BACKGROUND MATHEMATICS -
PRACTICE QUESTIONS

1. Integer arithmetic

   (a) Is 3 a common divisor of 72 and 81? Is it the greatest common divisor (gcd)? Justify your answer.

   (b) Using the euclidean algorithm, find the gcd of each of the following pairs of integers and in each case express this gcd as a linear combination of the two integers:

      i. 122 and 723
      ii. 235 and 115
      iii. 42 and 192

2. Modular arithmetic for integers

   (a) Test whether the following statements are true or false. Justify your answer in each case.

      i. $26 = 56 (\mathrm{mod}\, 3)$
      ii. $19 = -156 (\mathrm{mod}\, 34)$
      iii. $-7 = -23 (\mathrm{mod}\, 11)$

   (b) Reduce the following integers

      i. $99 \bmod 12$
      ii. $46 \bmod 5$
      iii. $-46 \bmod 5$

   (c) Reduce the following operations:

      i. $(17 + 23 - 5) \bmod 11$
      ii. $12 \times 8 \bmod 13$

iii. $5^7 \bmod 24$ (Hint: What is $5^2 \bmod 24$?)

iv. $5^7 \bmod 26$ (Hint: again consider $5^2 \bmod 26$?).

(d) Compute the addition and multiplication tables for the elements of

i. $\mathbb{Z}_5$

ii. $\mathbb{Z}_8$.

In each case list which elements have additive inverses and which have multiplicative inverses.

(e) Compute the addition and multiplication tables for the *non-zero* elements of

i. $\mathbb{Z}_6$

ii. $\mathbb{Z}_7$.

In each case list which elements have additive inverses and which have multiplicative inverses.

(f) Find all the distinct multiplicative powers of 3, that is, numbers which can be expressed in the form $3^i, i = 0, 1, 2, \ldots$, in

i. $\mathbb{Z}_7$

ii. $\mathbb{Z}_9$.

(g) Determine whether the multiplicative inverse of

i. 7 in $\mathbb{Z}_{43}$

ii. 4 in $\mathbb{Z}_{16}$

exists.

Using an extension of the euclidean algorithm compute these inverses (if they exist).

(h) Compute $\frac{2}{3}$ and $\frac{3}{5}$ in $\mathbb{Z}_{11}$, that is, find the numbers representing 2.3^{-1} and 3.5^{-1}.

3. Arithmetic for real polynomials, $\mathbb{R}[x]$

(a) Compute the following in $\mathbb{R}[x]$:

i. $(x-1)(2x^2+x-1)(3x^3+2x+4)(x-1)$

ii. $(x^5+2x^3-x^2+x-1)/(x^3+3x+1)$

(b) Find (by trial and error) a root of $x^3-7x^2+15x-9$ in $\mathbb{R}$

Use this root to find a corresponding linear factor.

Hence find a non-trivial factorization of $f(x)$.

Finally find **all** roots of $f(x)$. Justify your answer (i.e. give reasons why no other roots exist).

(c) Is $x^3-7x^2+15x-9$ reducible over $\mathbb{R}$?

Is $x^5+3x^4+2x^3-2x^2-3x-1$ irreducible over $\mathbb{R}$?

Give only a yes/no answer in each of the above cases.

(d) Reduce the polynomial $x^5 + 2x^4 - x^3 - 2x^2 - 3x - 1 \bmod x^3 - 2x^2 + 8x - 3$

4. Arithmetic for binary polynomials $\mathbb{Z}_2[x]$

(a) Compute the following in $\mathbb{Z}_2[x]$:

i. $(x^2 + x + 1) + (x^3 + x + 1) + (x + 1)$

ii. $(x^2 + x + 1)(x^3 + x + 1)(x + 1)$

iii. $(x^5 + x^3 + x^2 + 1)/(x^2 + x + 1)$

(b) Divide $x^2 + x + 1$ into $x^5 + x^3 + x^2 + 1$ using polynomial long division. What is the quotient and remainder?

(c) Given $f(x) = x^4 + x^3 + x$ and $g(x) = x^2 + x + 1$ polynomials in $\mathbb{Z}_2[x]$. Using long division of polynomials, find polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)\ g(x) + r(x)$ where $\deg(r(x)) < \deg(g(x))$.

(d) Given $a(x) = x^5 + x^3 + x + 1$ and $b(x) = x^2 + 1$ polynomials in $\mathbb{Z}_2[x]$. Using the euclidean algorithm, find $\gcd(a(x), b(x))$ and then polynomials $s(x)$ and $t(x)$ such that $\gcd(a(x), b(x)) = s(x)a(x) + t(x)b(x)$.

(e) List all the polynomials of degree 4 with coefficients in $\mathbb{Z}_2$, and then decide for each such polynomial $p(x)$, whether or not the equation $p(x) = 0$ has a solution x in $\mathbb{Z}_2$.

What do we call such solutions?

Determine whether each polynomial has linear factors.

Furthermore determine whether each polynomial is reducible or not.

(f) Reduce the polynomial $x^6 + x^4 + x^3 + x^2 + x \bmod x^3 + x^2 + x + 1$

What is the highest degree that the reduced form of an arbitrary polynomial modulo $x^3 + x^2 + x + 1$ can have?

(g) Compute $((x - 1)(x^2 + x - 1)) + (x^3 + x + 1) \bmod x + 1$

5. Finite fields

Refer to the handout giving the construction of GF(8) in terms of the irreducible polynomial $x^3 + x + 1$ and the primitive element α. That is, GF(8) = $\{a + b\alpha + c\alpha^2, a, b, c \in \mathbf{Z}_2, \alpha^3 + \alpha + 1 = 0\}$.

(a) Construct a 4-column table describing GF(8) as follows: list all the binary strings of length 3; for each such string *abc* list the corresponding polynomial $a + b\alpha + c\alpha^2$; where possible, describe each such string as a power α^i of α; and give its discrete logarithm i.

(b) Using your table, or otherwise, find the following three elements of GF(8) as binary strings:
(i) $(1 + \alpha + \alpha^2)^3$ (ii) $(1 + \alpha^2)(1 + \alpha)$ (iii) $(\alpha + \alpha^2)^{-1}$.