $a_{4} = 0$, $x$ becomes $x^{2} = (16)^{2} = 256$.

Since $a_{3} = 0$, $x$ becomes $x^{2} = (256)^{2} = 65,536 = 391$ mod $645$.

Since $a_{2} = 1$, $x$ becomes $(x * 11)^{2} = (391 * 11)^{2} = 4,301^{2} = 431^{2} = 185,761 = 1$ mod $645$.

Since $a_{1} = 0$, $x$ becomes $x^{2} = 1$.

Since $a_{0} = 0$, $x$ becomes $x^{2} = 1$, so the final answer is that $11^{644} = 1$ mod $645$.

You can check that this is true by the Chinese Remainder Theorem on page 235. Using CRT, one can find $s = 11^{644}$ mod $m$ from $s_{1} = 11^{644}$ mod $p_{1}$, ..., $s_{n} = 11^{644}$ mod $p_{n}$, where $p_{1},...,p_{n}$ is a factorization of $m$. The general procedure for computing $s$ in terms of $(s_{1},...,s_{n})$ and $(p_{1},...,p_{n})$ is more complex, but in particular it holds that if $s_{1} = ... = s_{n} = 1$ then $s = 1$. (Can you convince yourself that this special case of CRT is true? It’s not difficult: You can prove it by counterpositive, i.e. assuming that $s \neq 1$ mod $m$ you can show that there must exist $i$ s.t. $s_{i} \neq 1$ mod $p_{i}$.)

Using the above fact, we’ll show that $s = 1$ by showing that $11^{644} = 1$ mod $p_{i}$ for each prime factor $p_{i}$ of $m = 645$. We’ll do that using the Fermat’s theorem which says that $a^{b} = a^{b \mod p - 1} \mod p$ if $p$ is prime. Note that the factorization of 645 is $3 * 5 * 43$.

Note that $644 \mod 2 = 0$, and therefore by Fermat’s theorem (which applies because 3 is prime), $11^{644} = 11^{0} = 1$ mod 3.

Similarly, $644 \mod 4 = 0$, and therefore by Fermat’s theorem (which applies because 5 is prime), $11^{644} = 11^{0} = 1$ mod 5.

Finally, $644 \mod 42 = 14$, and therefore by Fermat’s theorem (which applies because 43 is prime), $11^{44} = 11^{14}$ mod 43. However, you can check by hand that $11^{14} = 1$ mod 43. (Even better, you can run a mini square-and-multiply algorithm to compute $11^{14}$ mod 43 using the binary expansion of $14 = (1110)_{2}$.)

Therefore, since $11^{644}$ is equal to 1 modulo all prime factors of 645, by CRT we get that it is also equal to 1 modulo 645.

---

2We have not discussed this theorem, so it’s an optional material, but it’s very useful!
Section 4.1

First Exercise: The formula for cardinality of the power set.

The predicate $Q(n)$ we are proving says that for all sets $S$ of cardinality $n$, there are $2^n$ subsets of $S$, and we need to prove this predicate for all non-negative $n$.

The base case is $n = 0$ in which case $S$ is an empty set and therefore it has one subset, the empty set, and hence the formula holds because $2^0 = 1$.

The inductive case is to prove that if for any $k \geq 0$ assumption $Q(k)$ holds, i.e. if the cardinality of a power set of any set of $k$ elements is $2^k$, then $Q(k + 1)$ holds. Now, what is $Q(k + 1)$? $Q(k + 1)$ says that for any set $S$ of cardinality $k + 1$ the number of its subsets is $2^{k+1}$. Let $a$ be any element of $S$ (since $k + 1 \geq 1$ the set $S$ is non-empty), and let’s divide the set $P(S)$ of subsets of $S$ into two categories (i.e. into two sets):

- $C_0$ is the set of subsets of $S$ which do not include $a$,
- $C_1$ is the set of subsets of $S$ which do include $a$.

Now, note that $C_0$ is identical to the set of (all) subsets of set $S' = S - \{a\}$. But since $|S'| = |S| - 1 = k$, we can use the inductive hypothesis to conclude that there are $2^k$ subsets in category $C_0$.

Note that $C_1$ and $C_0$ have exactly the same number of elements because for every set $X$ in $C_0$ there is a unique set $x \cup \{a\}$ in $C_1$, and for every set $Y$ in $C_1$ there is a unique set $y - \{a\}$ in $C_0$. Therefore $C_1$ has the same number of elements as $C_0$, i.e. $2^k$. And therefore $P(S)$ has $2^k + 2^k = 2^{k+1}$ elements, as needed.

