EXERCISES

A.H.M. LEVELT AND T.M.L. MULDERS

1. Determine the number of digits of the following numbers.
   (a) 1000!
   (b) 2^{10000}

2. Determine the floating point representation of $e = \exp(1)$ up to 10, 50 and 500 digits.

3. Determine the following numbers exact and up to 10 digits in their floating point representation.
   (a) $\cos(\pi/6)$
   (b) $\ln(2e)$
   (c) $\arctan(\sqrt{3}+2)$

4. Determine the factorization of the following numbers,
   (a) 98765432101234567890
   (b) $(2^{10})^{(2^{10})}$

5. Let

$$h(x) = \frac{x^5 - 3x^4 - 4x^3 - 11x^2 + 6x - 11}{x^5 - 5x^4 + 4x^3 - x^2 + 5x - 4}$$

   (a) Let $f(x)$ be the numerator of $h(x)$.
   (b) Let $g(x)$ be the denomerator of $h(x)$.
   (c) Let $d(x)$ be the $\gcd(f(x), g(x))$.
   (d) Determine $f(x)/d(x)$ and $g(x)/d(x)$.
   (e) Type normal(h). What happens?
   (f) Type convert(h,'parfrac',x). What happens?

6. (a) Let $f(x) = e^{-x^2}$. Determine $f'(x)$.
   (b) Let $f(x) = \ln(x)$. Determine $F(x)$ such that $F'(x) = f(x)$.
   (c) Let $h(x)$ be as in exercise 5. Determine $h'(x)$.
   (d) Determine $H(x)$ such that $H'(x) = h(x)$.

7. (a) Determine the taylor series in $x = 0$ of $\sin(x)$ up to order 10.
   (b) Determine the taylor series in $x = 0$ of e^x up to order 20
   (c) Let

$$f(x) = \frac{1}{1 - x - x^2}.$$

Date: august 1995.

Determine the taylor series in $x = 0$ of $f(x)$ up to order 20. What can you say about the coefficients of this taylor series?

8. Solve the following (system of) equation(s).
   (a) $ax^2 + bx + c = 0$.
   (b) $x^8 + x^3 - x^2 - 1$.
   (c) $\sin(x) = \cos(x)$.
   (d) $\begin{cases} x + y = a \\ cx - 3y = b \end{cases}$
   (e) $\begin{cases} x^2 + 1 = y \\ y - 3 = x \end{cases}$
   (f) $\begin{cases} x^2 + y^2 - 5 = 0 \\ xy - y^2 + 2 = 0 \end{cases}$
   (g) $x^2 + x + 1 = y^2, \qquad x, y \in \mathbb{Z}$
   (h) $x^2 + x + 1 = y^2, \qquad x, y \in \mathbb{Z}/2\mathbb{Z}$ and $x, y \in \mathbb{Z}/11\mathbb{Z}$
   (i) Solve $x^8 + x^3 - x^2 - 1$ numerical.

9. Let

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

   (a) Determine $\det(A)$ and $\det(B)$.
   (b) Determine A^{-1} and B^{-1}.
   (c) Determine $C = AB$.

10. Let

$$A = \begin{pmatrix} x & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & y \end{pmatrix}$$

   For which $x, y \in \mathbb{R}$ holds: $\det(A) = 0$?

11. Let

$$A = \begin{pmatrix} -12 & 12 & 4 & 0 \\ 4 & 4 & 4 & 4 \\ -40 & 4 & 4 & 4 \\ 21 & 0 & 0 & 4 \end{pmatrix}$$

   (a) Determine A^4.
   (b) Determine the characteristic polynomial of A. Can you explain the relation between this result and the result in (a)?

12. Let
$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 1 & x_4 & x_4^2 & x_4^3 \end{pmatrix}$$
   (a) Determine $\det(a)$.
   (b) Factorize $\det(a)$.
   (c) Generalize this exercise to a 6×6 matrix

13. Plot the following surfaces

   (a) $\begin{cases} x = \sin(s)\cos(t) & s \in [0, 2\pi] \\ y = \cos(s)\cos(t) & t \in [0, 2\pi] \\ z = \sin(t) & \end{cases}$

   (b) $\begin{cases} x = \sin(s)\cosh(t) & s \in [0, 2\pi] \\ y = \cos(s)\cosh(t) & t \in [-2, 2] \\ z = \sinh(t) & \end{cases}$

