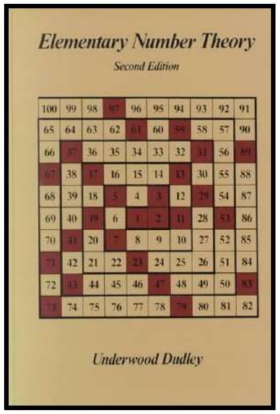
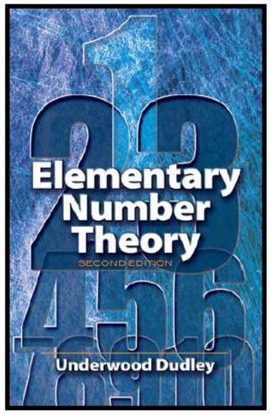
Elementary Number Theory

Section 13. Numbers in Other Bases—Proofs of Theorems





Theorem 13.1

Theorem 13.1. Every positive integer can be written as a sum of distinct powers of 2.

Proof. Let n be a positive integer. We prove the result by induction. For base cases, we have $1 = 2^0$, $2 = 2^1$, and $3 = 2^1 + 2^0$, so that the claim is true if the integer is 1, 2, or 3. For the induction hypothesis suppose that every integer k, with $k \le n-1$, can be written as a sum of distinct powers of 2. Consider integer $k = n$. Now there is an integer r such that $2^r \le n < 2^{r+1}$ (because n lies between two distinct powers of 2). That is, the largest power of 2 that is not larger than n is 2^r. Let $n' = n - 2^r$. Then $n' \le n-1$ and so by the induction hypothesis we know that n' can be written as the sum of distinct powers of 2: $n' = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_k}$ where $e_i \ne e_j$ for $i \ne j$. Since $n' = n - 2^r$, we have $n = 2^r + 2^{e_1} + 2^{e_2} + \cdots + 2^{e_k}$ so that n can be written as a sum of powers of 2. Finally, we show that the powers of 2 are distinct; that is, $r \ne e_i$ for $i = 1, 2, \ldots, k$.

Theorem 13.1 (continued)

Theorem 13.1. Every positive integer can be written as a sum of distinct powers of 2.

Proof (continued). ASSUME $r = e_j$ for some $1 \le j \le k$. Then

$$\begin{aligned} n &= 2^r + 2^{e_1} + 2^{e_2} + \cdots + 2^{e_k} \\ &= 2^{e_1} + 2^{e_2} + \cdots + 2^{e_{j-1}} + 2 \cdot 2^r + 2^{e_{j+1}} + \cdots + 2^{e_k}. \end{aligned}$$

But then $2 \cdot 2^r = 2^{r+1} \le n$, CONTRADICTING the choice of r as the largest exponent such that $2^r \le n$. So the assumption that $r = e_j$ for some $1 \le j \le k$ is false. That is, $n = 2^r + 2^{e_1} + 2^{e_2} + \cdots + 2^{e_k}$ is a sum of distinct powers of 2. Therefore, by induction, we have that the claim holds for every positive integer n, as claimed. □

Theorem 13.2

Theorem 13.2. Every positive integer can be written as the sum of the distinct powers of 2 in only one way.

Proof. Suppose that n has two representations as a sum of distinct powers of 2. Then

$$n = d_0 + d_1 \cdot 2 + d_2 \cdot 2^2 + \cdots d_k \cdot 2^k = e_0 + e_1 \cdot 2 + e_2 \cdot 2^2 + \cdots + e_k \cdot 2^k,$$

where each d_i and each e_i is either 0 or 1 (representing absence or presence, respectively, of the power of 2). Notice that we can assume without loss of generality we can assume that both representations go up to power k, since we can use coefficients of 0. Subtracting the representations gives

$$0 = (d_0 - e_0) + (d_1 - e_1) \cdot 2 + (d_2 - e_2) \cdot 2^2 + \cdots + (d_k - e_k) \cdot 2^k. \quad (*)$$

By Lemma 2.1 we can conclude that $2 \mid (d_0 - e_0)$. But since d_0 and e_0 are each either 0 or 1, then $d_0 - e_0 \in \{-1, 0, 1\}$ and so we must have $d_0 - e_0 = 0$, or $d_0 = e_0$.

Theorem 13.2 (continued)

Theorem 13.2. Every positive integer can be written as the sum of the distinct powers of 2 in only one way.