4. Denote $SC_n = 1^3 + 2^3 + \ldots + n^3$.

a Statement $P(1)$ is that $SC_1 = 1 = (1 * 2/2)^2$.

b The statement is obviously true.

c The inductive hypothesis is that $P(k)$ is true for some $k \geq 1$, i.e. that $SC_k = (k(k + 1)/2)^2$.

d To prove the inductive step we need to prove $P(k + 1)$, i.e. that $SC_{k+1} = ((k+1)(k+2)/2)^2$, assuming the inductive hypothesis stated above.

e Observe that $SC_{k+1} = SC_k + (k + 1)^3$, and therefore by inductive hypothesis we have

\[
SC_{k+1} &= (k(k + 1)/2)^2 + (k + 1)^3 \\
&= (k + 1)^2 * ((k/2)^2 + (k + 1)) \\
&= (k + 1)^2 * (k^2 + 4k + 4)/4 \\
&= (k + 1)^2 * ((k + 2)/2)^2 \\
&= ((k + 1)(k + 2)/2)^2
\]

f Since we showed $P(1)$ and we showed that, for every $k \geq 1$, if $P(k)$ then $P(k + 1)$, by the principle of induction it follows that $P(n)$ for all $n \geq 1$.

6. Let $S_n = 1 * 1! + 2 * 2! + \ldots n * n!$. The predicate $P(n)$ is that $S_n = (n + 1)! - 1$. We want to prove $P(n)$ for all positive $n$. The base step is $n_0 = 1$, i.e. that $S_1 = 2! - 1 = 1$, which is true. The inductive step is that assuming that $P(k)$ is true, i.e. that $S_k = (k + 1)! - 1$ for some $k \geq 1$, we need to show that $P(k + 1)$ is true, i.e. that $S_{k+1} = (k + 2)! - 1$. So let’s examine what $S_{k+1}$ is and let’s try to relate it to $S_k$ and use the inductive assumption we have:

\[
S_{k+1} &= S_k + (k + 1)(k + 1)! \quad \text{by definition of } S_{k+1} \\
&= (k + 1)! - 1 + (k + 1)(k + 1)! \quad \text{by the inductive assumption} \\
&= (k + 1)![(k + k + 1) - 1] \\
&= (k + 1)!(k + 2) - 1 \\
&= (k + 2)! - 1
\]
And this is what we were supposed to show so this completes the inductive step, and by the principle of induction, the two steps imply that \( P(n) \) is true for all positive integers \( n \).

10. Let \( S_n = 1/(1*2) + 1/(2*3) + ... + 1/(n*(n+1)) \). By evaluating the first few terms it seems that \( S_n = n/(n+1) \). Our predicate \( P(n) \) is that this equality indeed holds for \( n \). Let’s prove it for all positive \( n \). The base case, for \( n_0 = 1 \), is true because \( S_1 = 1/2 \). Now the inductive step: Assuming that \( S_k = k/(k+1) \) for some \( k \geq 1 \), let’s prove that \( S_{k+1} = (k+1)/(k+2) \):

\[
S_{k+1} = \frac{S_k + 1}{(k+1)(k+2)} \quad \text{by definition of } S_{k+1}
\]

\[
= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \quad \text{by the inductive assumption}
\]

\[
= \frac{k(k+2)}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)}
\]

\[
= \frac{k^2 + 2k + 1}{(k+1)(k+2)}
\]

\[
= \frac{(k+1)^2}{(k+1)(k+2)}
\]

\[
= \frac{k+1}{k+2}
\]

This completes the inductive step, and hence by the principle of induction, these two steps shows that \( S_n = n/(n+1) \) for every positive integer \( n \).

18. 

a \( P(2) \) says that \( 2! < 2^2 \).

b \( P(2) \) is obviously true because \( 2! = 2 < 2^2 = 4 \).

c The inductive hypothesis says that \( P(k) \) is true for some \( k \geq 2 \), i.e. that \( k! < k^k \).

d To prove the inductive step we need to prove \( P(k+1) \), i.e. that \( (k+1)! < (k+1)^{k+1} \), assuming \( P(k) \) stated above.

e Observe that \( (k+1)! = k! \times (k+1) \). Therefore by \( P(k) \) we have that \( (k+1)! < k^k \times (k+1) \), but \( k^k \times (k+1) < (k+1)^{k+1} \times (k+1) = (k+1)^{k+2} \), so it follows that \( (k+1)! < (k+1)^{k+1} \).

f We have shown that \( P(2) \) is true and that, for any \( k \geq 2 \) \( P(k) \) implies \( P(k+1) \). Therefore by the principle of induction it follows that \( P(n) \) is true, i.e. that \( n! < n^n \), for all \( n \geq 2 \).