   (c) $\begin{cases} x = \sin(s)t & s \in [0, 2\pi] \\ y = \cos(s)t & t \in [-4, 4] \\ z = t & \end{cases}$

   (d) $\begin{cases} x = \sin(s)(2 + \cos(t)) & s \in [0, 2\pi] \\ y = \cos(s)(2 + \cos(t)) & t \in [0, 2\pi] \\ z = \sin(t) & \end{cases}$

   (e) $\begin{cases} x = \sin(s)(4 + t\cos(\frac{1}{2}s)) & s \in [0, 2\pi] \\ y = \cos(s)(4 + t\cos(\frac{1}{2}s)) & t \in [-1..1] \\ z = t\sin(\frac{1}{2}s) & \end{cases}$

14. Solve, using Maple, for all $a \in \mathbb{R}$ the following system of linear equations:
$$\begin{cases} 2ax + 6y = 5 \\ 5x + (a-2)y = 7 \end{cases}$$
   Is the solution always correct?

15. Compute the extremal values of the function
$$f\colon x \mapsto x^5/5 - x^4/2 + x^2 - x.$$

16. Let
$$A = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 5 & 3 \\ 4 & 2 & 6 \end{pmatrix} \text{ and } B = \begin{pmatrix} 3 & 5 \\ 0 & 1 \\ 7 & 4 \end{pmatrix}.$$
   Compute A^{-1}, AB and $(A^2 + A)B$ using Maple.

17. Use Maple to verify the formula
$$4\arctan(1/5) - \arctan(1/239) = \pi/4.$$
   This formula can be used to find approximations of $\pi/4$. How?

18. Experiment with Maple and its on-line help system.

19. Let $p \in \mathbb{N}$ be a prime number.
    (a) Write a Maple-routine *multtable* which returns the multiplication table in $\mathbb{Z}_p$ as in the following example for p = 5.
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$
    where the ij^{th} element is equal to $ij \bmod p$.
    (b) Write a Maple-routine *divtable* which returns the table of division in $\mathbb{Z}_p$ as in the folling example for p = 5.
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \\ 2 & 4 & 1 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$
    where the ij^{th} element is equal to $ij^{-1} \bmod p$.

20. For the Fibonacci numbers F_n we have the following formula.
$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right).$$
    (a) Write a Maple-routine to compute the Fibonacci numbers using their recursive definition (don't forget the remember option).
    (b) Write a Maple-routine to compute the Fibonacci numbers using above-mentioned formula.
    (c) Compare the speed of these routines.

21. Write a routine in Maple which computes the Fibonacci-polynomials $F_n(x)$. The Fibonacci-polynomials are defined as follows:
$$\begin{cases} F_0(x) = 1 \\ F_1(x) = x \\ F_n(x) = xF_{n-1}(x) + F_{n-2}(x) \quad \text{voor } n \geq 2 \end{cases}$$
    Compute $F_{50}(y)$.

22. Write a Maple-routine *elsym* such that elsym$(i, [x_1, x_2, \ldots, x_n])$ returns the ith elementary symmetric polynomial in $x_1, x_2, \ldots, x_n$.

23. Write a package to do integer arithmetic. Do this as follows:
    - Choose a base B (B a global variable).
    - Represent a non-negative integer by a list $[a_{n-1}, \ldots, a_1, a_0]$ where $0 \leq a_i < B$ and $a_{n-1} \neq 0$ or by $[0]$. A list $[a_{n-1}, \ldots, a_1, a_0]$ will represent the number $a_0 + a_1B + \cdots + a_{n-1}B^{n-1}$ and $[0]$ will represent 0.

- Represent an integer by a list $[s, p]$ where $s \in \{-1, 0, 1\}$ and p the representation of a non-negative integer. $[0, [0]]$ will represent 0, $[1, [a_{n-1}, \ldots, a_0]]$ will represent $a_0 + a_1 B + \cdots + a_{n-1} B^{n-1}$ and $[-1, [a_{n-1}, \ldots, a_0]]$ will represent $-(a_0 + a_1 B + \cdots + a_{n-1} B^{n-1})$.
- Write Maple-routines for:
  - comparing integers
  - adding integers
  - subtracting integers
  - multiplying integers

Be sure that all operations you perform are elementary. Test your code on examples using $B = 1000$.

24. Extend the package from the previous exercise with a routine to compute the quotient and remainder when dividing two base B numbers.