Proof (continued). ...

$$0 = (d_0 - e_0) + (d_1 - e_1) \cdot 2 + (d_2 - e_2) \cdot 2^2 + \cdots + (d_k - e_k) \cdot 2^k. \quad (*)$$

Now we substitute $d_0 - e_0 = 0$ into $(*)$ and divide both sides by 2 to get

$$0 = (d_1 - e_1) + (d_2 - e_2) \cdot 2 + \cdots + (d_k - e_k) \cdot 2^{k-1}. \quad (**)$$

The same argument as above implies that $d_1 - e_1 = 0$. Iterating this process, we similarly get $d_i - e_i = 0$ for each $1 \leq i \leq k$. That is, $d_i = e_i$ for $1 \leq i \leq k$ and hence the two representations of n are the same. That is, every positive integer can be written as the sum of the distinct powers of 2 in at most one way, as claimed. □

Theorem 13.3

Theorem 13.3. Let $b \geq 2$ be any integer (called the *base*). Any positive integer n can be written uniquely in the base b; that is, in the form

$$n = d_0 + d_1 \cdot b + d_2 \cdot b^2 + \cdots + d_k \cdot b^k$$

for some k, with $0 \leq d_i < b$ for $i \in \{0, 1, 2, \ldots, k\}$.

Proof. Let n be a positive integer. We divide n by b to get, by the Division Algorithm (Theorem 1.2), $n = q_1 b + d_0$ where $0 \leq d_0 < b$. Next, we divide the quotient q_1 by b to get $q_1 = q_2 b + d_1$ where $0 \leq d_1 < b$. Continuing the process we have

$$q_2 = q_3 b + d_2 \text{ where } 0 \leq d_2 < b,$$

$$q_3 = q_4 b + d_3 \text{ where } 0 \leq d_3 < b,$$

etc. Since $n > q_1 > q_2 > \cdots$ and each q_i is nonnegative, then the sequence of q_i's must terminate at some $i = k$, where $q_k = 0 \cdot b + d_k$ where $0 \leq d_k < b$.

Theorem 13.3 (continued 1)

Theorem 13.3. Let $b \geq 2$ be any integer (called the *base*). Any positive integer n can be written uniquely in the base b; that is, in the form

$$n = d_0 + d_1 \cdot b + d_2 \cdot b^2 + \cdots + d_k \cdot b^k$$

for some k, with $0 \leq d_i < b$ for $i \in \{0, 1, 2, \ldots, k\}$.

Proof (continued). Combining these results gives

$$\begin{aligned} n &= d_0 + q_1 b = d_0 + (d_1 + q_2 b)b = d_0 + d_1 b + q_2 b^2 \\ &= d_0 + d_1 b + (d_2 + d_3 b)b^2 = d_0 + d_1 b + d_2 b^2 + q_3 b^3 \\ &= d_0 + d_1 b + d_2 b^2 + (d_3 + d_4 b)b^3 = d_0 + d_1 b + d_2 b^2 + d_3 b^3 + d_4 b^4 \\ &\vdots \\ &= d_0 + d_1 b + d_2 b^2 + d_3 b^3 + \cdots + d_k b^k, \end{aligned}$$

so a representation exists.

Theorem 13.3 (continued 2)

Proof (continued). To show uniqueness of the representation, suppose we have two representations of n base b,

$$n = d_0 + d_1 b + d_2 b^2 + d_3 b^3 + \cdots + d_k b^k = e_0 + e_1 b + e_2 b^2 + e_3 b^3 + \cdots + e_k b^k,$$

where $0 \leq d_i < b$ and $0 \leq e_i < b$ for $i = 0, 1, 2, \ldots, k$. Subtracting the representations gives

$$0 = (d_0 - e_0) + (d_1 - e_1)b + (d_2 - e_2)b^2 + (d_3 - e_3)b^3 + \cdots + (d_k - e_k)b^k. \quad (*)$$

By Lemma 2.1 we can conclude that $b \mid (d_0 - e_0)$. But since d_0 and e_0 are each either $0, 1, 2, \ldots, b - 1$, then $d_0 - e_0 \in \{-b + 1, -b + 2, \ldots, -1, 0, 1, \ldots, b - 1\}$ and so we must have $d_0 - e_0 = 0$, or $d_0 = e_0$. Now we substitute $d_0 - e_0 = 0$ into $(*)$ and divide both sides by b to get

$$0 = (d_1 - e_1) + (d_2 - e_2) \cdot 2 + \cdots + (d_k - e_k) \cdot 2^{k-1}. \quad (**)$$

The same argument as above implies that $d_1 - e_1 = 0$.

Theorem 13.3 (continued 3)

Theorem 13.3. Let $b \geq 2$ be any integer (called the *base*). Any positive integer n can be written uniquely in the base b; that is, in the form

$$n = d_0 + d_1 \cdot b + d_2 \cdot b^2 + \cdots + d_k \cdot b^k$$

for some k, with $0 \leq d_i < b$ for $i \in \{0, 1, 2, \ldots, k\}$.

Proof (continued). Iterating this process, we similarly get $d_i - e_i = 0$ for each $1 \leq i \leq k$. That is, $d_i = e_i$ for $1 \leq i \leq k$ and hence the two representations of n are the same. That is, every positive integer has a unique representation base b, as claimed. □