Base b Representations of Integers

Ryan C. Daileda

Trinity University

Number Theory

Introduction

We usually represent integers as finite strings of decimal digits, e.g. 8906.

This familiar *place-value notation* is actually shorthand for a sum involving powers of the *base* 10:

$$8906 = 8 \cdot 10^3 + 9 \cdot 10^2 + 0 \cdot 10^1 + 6 \cdot 10^0.$$

The use of base 10 representations is convenient, but otherwise arbitrary.

It is possible to express integers in a similar way using *any* base $b > 1$.

Base b Expansions

Our first goal is to establish the following result on the representation of integers in terms of powers of b.

Theorem 1

Let $b > 1$ be an integer. Every $n \in \mathbb{N}$ can be written uniquely in the form

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0, \tag{1}$$

with $a_i \in \{0, 1, 2, \ldots, b-1\}$ for all i and $a_m \neq 0$.

Remark. The expression (1) is called the *base b expansion* of n.

Proof. To establish the existence of base b expansions we induct on n.

If $n \in \{0, 1, 2, \ldots, b-1\}$, then setting $a_0 = n$ works.

Now suppose $n \geq b$ and we have shown that all positive integers less than n have base b expansions.

Use the division algorithm to write $n = bq + r$ with $r \in \{0, 1, 2, \ldots, b-1\}$.

Because $n \geq b$ we must have $q \geq 1$. And since $b > 1$, we must have

$$q = \frac{n-r}{b} \leq \frac{n}{b} < n.$$

So q is a positive integer strictly less than n. By the inductive hypothesis we can write

$$q = a'_\ell b^\ell + a'_{\ell-1} b^{\ell-1} + \cdots + a'_1 b + a'_0$$

with $a'_i \in \{0, 1, 2, \ldots, b-1\}$ and $a'_\ell \neq 0$.

We therefore have

$$\begin{aligned} n &= bq + r \\ &= b(a'_\ell b^\ell + a'_{\ell-1} b^{\ell-1} + \cdots + a'_1 b + a'_0) + r \\ &= a'_\ell b^{\ell+1} + a'_{\ell-1} b^\ell + \cdots + a'_1 b^2 + a'_0 b + r, \end{aligned}$$

which is a base b expansion for n with $m = \ell + 1$, $a_0 = r$ and $a_i = a'_{i-1}$ for $i \geq 1$.

This completes the induction, and proves that every positive integer has a base b expansion.

We now prove uniqueness. Suppose that

$$a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 = c_\ell b^\ell + c_{\ell-1} b^{\ell-1} + \cdots + c_1 b + c_0,$$

with $a_i, c_i \in \{0, 1, \ldots, b-1\}$, $a_m \neq 0$ and $c_\ell \neq 0$.

Our first goal is to show that $m = \ell$.
Notice that

$$\begin{aligned} a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 \\ &\leq (b-1)b^m + (b-1)b^{m-1} + \cdots + (b-1)b + (b-1) \\ &= (b-1)(b^m + b^{m-1} + \cdots + b + 1) \\ &= (b-1)\frac{b^{m+1}-1}{b-1} = b^{m+1} - 1 < b^{m+1}. \end{aligned}$$

Furthermore, since $c_\ell \neq 0$,

$$c_\ell b^\ell + c_{\ell-1} b^{\ell-1} + \cdots + c_1 b + c_0 \geq b^\ell.$$

Since we have assumed the two expansions agree, we conclude that

$$b^\ell < b^{m+1} \;\Rightarrow\; \ell < m+1 \;\Rightarrow\; \ell \leq m.$$

By a symmetric argument, we find that $m \leq \ell$ as well, and hence $m = \ell$.

Now subtract the second expansion from the first:

$$(a_m - c_m)b^m + (a_{m-1} - c_{m-1})b^{m-1} + \cdots + (a_1 - c_1)b + (a_0 - b_0) = 0.$$

Since $|a_i - c_i| < b$ for all i, we have

$$\begin{aligned} \left|(a_{m-1} - c_{m-1})\right. & \left. b^{m-1} + \cdots + (a_1 - c_1)b + (a_0 - b_0)\right| \\ & \leq (b-1)b^{m-1} + \cdots + (b-1)b + (b-1) = b^m - 1, \end{aligned}$$

as above.

This means that

$$|a_m - c_m| b^m \leq b^m - 1,$$

which is impossible unless $a_m = c_m$.

Now repeat this argument to obtain $a_{m-1} = c_{m-1}$, $a_{m-2} = c_{m-2}$, etc. This completes our proof. □

Remarks.

- We will denote the base b expansion

$$a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

  by the *base b place-value notation*

$$(a_m a_{m-1} \cdots a_1 a_0)_b.$$

  When $b = 10$ we omit the parentheses.
- The existence proof above gives a recursive procedure for computing base b expansions through the division algorithm.

Example 1

Find the base 3 expansion of 709.

Solution. We have:

$$\begin{aligned} 709 &= 3 \cdot 236 + 1, \\ 236 &= 3 \cdot 78 + 2, \\ 78 &= 3 \cdot 26 + 0, \\ 26 &= 3 \cdot 8 + 2, \\ 8 &= 3 \cdot 2 + 2, \\ 2 &= 3 \cdot 0 + 2. \end{aligned}$$

The remainders give the base 3 expansion:

$$709 = (222021)_3.$$

Example 2

Find the *binary* (base 2) expansion of 709.

