Manuel Kauers
RISC-Linz

Hagenberg, December 17, 2002

Computer Algebra Exercises
Solution 1

Ex. (A) Let $x, y \in \mathbb{Z}$ with the digital representations

$$x = [x_1, x_2, \ldots, x_n], \quad y = [y_1, \ldots, y_n]$$

with $x_i, y_i \in \{0, 1, \ldots, 9\}$ $(i = 1, \ldots, n)$. Then the classical algorithm works by first computing $x \cdot y_i$ for each i which takes linear time for each i, and so it takes $\mathrm{O}(n^2)$ time to determine all of them. In the next step, the $x \cdot y_i$ are padded with up to $n-1$ zeroes taking overall $\mathrm{O}(n^2)$ time. Finally, the padded $x \cdot y_i \cdot 10^(n-i)$ need to be added, which again takes $\mathrm{O}(n^2)$ time. Hence, the overall cost of classical multiplication is $\mathrm{O}(n^2)$.

Various improvements to polynomial multiplication have been suggested during the past. The easiest one I know of is the algorithm of Karatsuba. This is a divide and conquer algorithm. Let K be a field and $p, q \in K[X]$ of degree n such that

$$p = p_1 X^{n/2} + p_0, \qquad q = q_1 X^{n/2} + q_0.$$

Then, compute $p_1 \cdot q_1$, $p_0 \cdot q_0$, and $(p_0 + p_1) \cdot (q_0 + q_1)$ recursively and return

$$p_1 \cdot q_1 X^n + ((p_0 + p_1) \cdot (q_0 + q_1) - p_0 \cdot q_0 - p_1 \cdot q_1) X^{n/2} + p_0 \cdot q_0$$

which is easily verified to be equal to $p \cdot q$. The complexity of this algorithm is

$$T(1) = \mathrm{O}(1), \qquad T(n) = 3T(n/2) + \mathrm{O}(n)$$

which leads to $T(n) = \mathrm{O}(n^{\log_2 3})$ which is slightly better than $\mathrm{O}(n^{\log_2 4}) = \mathrm{O}(n^2)$.

Further improvement can be achived using FFT based algorithms which lead to a multiplication time of $\mathrm{O}(n \log n)$.

Ex. (B) Definition: Let R be a commutative ring and $p \in R$ with 1.

1. p is a *unit* if there exists an inverse $q =: p^{-1}$ of p such that $p \cdot q = 1$. (Example: every field element.) The set of all units of R is denoted as $R^\times$.

2. p is a *zero divisor* if $p \neq 0$ and there is a $q \neq 0$ such that $p \cdot q = 0$.

3. p is a *prime* element if $p \notin R^\times \cup \{0\}$ and

$$\forall\, u, v \in R : p \mid u \cdot v \Longrightarrow p \mid u \vee p \mid v.$$

4. p is *irreducible* if $p \notin R^\times \cup \{0\}$ and

$$\forall\, u, v \in R : p = u \cdot v \Longrightarrow u \in R^\times \vee v \in R^\times.$$

In general, primarity implies irreducibility. In factorial rings, primarity and irreducibility are equivalent.

Consider $2 \in \mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\}$. We claim that 2 is irreducible but not prime.

Proof: 2 is not prime, because $2 \mid 6$ and $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ but $2 \nmid 1+\sqrt{-5}$ and $2 \nmid 1-\sqrt{-5}$. On the other hand, to prove that 2 is irreducible, assume that

$$\begin{aligned} 2 &= (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) \\ &= ac + ad\sqrt{-5} + bc\sqrt{-5} - 5bd. \end{aligned}$$

for $a, b, c, d \in \mathbb{Z}$. We have to show that (a, b) or (c, d) is trivial. We rewrite the last equation as a system of polynomial equations over $\mathbb{Z}$

$$ad + bc = 0, \qquad ac - 5bd = 2$$

and using Maple as shown in Ex. D below, we obtain

$$a = 2\frac{c}{c^2 + 5d^2}, \qquad b = -2\frac{d}{c^2 + 5d^2}.$$

To solve this in $\mathbb{Z}$, $c^2 + 5d^2$ needs to be divisor of c and d. In $\mathbb{Z}$ this requires $c^2 + 5d^2 \leq |d|$ which is only possible for $d = 0$. With this, $a = 2c/c^2$ is only satisfiable for $c = \pm 1$. But now, we have

$$2 = (a + b\sqrt{-5}) + \underbrace{(\pm 1 + 0 \cdot \sqrt{-5})}_{\in R^\times},$$

which completes the proof.

Ex. (C) Implementation of lists is possible similar to the recursive definition of a list: If X is a set of elements, then $x \in X$ is a list and for each $x \in X$ and each list l, (x, l) is also a list.

In this implementation, the basic operations take the following costs:

Operation	Time complexity
Append a new element to the front	O(1)
Remove an element from the front	O(1)
Search for an element	O(n)
Invert a list	O(n)
Concatenation of two lists	O(n)

Ex. (D) Let p_1, p_2, p_3 denote the respective lefthand side polynomials of rows 1, 2, and 3. Then, in Maple:

```
> solve({p1=0,p2=0,p3=0},{x,y});
```

$$\{y = \mathrm{RootOf}(\_Z^2 + 1), x = 0\}$$

```
> allvalues(%);
```

$$\{x = 0, y = I\}, \{x = 0, y = -I\}$$

and hence, $\mathrm{Var}(p_1, p_2, p_3) = \{(0, \mathrm{i}), (0, -\mathrm{i})\}$.

Ex. (E) In Maple:

```
> sum(i^2, i=1..n);
```

$$\frac{1}{3}(n+1)^3 - \frac{1}{2}(n+1)^2 + \frac{1}{6}n + \frac{1}{6}$$

```
> simplify(%);
```

$$\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$