Prof. Friedrich Eisenbrand
Alfonso Cevallos

Discussions from: March 3, 2015

Computer Algebra

Spring 2015

Assignment Sheet 2

Exercises marked with a ⋆ can be handed in for bonus points. Due date is March 17.

Exercise 1

Show that the following alternative algorithm for computing the gcd of $a, b \in \mathbb{N}$ is correct, and give an upper bound on its running time.

Data: $a, b \in \mathbb{N}$
Result: $gcd(a, b)$
$x = a,\ y = b,\ e = 0$;
while $2|x$ *and* $2|y$ **do**
  $x = x/2,\ y = y/2,\ e = e + 1$
end
while $y \neq 0$ **do**
  while $2|x$ **do**
    $x = x/2$
  end
  while $2|y$ **do**
    $y = y/2$
  end
  if $y < x$ **then**
    $(x, y) = (y, x)$
  end
  $y = y - x$;
end
return $x \cdot 2^e$

Exercise 2
Let (g, x, y) be the output of the Extended Euclidean Algorithm on input a, b (so that $g = (a, b) = xa + yb$). Show that, if $a \geq b > 0$, we have $|x| \leq b/g$ and $|y| \leq a/g$. Then prove that this algorithm runs in time $O(\text{size}(a) \cdot \text{size}(b))$.

Exercise 3
Implement the fast modular exponentiation function in Python.

Exercise 4 ($\star$)
In this exercise we analyse how to efficiently implement a general version of the Chinese remainder theorem: Suppose we are given relatively prime numbers $N_1, \cdots, N_t$, and numbers $a_1, \cdots, a_t$ such that $0 \le a_i < N_i$. Let $N = \prod_{i=1}^{t} N_i$. Show that in time $O(\text{size}^2(N))$ one can compute the unique integer $0 \le a < N$ such that $a \equiv a_i \mod N_i$ for $1 \le i \le t$.

Exercise 5 ($\star$)
Recall the Fibonacci numbers: $F(0) = 0$, $F(1) = 1$, and $F(n) = F(n-1) + F(n-2)$ for $n \ge 2$. Consider the following two algorithms for computing the n-th Fibonacci number.

$Fib_1(n)$:
if $n == 0$ *or* $n == 1$ **then**
  return n
end
return $Fib_1(n-1) + Fib_1(n-2)$

$Fib_2(n)$:
Let $A = \binom{a\ b}{c\ d} = \binom{1\ 1}{1\ 0}^{n-1}$;
return a

Note: The computation on A is left intentionally vague. How can this be done efficiently?

- Prove they are correct.
- Estimate their running time.
- Implement them and compare their running time for different values of n.

Exercise 6 ($\star$)
Prove that the greatest common divisor of integers a, b, c (not all zero) is the smallest positive integer expressible as $xa + yb + zc$, for integers x, y, z.

Exercise 7
Let $(G, \cdot)$ be a (not necessarily Abelian) group, with neutral element e.

- Prove that $a \cdot b = e$ implies $b \cdot a = e$.
- Suppose $a \cdot b \cdot c = e$. Does this imply that $c \cdot a \cdot b = e$?; $a \cdot c \cdot b = e$? In each case either prove the statement or provide a counter-example.

Exercise 8
Let a and b be integers. Prove that the subset $a\mathbb{Z} + bZ = \{ax + by \mid x, y \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. Prove also that the subset $a\mathbb{Z} + (5a + b)\mathbb{Z}$ is the same subgroup as before. What does this subgroup look like?

Exercise 9
Let n_1 and n_2 be two integers with gcd d. Prove that, for two arbitrary integers a_1 and a_2, there exists an integer a such that $a \equiv a_i \mod n_1$, $i = 1, 2$, if and only if $a_1 \equiv a_2 \mod d$.