16/01/2021

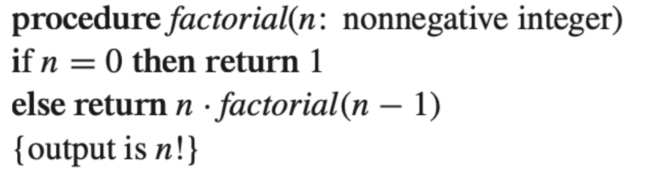
CS 1010 Discrete Structures Lecture 8: Modular Arithmetic

Maria Francis

January 16, 2021

Recursive Algorithms

An algorithm is recursive if it solves a problem by reducing it to an instance of the same problem with smaller input.

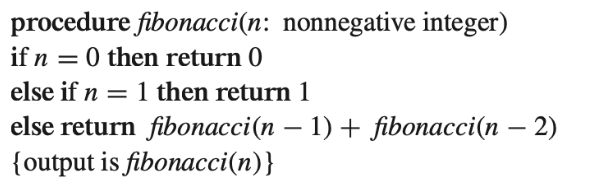


```
procedure factorial($n$: nonnegative integer)
if $n = 0$ then return 1
else return $n \cdot factorial(n - 1)$
{output is $n!$}
```

Trace steps for 4!: $4 \cdot 3!$, $3! = 3 \cdot 2!$, $2! = 2 \cdot 1!$ $1! = 1 \cdot 0!$
Insert value of $0! = 1$ and work backwards.

16/01/2021

Recursive Algorithms



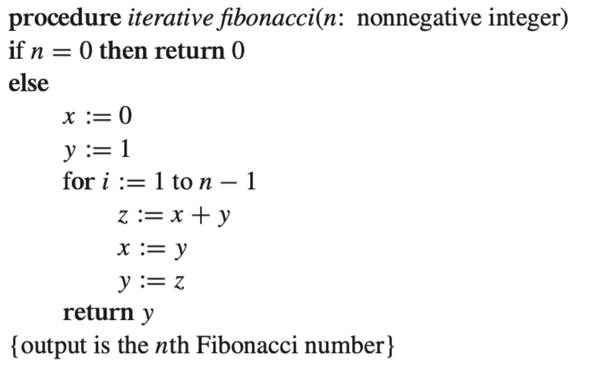
```
procedure fibonacci($n$: nonnegative integer)
if $n = 0$ then return 0
else if $n = 1$ then return 1
else return fibonacci($n - 1$) + fibonacci($n - 2$)
{output is fibonacci($n$)}
```

To show correctness of these algorithms we can use strong or weak induction.

Iteration vs Recursion

- Instead of the evaluation of the function at smaller integers, what if we start with the function at one or more integers, the base cases, and successively apply it to find the values of the function at successive larger integers. Then we have iterative functions.
- Advantage: Much less computation than a recursive procedure (unless special-purpose recursive machines are used).
- Recursive procedures are often the easiest to express and implement in some cases.
- To find f_n we express f_n as $f_{n-1} + f_{n-2}$ and then replace each with previous two and so on.
- We need $f_{n+1} - 1$ additions to find f_n. Not obvious, verify!

Iterative Algorithm



```
procedure iterative fibonacci(n: nonnegative integer)
if $n = 0$ then return 0
else
    $x := 0$
    $y := 1$
    for $i := 1$ to $n - 1$
        $z := x + y$
        $x := y$
        $y := z$
    return $y$
{output is the $n$th Fibonacci number}
```

16/01/2021

Iterative Algorithm

- This procedure initializes x as $f_0 = 0$ and y as $f_1 = 1$.
- $x + y$ is assigned to z.
- After going through the loop $n - 1$ times, x equals f_{n-1} and y equals f_n. (Verify!).
- Only $n - 1$ additions needed, so far less computation!
- Note that we had bounded f_n in the last class and it is a tight upper bound $\mathcal{O}(((1 + \sqrt{5})/2)^n)$.

Divisibility

- Modular arithmetic/ Clock arithmetic operates with remainders of integers when they are divided by a fixed integer, called the modulus.
- If a and b are integers with $a \neq 0$:a divides b if there is an integer c s.t. $b = ac$,i.e. if $\frac{b}{a}$ is an integer.
- a is called a factor or a divisor of b and b is a multiple of a.
- a divides b : $a \mid b$
- a does not divide b : $a \nmid b$.
- $a \mid b$ is $\exists c(ac = b)$ where the domain is $\mathbb{Z}$.
- $3 \nmid 7$ and $3 \mid 12$.