40. Statement \( P(n) \) says that for any sets \( A_1, ..., A_n, B \) it holds that \( (A_1 \cap ... \cap A_n) \cup B = (A_1 \cup B) \cap ... \cap (A_n \cup B) \).

Basis step: \( P(1) \) is obviously true.

Inductive step: Assuming \( P(k) \) let’s prove \( P(k+1) \). \( P(k+1) \) says that for any sets \( A_1, ..., A_{k+1}, B \) it holds that

\[
(A_1 \cap ... \cap A_k \cap A_{k+1}) \cup B = (A_1 \cup B) \cap ... \cap (A_k \cup B) \cap (A_{k+1} \cup B)
\]

(1)

Denote \( A_1 \cap ... \cap A_k \) as \( S \). The left side of equation (1) can be restated as \( (S \cap A_{k+1}) \cup B \), which by one of the distributive laws (see the table on page 124), this is equal to \( (S \cup B) \cap (A_{k+1} \cup B) \). By the inductive hypothesis \( S \cup B = (A_1 \cap ... \cap A_k) \cup B = (A_1 \cup B) \cap ... \cap (A_k \cup B) \), and therefore the left side of equation (1) is equal to the right side of this equation, as we needed to show. This completes the inductive step and hence it completes the whole proof by induction.
56. Statement $P(n)$ says that for any $\neg(p_1 \lor \ldots \lor p_n) \iff (\neg p_1 \land \ldots \land \neg p_n)$.

Basis step: $P(1)$ is obviously true.

Inductive step: Assuming $P(k)$ let’s prove $P(k+1)$. $P(k+1)$ says that

$$\neg(p_1 \lor \ldots \lor p_k \lor p_{k+1}) \iff (\neg p_1 \land \ldots \land \neg p_k \land \neg p_{k+1}) \quad (2)$$

Denote $(p_1 \lor \ldots \lor p_k)$ as $q$. The left side of equivalence (2) can be restated as $\neg (q \lor p_{k+1})$, which by the DeMorgan’s law is equivalent to

$$\neg q \land \neg p_{k+1} \quad (3)$$

But by the inductive assumption $\neg q$ is equivalent to $(\neg p_1 \land \ldots \land \neg p_k)$, and therefore expression (3) is equivalent to $((\neg p_1 \land \ldots \land \neg p_k) \land \neg p_{k+1})$, which is equivalent to the right side of equivalence (2), as we needed to show.

60. The predicate $P(n)$ says that if $p$ is prime and $p|a_1 \cdots a_n$ for any integers $a_1, \ldots, a_n$ then $p|a_i$ for some $i$.

Basis case: For $n = 1$ the statement $P(n)$ is trivially true.

Inductive case: Assuming $P(k)$ is true for some $k \geq 1$, show that $P(k+1)$ is true. So assume $P(k)$ is true and assume that $p|a_1 \cdots a_k$ for some prime $p$ and some integers $a_1, \ldots, a_k, a_{k+1}$. Denote $b = a_1 \cdots a_k$ and $c = a_{k+1}$. Therefore $p|b \cdot c$. First note that if $p$ is prime and $p|bc$ then we must have that either $p|b$ or $p|c$ (in other words, we’ll argue that $P(2)$ holds). You can see that this is true by examining the factorization of $b$ and $c$. If neither $b$ nor $c$ have $p$ as a factor then $bc$ cannot be a multiple of $p$. (Btw, a corresponding statement is not true for composite $p$’s!) Now, if $p|b$ then by the inductive assumption $P(k)$ we have that $p|a_i$ for some $i = 1, \ldots, k$. And if $p|c$ then $p|a_{k+1}$. Therefore there is always some $i = 1, \ldots, k + 1$ s.t. $p|a_i$, as needed.

---

Some of you might be tempted to conclude that $p|b$ or $p|c$ just because $p|b \cdot c$ and because $P(2)$ is true. However, this would be a logical error because we only showed $P(1)$ is true, and we have not showed yet whether $P(2)$ is true or not.