25. (a) Write a Maple-routine *representation* such that for positive integers a and B the call representation(a, B) returns the base B representation of a, i.e. if $a = a_0 + a_1 B + \cdots + a_n B^n$ it returns

$$[a_n, a_{n-1}, \ldots, a_1 a_0, B].$$

For example representation$(1000000, 121)$ returns $[68, 36, 56, 121]$.

(b) Write a maple-routine *len* which returns the number of digits in the above representation, i.e. len$(1000000, 121) = 9$.

(c) Write a Maple-routine *minimal_base* which, for a positive integer a, computes a base B for which len(a, B) is minimal.

(d) Can len(a, B) be smaller than length(a)? If yes, give an example.

26. The balanced ternary notation.

Prove that each non-zero integer can be written in a unique way as

$$d_0 + d_1 3 + d_2 3^2 + \cdots + d_n 3^n,$$

where $n \in \mathbb{N}$, $d_i \in \{-1, 0, 1\}$ and $d_n \neq 0$. This is called the *balanced ternary* notation. How can you see whether an integer in balanced ternary notation is positive or negative?

27. The mixed radix notation.

Let $m_0, m_1, \ldots, m_n$ be integers > 1. Prove that each $a \in \{0, 1, \ldots, m_0 m_1 \cdots m_n - 1\}$ can be written in a unique way as

$$d_0 + d_1 m_0 + d_2 m_0 m_1 + \cdots + d_n m_0 m_1 \cdots m_{n-1},$$

where $d_i \in \{0, 1, \ldots, m_i - 1\}$. This is called the *mixed radix* notation.

28. Let B be a positive integer > 1 and m an integer satisfying $0 < m < B$. Prove that $\lfloor B/(m+1) \rfloor m \geq \lfloor B/2 \rfloor$.

29. (a) Write a Maple-routine to compute a^n for positive integers a and n. Do this in two ways: by successive multiplication by a and by a divide-and-conquer technique. Compare the speed of both routines.
(b) Do the same as in (a) but now to compute a^n for a postive integer n and $a \in \mathbb{Z}_m$ (m a positive integer).
(c) For a positive integer n let l_n be the minimal number of multiplications needed to compute a^n. For example the minimal number of multiplications needed to compute a^15 is 5 (see lecture notes). Write a Maple-routine which computes for a positive integer m the set $\{n \in \mathbb{N} \mid l_n = m\}$.

30. Notation as in Lemma 1 of *Elementary arithmetic of the integers.* Prove that:

$$\begin{aligned} 1 = s_2 \leq -s_3 < s_4 < -s_5 < \cdots \\ 1 = t_1 \leq -t_2 < t_3 < -t_4 < \cdots \\ s_{i-1}u_i - s_iu_{i-1} = (-1)^{i+1}b \qquad i = 1, \ldots, n+1 \\ t_{i-1}u_i - t_iu_{i-1} = (-1)^i a \qquad i = 1, \ldots, n+1. \end{aligned}$$

31. Prove that for $a, b \in \mathbb{Z}$ such that $a \geq b > 0$ and not both 1, there exist integers s and t such that $\gcd(a, b) = sa + tb$ and $|s| < b, |t| < b$. Do s and t computed in the extended Euclid's algorithm satisfy these inequalities?

32. Prove Corollary 4 of *Elementary arithmetic of the integers.* Use the fact that $F_n = \left((\frac{\sqrt{5}+1}{2})^n - (\frac{\sqrt{5}-1}{2})^n\right)/\sqrt{5}$.

33. Show that for positive integers $a \geq b$ the time for computing q and r such that $a = qb + r$ (long division) can be bounded by $O(\ln(a)(\ln(q) + 1))$. Use this to show that the computation time of the extended Euclid's algorithm can be bounded by $O(\ln^2(a))$.

34. Do exercices 10, 11 and 12 from Chapter 2 of [1].

35. Write a Maple-routine *Karatsuba* which multiplies two n-digit base B numbers using Karatsuba's method. Use the package of exercise 23 to do your base B arithmetic.
Compare the speed of your routine with multiplication in Maple (take $B = 10$). How does the speed of your routine depend on the size of the input?