Basic Properties

- Let $a, b, c \in \mathbb{Z}$ where $a \neq 0$. Then:
  - if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$
  - if $a \mid b$ then $a \mid bc$ for all $c \in \mathbb{Z}$
  - if $a \mid b$ and $b \mid c$ then $a \mid c$.

  Verify!
- Corollary of above theorem: If $a, b, c \in \mathbb{Z}$, where $a \neq 0$ s.t. $a \mid b$ and $a \mid c$ then $a \mid mb + nc$ whenever m, n are integers.

Division Algorithm

- Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.
- Not really an algorithm but we still call it that way.
- d is called the divisor, a is called the dividend, q is called quotient, r, the remainder.
- $q = a \text{ div } d$, $r = a \text{ mod } d$.
- $101 = 11 \cdot 9 + 2$, $-11 = 3(-4) + 1$ and not $-11 = 3(-3) - 2$ because $r = -2$ is not positive or satisfy $0 \leq r < 3$.

Proof

- Foundation of algebra/algorithmic algebra.
- Let $a, b \in \mathbb{Z}$ be fixed and $b \neq 0$.
  $S = \{z \in \mathbb{N} : z = a - bx, x \in \mathbb{Z}\}$
- Can S be empty?
  - If $a \geq 0$, then $a - b(0) = a \geq 0$ and in S.
  - If $a < 0$, then $-a > 0$. Also, $b \geq 1$, $-ab \geq -a$, $a - ab \geq 0$ and in S.
- $S \subseteq \mathbb{N}$ and S is non-empty and so by WOP we have S has a smallest element, say r.
- $r = a - bq$ for some $x = q$. Thus $r = a - bq$ or $a = bq + r$.
- $r \in S$ and so $r \geq 0$. T.S.T. $r < b$.

Existence Proof

- If $r \geq b$, then $r - b \geq 0$.

$$0 \leq r - b = (a - bq) - b = a - b(q + 1).$$

- $a - b(q + 1)$ is in S and since b is positive, $r - b < r$ and so $a - b(q + 1)$ is a contradiction to r being the least element of S.
- So we have shown existence and now to show uniqueness.
- Lets suppose there are two sets of integers r_1, q_1 and r_2, q_2 s.t. $bq_1 + r_1 = a = bq_2 + r_2$, $0 \leq r_1 < b$, $0 \leq r_2 < b$.
- T.S.T. $r_1 = r_2$ and $q_1 = q_2$.

Uniqueness Proof

- Suppose $r_2 \geq r_1$.

$$\begin{aligned} 0 &= bq_1 + r_1 - bq_2 - r_2 \\ &= b(q_1 - q_2) - (r_2 - r_1) \end{aligned}$$

$b(q_1 - q_2) = r_2 - r_1$.We have $b > 0$ and $r_2 \geq r_1$, this implies $(q_1 - q_2) \in \mathbb{N}$.

- I.e. $r_2 - r_1$ must be one of $0, b, 2b, 3b, \ldots$.
- But $0 \leq r_1 \leq r_2 < b$, that means $r_2 - r_1 = 0$ and $r_2 = r_1$ and this implies $q_1 = q_2$.
- Symmetric proof for $r_1 \geq r_2$ and thus we have the complete proof of the theorem.

Modular Arithmetic

- In some cases we are interested in only remainders and we denote it with mod, $a \bmod m$ is the remainder when a is divided by m.
- If $a, b \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{0\}$ then a is congruent to b modulo m if $m \mid (a - b)$ represented as $a \equiv b(\bmod\ m)$. $a \equiv b(\bmod\ m)$ is a congruence, m is its modulus (plural moduli).
- If a and b are not congruent modulo m, we write $a \not\equiv b(\bmod\ m)$.
- What is the difference between : $a \equiv b(\bmod\ m)$ and $a \bmod m = b$?
- The first is a relation on $\mathbb{Z}$ and second is a function but they are related.

  Let $a, b \in \mathbb{Z}$ and let $m \in \mathbb{N} \setminus \{0\}$. Then $a \equiv b(\bmod\ m)$ if and only if $a \bmod m = b \bmod m$.

