UNBC

CPSC 499 Winter 2002

Midterm I—14 February 2002

- *Read each question carefully. Ask yourself what the point of the question is. Check to make sure that you have answered the question asked.*
- This is a **80** minute exam. This exam contains **2** pages of questions not including this cover page. Make sure that you have all of them.
- Answer all questions in your exam booklet. Clearly indicate which
- Partial marks shall be awarded for clearly identified work.

(3) **1.** (a) Explain briefly how arbitrary size integers are usually represented.

(2) (b) What considerations influence the choice of base B?

(3) **2.** Give the asymptotic complexities of the "grade school" arithmetic algorithms.

(4) **3.** The point of this question is to explain briefly how the recursive part of Karatsuba's algorithm works. Suppose that

$$0 \le \min(a, b, c, d) \le \max(a, b, c, d) < B^k \quad a \ne 0, c \ne 0$$

where B is the base of arithmetic that we are using, and $k \ge 16$ is some positive integer. Explain how Karatsuba's method computes the product

$$(aB^k + b) \cdot (cB^k + d)$$

(3) **4.** Explain the "leading digit trick" and how it helps in long division.

2 each **5.** Define the following words:

(a) associate,

(b) divisor,

(c) ideal,

(d) integral domain,

(e) irreducible element,

(f) kernel,

(g) principal ideal domain (PID)

(h) principal ideal,

(i) unique factorisation domain (UFD).

1 each **6.** (a) What are the units of $\mathbb{Z} \times \mathbb{Z}$?

(b) What are the zero divisors of $\mathbb{Z}_{12}$?

(c) Give an example of an element in $\mathbb{Q}[[X]]$ that is not in $\mathbb{Q}[X]$.

(d) What are the associates of 6 in $\mathbb{Z}[X]$?

(e) What are the divisors of 6 in $\mathbb{Q}$?

(f) Give an example of a ring that is not an integral domain.

(g) Give an example of a field.

(2) **7.** (a) Use Euclid's algorithm to find the greatest common divisor of 1113 and 4459.

(2) (b) Explain why we can't use Euclid's algorithm in the ring $\mathbb{Z}[X]$.

(3) **8.** (a) Consider the function γ from $\mathbb{Q}[X]$ to $\mathbb{Q}$ that yields the coefficient of the X^1 term, *e.g.,* $\gamma(13X^5 - 19X^3 + 11X - 2) = 11$, $\gamma(X^2 + 19) = 0$. Show that γ *is not* a homomorphism.

(3) (b) Show that the kernel of a homomorphism is an ideal.

(3) (c) Is the function from $\mathbb{Q}[X]$ to $\mathbb{Q}$ that yields the coefficient of the X^0 (constant) term a homomorphism? Justify your answer.

(3) **9.** (a) Show that $a|b$ *if and only if* $(b) \subseteq (a)$, where (a) is the principal ideals generated by a and (b) is the principal ideals generated by b.

(4) (b) Show that if I and J are ideals; K is the smallest ideal containing $I \cup J$; and $L = \{i + j \mid i \in I, j \in J\}$; then $K = L$.

[Hints: show that L is an ideal. Show that an ideal that contains I and J must contain L.]

Question	Score
1	/5
2	/3
3	/4
4	/3
5	/18
6	/7
7	/4
8	/9
9	/7
Total	/60