36. Write a Maple-routine *my_gcd* which for $a, b \in \mathbb{Z}$ computes the greatest common divisor of a and b. You may use the Maple-routines *irem* and *iquo* for this (do you need both?). Write your routine such that it will print output as in the following example.

$$\begin{array}{rcrcrcr} 30 & = & 1 & * & 18 & + & 12 \\ 18 & = & 1 & * & 12 & + & 6 \\ 12 & = & 2 & * & 6 & + & 0 \end{array}$$

37. Write a Maple-routine *my_gcdex* which for $a, b \in \mathbb{Z}$ retruns a list $[d, s, t]$ such that d is the greatest common divisor of a and b and $d = sa + tb$. You may use the Maple-routines

irem and *iquo* for this (do you need both?). Write your routine such that it will print output as in the following example.

$$\begin{array}{ccccccccccccccccc} 30 & = & 1 & * & 18 & + & 12 & \quad & 12 & = & 1 & * & 30 & + & -1 & * & 18 \\ 18 & = & 1 & * & 12 & + & 6 & & 6 & = & -1 & * & 30 & + & 2 & * & 18 \\ 12 & = & 2 & * & 6 & + & 0 & & 0 & = & 3 & * & 30 & + & -5 & * & 18 \end{array}$$

38. The Maple-routines *irem* and *iquo* work do the following:
    For $a, b \in \mathbb{Z}$ we have $a = \text{iquo}(a,b) * b + \text{irem}(a,b)$ where $-b < \text{irem}(a,b) < b$ and $\text{sgn}(\text{irem}(a,b)) = \text{sgn}(a)$ (when $\text{irem}(a,b) \neq 0$).
    Write Maple-routines *my_irem* and *my_iquo* such that for $a, b \in \mathbb{Z}$ the following holds:
    $a = \text{my\_iquo}(a,b) * b + \text{my\_irem}(a,b)$ where $-b/2 < \text{my\_irem}(a,b) \leq b/2$.
    Rewrite your routine from the previous exercise but now using *my_irem* and *my_iquo* instead of *irem* and *iquo*.
    Compare both routines on some large inputs. Which is faster?

39. For randomly chosen integers a and b the probability that they are relatively prime is $6/\pi^2$ (E. Cesaro, 1881). Check this theorem using Maple. For random number generation you can use teh Maple-routine *rand*.

40. Greatest common divisor in the ring of Gaussian integers.

    Let $G = \{n + mi \mid n, m \in \mathbb{Z}\}$ ($i = \sqrt{-1}$). Show that G is a ring under usual addition and multiplication. G is called the ring of Gaussian integers. Define the norm N on G by $N(n + mi) = n^2 + m^2$. Claim: for $a, b \in G$, $b \neq 0$, there are $q, r \in G$ such that $a = qb + r$ and $0 \leq N(r) < N(b)$. This can be seen as follows. Let $c = a/b$, $c_1 = \Re(c), c_2 = \Im(c), q_1 = \text{round}(c_1), q_2 = \text{round}(c_2)$ and $q = q_1 + q_2 i$. Here for $a \in \mathbb{R}$, $\text{round}(a) = n$ is the integer satifying $n \leq a < n + 1/2$ or $n - 1/2 \leq a \leq n$. Now prove that $N(q - c) \leq 1/2$ and $N(a - bq) \leq N(b)/2$.
    Write a Maple-routine *Gauss_div* which for $a, b \in G$ ($b \neq 0$) returns a list $[q, r]$ such that $q, r \in G$, $a = qb + r$ and $0 \leq N(r) < N(b)$ (*round* is a builtin Maple-routine).
    Write a Maple-routine *Gauss_gcd* which for $a, b \in G$ (not both 0) returns a list $[d, s, t]$ such that d is the greatest common divisor of a and b satisfying $\Re(d) > 0$, $\Im(d) \geq 0$ and $d = sa + tb$.
    Test your routines for several (large) a and b.

41. Write a Maple-routine *gcd2* to compute a greatest common divisor of two numbers $a, b \in \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$.

42. For randomly chosen integers a and b the probability that they are relatively prime is $6/\pi^2$ (E. Cesaro, 1881). Check this theorem using Maple. For random number generation you can use teh Maple-routine *rand*.

43. For integers $a > b > 0$ we can write $\frac{a}{b}$ as

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{}{\ddots\, a_{n-1} + \cfrac{1}{a_n}}}}}$$

where $a_0, a_1, \ldots, a_n$ are positive integers. This expression is denoted by $[a_0, a_1, \ldots, a_n]$ and is called a continued fraction.