Congruences

- I.e. $a \equiv b (\mathrm{mod}\ m)$ iff a and b have the same remainder when divided by m.
- Note that a mod m and b mod m are the remainders when a and b are divided by m.
- Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.
    - If $a \equiv b$ mod m then $m \mid (a - b) \Rightarrow (a - b) = km$.
    - If $a = b + km$ then $km = a - b$ and thus $m \mid (a - b)$ so $a \equiv b$ mod m .
- Set of all integers congruent to a modulo m is called congruence class of a modulo m.

CARL FRIEDRICH GAUSS (1777-1855)

- Prince of mathematics, a prodigy.
- German mathematician, one of the greatest.
- Noted result: first rigorous (geometric) proof of Fundamental Theorem of Algebra : polynomial of degree n has exactly n roots counting multiplicities.
- Another interesting writeup topic since but all proofs rely on techniques outside of algebra.
- Also constructive proofs for this theorem took as long as 1891 to come up. Still an active area of research.
- Gauss's famous statement shows how number theory, where modular arithmetic plays a huge role, captures the imagination of so many mathematicians:
  Mathematics is the queen of the sciences, and the theory of numbers is the queen of mathematics.

Congruences

- Let m be a positive integer. If $a \equiv b (\mathrm{mod}\ m)$ and $c \equiv d (\mathrm{mod}\ m)$, then

$$a + c \equiv b + d (\mathrm{mod}\ m) \text{ and } ac \equiv bd (\mathrm{mod}\ m).$$

- We have, $b = a + sm$ and $d = c + tm$ (from previous theorem).

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + M(at + cs + stm).$$

- This implies, $a + c \equiv b + d \bmod m$ and $ac \equiv bd \bmod m$.

Congruences

- Corollary to find values of the mod m function:

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m.$$

and

$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

- Somethings are not always true over congruences:

$$ac \equiv bc \bmod m \text{ does not imply } a \equiv b \bmod m$$

$$a \equiv b \bmod m \text{ and } c \equiv d \bmod m \text{ does not imply}$$
$$a^c \equiv b^d \bmod m.$$

Think of examples!

Arithmetic Modulo m

- We define arithmetic operations on $\mathbb{Z}_m$: the set of nonnegative integers less than m, $\{0, 1, \ldots, m-1\}$.
- We define the addition on these integers as $+_m$ as:

$$a +_m b = (a + b) \bmod m.$$

and multiplication $\cdot_m$ by

$$a \cdot_m b = (a \cdot b) \bmod m.$$

- The operations on RHS is ordinary operations on integers.
- $+_m$ and $\cdot_m$ satisfy a lot of properties of ordinary addition and multiplication.

Properties of $+_m$, $\cdot_m$

- Closure: If $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b \in \mathbb{Z}_m$.
- Associativity: If $a, b, c \in \mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
- Commutativity: If $a, b \in \mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- Identity: The elements 0 and 1 are identity elements for addition and multiplication modulo m respectively. $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$.

Properties of $+_m, \cdot_m$

- Additive Inverses: If $a \neq 0$ and $a \in \mathbb{Z}_m$, then $m - a$ is an additive inverse of a mod m and for 0 it is its own additive inverse. I.e. $a +_m (m - a) = 0$.
- Distributivity: If $a, b, c \in \mathbb{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (\cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m b) +_m (b \cdot_m c)$.
- Note that no property about multiplicative inverses: no multiplicate inverse for 2 mod 6. In fact inverses can exist only if $gcd(a, m) = 1$.
- Note: $\mathbb{Z}_m$ with $+_m$ is a commutative group but with no inverses $\mathbb{Z}_m$ with $\cdot_m$ is not a group.
- $\mathbb{Z}_m$ with $+_m$ and $\cdot_m$ is a commutative ring.

Integer Representation

- Integers can be expressed using any integer greater than one as a base.
- Common ones in computer science: decimal (base 10),binary (base 2), octal (base 8), and hexadecimal (base 16).
- Let $b > 1, b \in \mathbb{Z}$. Then if n is a positive integer, it can be expressed uniquely in the form

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

  where k is a nonnegative integer, a_0, $a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.
- Proof: Use mathematical Induction.
- The representation of n is called base b expansion of n, given by $(a_k a_{k-1} \ldots a_1 a_0)_b$. Decimal expansions are the most common representation and 10 is omitted typically.

