RAM Math Circle - Chennai

Worksheet for February 16, 2025

1 Representing numbers in bases other than 10

Choose any positive integer $b \geq 2$; any natural number n can be represented in *base* b using an expansion of the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 b^0.$$

We use the following notation to say that we are expressing n in base b:

$$(n)_b = a_k a_{k-1} \ldots a_1 a_0.$$

We may also use the notation:

$$n = [a_k, a_{k-1}, \ldots, a_1, a_0]_b$$

The second notation is especially useful when the base b is larger than 10, in which case the coefficients a_i may be larger than 10.

Examples:

1. if we are looking to express 42 in base 2. Then we begin by looking for the largest power of 2 less than 42, which is $2^5 = 32$. Divide 42 by 32, the quotient is one and remainder is 10, so now we look for the largest power of 2 less than 10, and continue. The result is:

   $$42 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0.$$

   So we may say that the representation of 42 in base 2 is 101010.

   According to our notation we will write $(42)_2 = 101010$.

2. As another example, consider writing 691 in base 7: note that $7^2 = 49, 7^3 = 343, 7^4 = 2401$, so

   $$641 = 2 \times 7^3 + 0 \times 7^2 + 0 \times 7^1 + 5 \times 7^0.$$

   So we get $(691)_7 = 2005$.

3. 143 in base 12 is $[11, 11]_{12}$

Exercises in converting back to decimal representation:

1. $[1, 1]_2$
2. $[1, 1, 1]_2$
3. $[1, 1, 1, 1]_2$
4. $[1, 1, 1, 1, 1]_2$
5. $[2, 2]_3$
6. $[2, 2, 2]_3$
7. $[2, 2, 2, 2]_3$
8. $[2, 2, 2, 2, 2]_3$
9. Can you generalise your observation from the above exercises?

---

2 Computing a^n

The number of computations required to compute 2^n is $(n-1)$ multiplications.

If n is a power of 2, we can use successive squaring which required half as many computations. For example:

$$2^{2^{10}} = (2^{2^9})^2,$$

which is much less than using 1023 multiplications.

If n is not a power of 2, then it is useful to break up n into powers of 2, and multiply the results together. For example

$$2^{1025} = 2^{1024} \times 2 = 2^{2^{10}} \times 2.$$

Another example: compute 3^{15}.

$$\begin{aligned} 3^{15} &= 3^8 \times 3^7 \\ &= 3^8 \times 3^4 \times 3^2 \times 3^1 \\ &= (3^4)^2 \times 3^4 \times 3^2 \times 3 \\ &= 6561 \times 81 \times 9 \times 3 \\ &= 6561 \times 81 \times 27 \\ &= 6561 \times 2187 \\ &= 14348907 \end{aligned}$$

In both these examples, we express n in binary, and use the binary coefficients to express a^n as a product of powers for faster computation.

3 Computing $a^n \pmod m$

Recall that if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$.

1. Compute $2^{644} \pmod{645}$.

   $644 = [1,0,1,0,0,1,0,0,0,0]_2$ that is, $644 = 2^{512} \times 2^{128} \times 2^4$. Now we use successive squaring to reduce the number of computations.

   $$2^{128} = (((2^{16})^2)^2)^2$$

   Note that $2^{16} = 65536$, which is 391 modulo 645.

$$\begin{aligned} (((2^{16})^2)^2)^2 &\equiv ((65536^2)^2)^2 \pmod{645} \\ &\equiv ((391^2)^2)^2 \pmod{645} \\ &\equiv ((16)^2)^2 \pmod{645} \\ &\equiv (256)^2 \pmod{645} \\ &\equiv 65536 \pmod{645} \\ &\equiv 391 \pmod{645} \end{aligned}$$

Notice that the computations become easier since we can use the earlier computations in the later steps.

$$\begin{aligned} 2^{512} &\equiv ((2^{128})^2)^2 (\text{mod } 645) \\ &\equiv (391^2)^2 (\text{mod } 645) \\ &\equiv 16^2 (\text{mod } 645) \\ &\equiv 256 (\text{mod } 645) \end{aligned}$$

Putting these together, we have

$$\begin{aligned} 2^{644} &\equiv 2^{512} \times 2^{128} \times 2^4 (\text{mod } 645) \\ &\equiv 256 \times 391 \times 16 (\text{mod } 645) \\ &\equiv 88366 (\text{mod } 645) \\ &\equiv 1 (\text{mod } 645) \end{aligned}$$

2. Let $a = 1, 2, \ldots, 10$. Make a list of all the answers you get for a^4 mod 5, a^6 mod 7, a^{10} mod 11, a^{12} mod 13. Do you see any patterns? How will you try to extend them, if any?

4 Prime numbers

Let n be an integer and let p denote a prime number. If n is nonzero, we denote by $\text{ord}_p(n)$ the non-negative integer k such that p^k divides n and p^{k+1} does not divide n. We define $\text{ord}_p(0) = 0$.

Notice that $\text{ord}_p(n)$ is the number of successive zeroes appearing at the end of base p expansion of n.

Exercises

1. Find $\text{ord}_2(12), \text{ord}_3(12), \text{ord}_5(12), \text{ord}_3(14), \text{ord}_3(15), \text{ord}_5(15), \text{ord}_5(75), \text{ord}_{11}(121), \text{ord}_{11}(363)$.
2. What is $\text{ord}_2(192)$? What is the base 2 representation of 192? What is $\text{ord}_3(54)$? What is the base 3 representation of 54?
3. Let us examine some properties of $\text{ord}_p(n)$.
   (a) i. What is $\text{ord}_3(14 \times 15)$?
   ii. What is $\text{ord}_5(75 \times 15)$?
   iii. What is $\text{ord}_{11}(121 \times 363)$?
   (Note that the orders get added.)
   (b) i. What is $\text{ord}_3(14 + 15)$?
   ii. What is $\text{ord}_5(75 + 15)$?
   iii. What is $\text{ord}_{11}(121 + 363)$?
   (Observe that the order of the sum is the minimum of the orders of the individual numbers.)