(a) Show how the numbers $a_0, a_1, \ldots, a_n$ can be extracted from the results during the execution of Euclid's algorithm.
(b) Write a Maple-routine *calc_frac* which computes the rational number corresponding to a continued fraction.
(c) Write a Maple-routine *determine_frac* which computes the continued fraction corresponding to a rational number.
(d) Test whether your routines are each others inverse.

44. Write a Maple-routine for multiplying polynomials using Karatsuba's method.

45. Experiment using Maple's *normal* function and study Maple's on-line help on this function. What normal form is used by Maple?

46. Simplify the following expressions using Maple (think of expand, normal, simplify, factor, combine, radsimp, etc.).
(a) $(\exp(x) + x)/(\exp(2x) + 2x\exp(x) + x^2)$
(b) $(x^5 + 40x^4 + 595x^3 + 3905x^2 + 9680x + 1331)^{1/3}$
(c) $(x-2)^{3/2}/(x^2 - 4x + 4)^{1/4}$
(d) $(\sqrt{(}x) - y)/(x - y^2)$
(e) $1/(2 + 5^{1/3})$
(f) $\cos(x + y) + \sin(x)\sin(y) + 2^{x+y}$
(g) $2\cos(x)^2 - \cos(2x)$

47. Write a Maple-routine *recursive* which returns the recursive representation of a multivariate polynomial. For example

$$\mathrm{recursive}(x^3y^2z^2 + x^3y^2 + 3x^3y + zyx^2 - xy^4 + xzy^2 + yz - y + 3z, [x, y, z])$$

should return

$$((z^2 + 1)y^2 + 3y)x^3 + zyx^2 - (y^4 - zy^2)x + (z - 1)y + 3z.$$

48. Write a Maple-routine *horner* which returns the representation of a polynomial according to Horner's evaluation rule. For example

$$\mathrm{horner}(79x^5 + 56x^4 + 63x^2 + 57x - 59)$$

should return

$$-59 + (57 + (63 + (56 + 79x)x^2)x)x.$$

Do not use Maple's *convert* routine for this.

49.

50. Define the nth Legendre polynomial $P_n(x)$ as the coefficient of y^n in the Taylor expansion of $1/\sqrt{(1 - 2xy + y^2)}$.
    (a) Write a Maple-routine to compute the nth Legendre polynomial.
    (b) Compute $\int_{-1}^{1} P_n(x)P_m(x)$ for several n and m and conjecture a general formula for this integral.
    (c) Let $Q_n(x)$ be defined by $Q_0(x) = 1, Q_1(x) = x$ and $Q_n(x) = (n-1)/n(xQ_{n-1}(x) - Q_{n-2}(x)) + xQ_{n-1}(x)$. Write a Maple-routine to compute the polynomials Q_n.
    (d) COmpare the polynomials P_n and Q_n.

51. An (ordinary, linear) differential operator of order n is an object of the following form:

$$P = \sum_{i=0}^{n} P_i(x)\left(\frac{d}{dx}\right)^i,$$

where the $P_i(x)$ are functions of x (usually assumed to be differentiable infinitely many times). One can think of P as an operator acting on the set of functions, which are infinitely many times differentiable, as follows:

$$Pf = \sum_{i=0}^{n} P_i(x)\left(\frac{d^i f}{dx^i}\right).$$

Now it is clear how to add these operators and how to multiply them with functions. For operators P and Q we can also define their composition (or product) PQ as the unique operator R such that for all functions $Rf = P(Qf)$. Notice that in general we have $PQ \neq QP$.

Implement differential operators in Maple, i.e. find a good data structure to represent them and write routines for the following operations:

- Multiplication with function
- Addition
- Composition
- Action on functions

52. A partition of a positive integer n is a list $[a_1, a_2, \ldots, a_r]$ where $a_1, a_2, \ldots, a_r$ are positive integers such that $a_1 \geq a_2 \geq \cdots \geq a_r$ and $n = a_1 + a_2 + \cdots + a_r$.
    (a) Write a Maple-routine *partitions* such that partitions(n) returns a list of all partitions of n.
    Hint: First write a routine P such that P(n, k) returns all partitions $[a_1, a_2, \ldots, a_r]$.
    (b) Let N_n denote the number of partitions of n. Write a Maple-routine N which computes N_n (without actually computing all permutations).
    A second way to compute N_n can be extracted from the following identity, due to Euler.

$$\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} = 1 + N_1x + N_2x^2 + N_3x^3 + \cdots$$

Try to understand this identity and write a Maple-routine which computes N_n using this identity (use the Maple-routines *taylor* and *coeff*).
Compare the speed of both routines.