Other Representations

- Binary expansion: Each digit is either a 1 or 0, a bit string.
- Consider $(101011111)_2$:

$$\begin{aligned}(101011111)_2 &= 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4\\ &1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0\\ &= 351.\end{aligned}$$

- Octal Expansion: Each digit is from $\{0, 1, 2, \ldots, 8\}$.
- Consider $(7016)_8$:

$$\begin{aligned}(7016)_8 &= 7\cdot 8^3 + 0\cdot 8^2 + 1\cdot 8 + 6\\ &= 3598.\end{aligned}$$

Other Representations

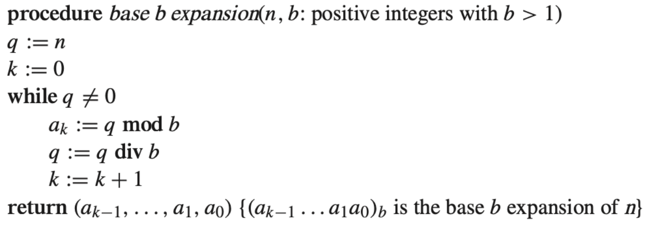
- Hexadecimal expansion: Digits are from the set $\{0, 1, 2, \ldots, 9, A, B, C, D, E, F\}$ where A to F letters represent the numbers 10 to 15.
- Consider $(2AE0B)_{16}$:

$$\begin{aligned}(2AE0B)_{16} &= 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 11 \\ &= 175627.\end{aligned}$$

- Each hexadecimal digit can be represented using four bits. Eg: $(1110\ 0101)_2 = (E5)_{16}$
- Bytes, bit strings of length eight, can be represented by two hexadecimal digits.

Basis Conversion

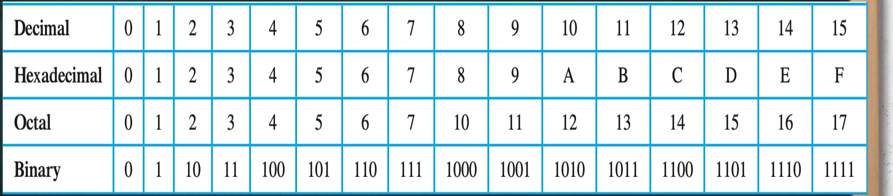
- How do we get a base b expansion of n?
- Divide n by b to get q_0, r_0 r_0 is the rightmost digit in the expansion.
- Divide q_0 by b to get r_1 as remainder, the second digit from the right in the base b expansion.
- Continue this process until quotient is equal to 0.



```
procedure base b expansion($n, b$: positive integers with $b > 1$)
$q := n$
$k := 0$
while $q \neq 0$
    $a_k := q$ mod $b$
    $q := q$ div $b$
    $k := k + 1$
return $(a_{k-1}, \ldots, a_1, a_0)$ {$(a_{k-1} \ldots a_1 a_0)_b$ is the base $b$ expansion of $n$}
```

Basis Conversion

- Conversion between binary and octal and between binary and hexadecimal expansions is easy because: each octal digit corresponds to a block of three binary digits and each hexadecimal digit corresponds to a block of four binary digits.



Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Basis Conversion

- To convert $(11111010111100)_2$ to hexadecimal we group the binary number into blocks of four adding leftmost zeroes if needed.
- We get 0011, 1110, 1011 and 1100 which corresponds to $(3EBC)_{16}$.
- Interesting read : Algorithms to do addition, multiplication, modular exponentiation using binary expansion which is extremely useful in computer science.
- All these have applications in computer science especially in cryptography.
- Studying how to do these operations algorithmically is computer algebra/computational algebra.

Prime Numbers

- High school definition relies on divisibility: A prime is an integer p greater than 1 that is divisible by no positive integers other than 1 and p.
- A positive integer that is greater than 1 and is not prime is called composite. Equivalently, the integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$.
- Building blocks of positive integers as witnessed by Fundamental Theorem of Arithmetic (FTA)/ Unique Factorization Theorem. *Every integer greater than 1 is either a prime number or can be represented as the product of prime numbers and that this representation is unique, up to (except for) the order of the factors.*

Prime Numbers

- We saw the proof using strong induction. But the uniqueness upto ordering was not discussed.
- For that you need Euclid's Lemma: If a prime p divides the product of two integers a and b, ab then p divides either a or b.
- In modern algebra, the Euclid's lemma is taken as the definition of prime number and the first definition as irreducible. In integers, both the definitions coincide.
- Consider two prime factorizations for $n = p_1 p_2 \dots p_j = q_1 q_2 \dots q_k$, where p_is and q_is are prime.
- Proof Idea: $p_1 \mid q_1 q_2 \dots q_k$ and by Euclid's Lemma $p_1 \mid q_i$ for some i. Wlog $i = 1$.
- But p_1 and q_1 are prime which implies $p_1 = q_1$ and thus we cancel those terms out and do the same for the remaining prime divisors.