Solution. We have:

$$\begin{aligned} 709 &= 2\cdot 354+1, \;\; 354 = 2\cdot 177+0, \\ 177 &= 2\cdot 88+1, \;\; 88 = 2\cdot 44+0, \\ 44 &= 2\cdot 22+0, \;\; 22 = 2\cdot 11+0, \\ 11 &= 2\cdot 5+1, \;\; 5 = 2\cdot 2+1, \\ 2 &= 2\cdot 1+0, \;\; 1 = 2\cdot 0+1. \end{aligned}$$

The remainders give the binary expansion:

$$709 = (1011000101)_2$$

Repeated Squaring

We can use binary expansions to give an extremely efficient algorithm for modular exponentiation.

Example 3

Find the remainder when 5^{709} is divided by 1234.

Solution. The binary expansion $709 = (1011000101)_2$ expresses 709 as a sum of powers of 2:

$$709 = 2^9 + 2^7 + 2^6 + 2^2 + 2^0.$$

We now compute the first 9 squares of 5, modulo 1234:

$$5^{2^0} = 5 \pmod{1234}, \ \ 5^2 = 25 \pmod{1234},$$
$$5^{2^2} = (5^2)^2 = 625 \pmod{1234},$$

$$
\begin{aligned}
5^{2^3} &= (5^{2^2})^2 = 625^2 = 390625 \equiv 681 \pmod{1234},\\
5^{2^4} &= (5^{2^3})^2 \equiv 681^2 = 463761 \equiv 1011 \pmod{1234},\\
5^{2^5} &= (5^{2^4})^2 \equiv 1011^2 = 1022121 \equiv 369 \pmod{1234},\\
5^{2^6} &= (5^{2^5})^2 \equiv 369^2 = 136161 \equiv 421 \pmod{1234},\\
5^{2^7} &= (5^{2^6})^2 \equiv 421^2 = 177241 \equiv 779 \pmod{1234},\\
5^{2^8} &= (5^{2^7})^2 \equiv 779^2 = 606841 \equiv 947 \pmod{1234},\\
5^{2^9} &= (5^{2^8})^2 \equiv 947^2 = 896809 \equiv 925 \pmod{1234}.
\end{aligned}
$$

Therefore

$$
\begin{aligned}
5^{709} &= 5^{2^9+2^7+2^6+2^2+2^0} = 5^{2^9}\cdot 5^{2^7}\cdot 5^{2^6}\cdot 5^{2^2}\cdot 5^{2^0}\\
&\equiv 925\cdot 779\cdot 421\cdot 625\cdot 5 \equiv \boxed{147} \pmod{1234}.
\end{aligned}
$$

Divisibility Tests

Fix a base $b > 1$ and let d be any positive divisor of $b - 1$. Then $b \equiv 1 \pmod{d}$.

Let $n \in \mathbb{N}$ have the base b expansion $(a_m a_{m-1} \cdots a_0)_b$.

Then

$$\begin{aligned} n &= a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 \\ &\equiv a_m 1^m + a_{m-1} 1^{m-1} + \cdots + a_1 \cdot 1 + a_0 \pmod{d} \\ &\equiv a_m + a_{m-1} + \cdots a_1 + a_0 \pmod{d}. \end{aligned}$$

We immediately obtain the following divisibility test.

Theorem 2

If $n = (a_m a_{m-1} \cdots a_0)_b$ and $d | b - 1$, then $d | n$ if and only if $d | a_m + a_{m-1} + \cdots + a_1 + a_0$.

The nontrivial positive divisors of $10 - 1 = 9$ are 3 and 9.

We can therefore test for divisibility by 3 or 9 by summing the decimal digits of an integer.

For example, if $n = 9550684$, then

$$9 + 5 + 5 + 0 + 6 + 8 + 4 = 37 \not\equiv 0 \pmod{3},$$

so that $3 \nmid n$.

On the other hand, if $n = 3788058$, then

$$3 + 7 + 8 + 8 + 0 + 5 + 8 = 39 \equiv 0 \pmod{3},$$

so that $3|n$ (but $9 \nmid n$).

Suppose instead that $d|b+1$. Then $b \equiv -1 \pmod{d}$ so that

$$\begin{aligned}(a_m a_{m-1} \cdots a_0)_b &= a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 \\ &\equiv a_m(-1)^m + a_{m-1}(-1)^{m-1} + \cdots + a_1(-1) + a_0 \pmod{d}\end{aligned}$$

which is the *alternating sum* of the base b "digits."

Theorem 3

If $n = (a_m a_{m-1} \cdots a_0)_b$ and $d|b+1$, then $d|n$ if and only if $d|(-1)^m a_m + (-1)^{m-1} a_{m-1} + \cdots - a_1 + a_0$.

If $b = 10$, then $b + 1 = 11$, so the only nontrivial choice for d is 11. Taking $n = 53084471$ we find that

$$5 - 3 + 0 - 8 + 4 - 4 + 7 - 1 = 0,$$

and hence $11|n$.