53. In this exercise we will do some 'experimental mathematics'. Let

$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{n=0}^{\infty}a_n x^n.$$

   (a) Write a Maple-routine *approx* that computes $\prod_{n=1}^{\infty}(1-x^n) \bmod x^m$.
   (b) Look at the differences of the exponents of succeeding terms appearing. Can you now guess what terms will appear.
   (c) Look at the coefficients of the terms appearing. Can you now guess what the coefficients will be in general.
   (d) Write now a Maple-routine that computes $\prod_{n=1}^{\infty}(1-x^n) \bmod x^m$ without computing a product of polynomials.

54. Check that a is a primitive nth root of unity in $\mathbb{F}_p$.
   (a) $p=41, n=8, a=14$.
   (b) $p=97, n=32, a=28$.
   (c) $p=12289, n=1024, a=-1987$.
   (d) $p=104857601, n=1048576, a=-25430071$.

55. (a) Write a Maple-routine *fft* to perform the fast Fourier transformation, i.e. when p is a prime number, n a power of 2, ω a primitive nth root of unity in $\mathbb{F}_p$ and $a=[a_0,a_1,\ldots,a_{n-1}]$ a list of elements of $\mathbb{F}_p$, then $\mathrm{fft}(a,\omega,p)$ returns a list $[A_0,A_1,\ldots,A_{n-1}]$, the Fourier transform of a.
   (b) Write a Maple-routine *ifft* for the inverse Fourier tramsformation.
   (c) Check that your routines are each others inverse by the following example: $a=[1,4,3,10,5,16,5,0], \omega=2, p=17$.
   (d) Get an idea of the speed of your routines by studying the following big example: $p=12289, n=2^{10}, \omega=-1987$ and a list of random numbers of length 2^{10}.

56. Study the Maple-routines *FFT* and *iFFT*, the fast Fourier transforms and its inverse over the complex numbers (remind the on-line help). Compare the speed of these routines and your routines *fft* and *ifft*.

57. Write a Maple-routine to evaluate a polynomial in the nth roots of unity (of a finite prime field) using Horner's rule. Do the same again but now using your *fft*-routine from exercise 55. Compare the speed of both routines.

58. Write a Maple-routine to interpolate a polynomial in the nth roots of unity (of a finite prime field) using Lagrange's interpolation formula. Do the same again but now using your *ifft*-routine from exercise 55. Compare the speed of both routines.

59. Write a Maple-routine to multiply two polynomials using the fast Fourier transformation. Use your routines *fft* and *ifft* of exercise 55. Use your routine to multiply $(x+1)^{15}$ and

$(x+2)^{15}$ in $\mathbb{F}_p[x]$ where $p = 104857601$ (use the primitive 32th root of unity $\omega = 43262874$).

60. Compute all prime numbers $\leq 2^{31}$ of the form $1 + 2^{20}k$ (use the Maple-routine *isprime*). How many are there? Compare this with the result in the lecture notes.

61. (a) Write a Maple-routine to compute a primitive element of $\mathbb{F}_p$ (use the Maple-routine *numtheory[factorset]*).
    (b) Write a Maple-routine that returns $[n, \omega]$, where n is the largest power of 2 that divides $p-1$ and ω is a primitive nth root of unity in $\mathbb{F}_p$.
    (c) Use the routine of (b) to compute a primitive 2^{20}th root of unity in F_p, where $p = 2^{20} \cdot 625 + 1$.

62. Do some experiments using your *fft* routine of exercise 55. You can use your routine of exercise 61 to find primitive roots of unity. Use random lists as input.

63. Write a Maple-routine to compute the resultant of two polynomials with coefficients in $\mathbb{Q}$. Do this in two ways: using the definition of the resultant and using the recursive formula which comes from pseudo-division of the polynomials (see lecture notes). Compare the speed of these routines and the Maple-routine *resultant*.

64. Write a Maple-routine *resultant_ex* which computes the resultant r of two polynomials f, g, with coefficients in $\mathbb{Q}$, and also polynomials a and b such that $r = af + bg$, $\deg(a) < \deg(g)$ and $\deg(b) < \deg(f)$.

References

[1] K.O. Geddes, S.R. Czapor, G. Labahn Algorithms for computer algebra, 1992, Kluwer