Primality Testing

- Many applications like cryptography need to check if the integer is prime.
- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
- n is composite so it has a factor a, $1 < a < n$.
- $n = ab$, where b is a positive integer > 1.
- We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- If a and b are both greater than $\sqrt{n}$ then $ab > \sqrt{n} \cdot \sqrt{n} = n$, a contradiction.
- So either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, they are primes themselves or have factors that are less than itself by FTA.
- Brute force primality testing algorithm (trial division): Divide n by all primes not exceeding $\sqrt{n}$ and conclude that n is prime if it is not divisible by any of these primes.

16/01/2021

Infinitude of Primes

- Known since Euclid's times that there are infinitely many primes.
- Euclid's proof is what we will discuss, simple and very elegant proof admired by mathematicians.
- First proof presented in the book Proofs from THE BOOK, were THE BOOK is the imagined collection of perfect proofs that the famous mathematician Paul Erdős claimed is maintained by God!
- There are many proofs for proving primes are infinite and new ones keep coming up. Check the American Mathematical Monthly for different proofs.

Euclid's Proof

- Assume there are only finitely many primes $p_1, p_2, \ldots, p_n$.
- Let $Q = p_1 p_2 \cdots p_n + 1$.
- By FTA either Q is prime or can be written as a product of two or more primes.
- But none of the primes we listed divide Q since if $p_j \mid Q$ then $p_j \mid Q - p_1 p_2 \cdots p_n = 1$.
- Hence there is a prime not in the list $p_1, p_2, \ldots, p_n$: either Q is a prime or a prime factor of Q.
- Thus we have infinitely many primes.
- Nonconstructive since we do not give a prime that is not in the list.

Infinite Primes

- Quest to look for larger and larger primes.
- Primes of the form $2^p - 1$, where p is a prime are called Mersenne primes.
- An efficient test called Lucas-Lehmer test determines where $2^p - 1$ is prime or not.
- Examples: $2^2 - 1 = 3$, $2^3 - 1 = 7$ are Mersenne primes and $2^{11} - 1 = 2047 = 23 \cdot 89$ is not.
- Computers have made the job of finding primes easier.

Infinite Primes

- What about the distribution of primes? Like for example how many primes less than a number x?
- Prime Number Theorem: The ratio of the number of primes not exceeding x ($\pi(x)$) and x/lnx approaches 1 as x grows without bound,

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{lnx}} = 1.$$

- A conjecture for a long time and proved in 1896 by Hadamard and Poussin using complex analysis. Not easy to see.
- Important because it gives us a way to estimate the chances that a randomly chosen number is prime. We have that $\pi(x)$ can be approximated by x/lnx and therefore the odds that a randomly chosen integer less than n is prime is approximately :

$$(n/ln\ n)/n = 1/lnn.$$

Infinite Primes

- There are many efficient and clever algorithms that can be used for finding primes (not always correct) and they use the above results about the odds of a random integer being prime and use primality checking algorithms.
- In 2002, Manindra Agrawal, Neeraj Kayal, and Nitin Saxena gave a polynomial-time algorithm (AKS) in the number of bits in the binary expansion of an integer for determining whether a positive integer is prime. Very important result called Primes is in P.
- But even though primality checking can be done efficiently (read polynomial time), factorization of large numbers still remains extraordinarily time-consuming.
- No polynomial-time algorithm for factoring integers is known. Hardness of this is what the security of many crypto algorithms are based on.

Conjectures about Primes

- Goldbach's Conjecture: We have seen this. Every even integer n, $n > 2$ is the sum of two primes.
  - No proof yet but widely believed to be true.
- There are infinitely many primes of the form xxxx, for example of the form $n^2 + 1$, n is a positive integer.
- Twin Prime Conjecture:
  - Twin Primes are pairs of primes that differ by 2 such as 3 and 5, 5 and 7, 4967 and 4969.
  - The conjecture says there are infinitely many twin primes.
- Interesting to read: Terrence Tao, a living mathematical prodigy who writes a detailed blog with most inspiring articles as well as technical expositions.