Euclidean & Modular Algorithms

(Due date: Sunday March 27th)

1. (a) Prove that in $\mathbb{Z}[x]$ one cannot "divide" x^2 by $2x+1$.

   (b) Let R be an integral domain with field of fractions K, and a, $b \in R[x]$ of degree $n \geq m \geq 0$. Then we can apply the polynomial division algorithm in $K[x]$ to compute q, $r \in K[x]$ such that $a = qb + r$ with $\deg r < \deg b$.

      i. Prove that there exist q, $r \in R[x]$ with $a = qb + r$ and $\deg r < \deg b$ if and only if $\mathrm{lc}(b) \mid \mathrm{lc}(r)$ every time the algorithm passes through the "division" step, and that they are unique in that case.

      ii. Modify the standard Euclidean Algorithm over $F[x]$ in such a way that on inputs a, b, it decides whether q, $r \in R[x]$ exist, and if so, computes them. Show that this takes the same number of operations in R as given in the text, where one operation is either an addition or a multiplication in R, or a test which decides whether an element $c \in R$ divides another element $d \in R$, and if so, computes the quotient $d/c \in R$.

2. (a) For each of the following pairs of integers, find their gcd by using the Euclidean Algorithm:
   $34, 21;\ 136, 51;\ 481, 325;\ 877, 3206.$

   (b) The Euclidean Algorithm for integers can be slightly speeded up if it is permitted to carry out divisions with negative remainders, so that $r_{i-1} = r_i q_i + r_{i+1}$ with $-|r_i/2| < r_{i+1} \leq |r_i/2|$. Do the four examples above using this method.

3. Let R be an Euclidean domain, and $f, g \in R$. Show that the two ideals $\langle f,\, g\rangle$ and $\langle \gcd(f, g)\rangle$ coincide.

4. Prove that the Extended Euclidean Algorithm for positive integers $\lfloor \log f \rfloor = n \geq \lfloor \log g \rfloor = m$ can be performed with $\mathcal{O}(mn)$ word operations.

5. Use the Extended Euclidean Algorithm to compute $\gcd(f, g)$ for f, $g \in \mathbb{Z}_p[x]$ in each of the following examples. In each case, compute the corresponding polynomials s and t such that $\gcd(f, g) = sf + tg$.

   (a) $f = x^3 + x + 1$, $g = x^2 + x + 1$ for $p = 2,\ 3$

   (b) $f = x^4 + x^3 + x + 1$, $g = x^3 + x^2 + x + 1$ for $p = 2,\ 3$

   (c) $f = x^5 + x^4 + x^3 + x + 1$, $g = x^4 + x^3 + x + 1$ for $p = 5$

   (d) $f = x^5 + x^4 + x^3 - x^2 - x - 1$, $g = x^3 + x^2 + x + 1$ for $p = 3,\ 5$

6. Prove that $\mathbb{Z}[x]$ is not an Euclidean domain.

7. Show that for polynomials f, $g \in F[x]$ of degrees $n \geq m$, where F is a field, computing all entries s_i in the Extended Euclidean Algorithm from the quotients q_i takes at most $2m^2 + \mathcal{O}(m)$ operations in F.

8. Let R be an Euclidean domain, and m, $f \in R$.

   (a) Show that $f \bmod m$ is a zero divisor in $R/\langle m \rangle$ if and only if $\gcd(f, m) \neq 1$, if and only if $f \bmod m$ is not invertible in $R/\langle m \rangle$.

   (b) Give an example of a ring containing nonzero elements that are neither units nor zero divisors.

9. Let R be an Euclidean domain and a, b, $c \in R$.

   (a) Show that the congruence $ax \equiv b \bmod c$ has a solution $x \in R$ if and only if $g = \gcd(a, c)$ divides b. Prove that in the latter case, the congruence is equivalent to $(a/g)x \equiv b/g \bmod c/g$.

   (b) For $R = \mathbb{Z}$ and $a = 5, 6, 7$, determine whether the congruence $ax \equiv 9 \bmod 15$ is solvable. If so, give all solutions $x \in \{0, \ldots, 14\}$.

10. Let $m_0, \ldots, m_r \in \mathbb{N}_{\geq 2}$.

    (a) Prove that every nonnegative integer $a < m_0 \ldots m_r$ has a *mixed-radix representation* of the form

    $$a = a_0 + a_1 m_0 + a_2 m_0 m_1 + \ldots + a_r m_0 \ldots m_{r-1},$$

    with unique integers a_i satisfying $0 \leq a_i < m_i$ for all i.

    (b) Relate this to the usual p-adic representation of an integer a, for any integer $p > 1$.

    (c) Compute the above representation of $a = 42$ for $m_0 = 2$, $m_1 = 3$, $m_2 = 2$, and $m_3 = 5$.

    (d) What is the analogue of the mixed-radix representation for polynomials?

11. Let R be a ring (commutative, with 1) and $u \in R$. Prove that Horner's rule not only computes the remainder $f(u)$ of a polynomial $f \in R[x]$ of degree $n-1$ on division by $x - u$, but also the coefficients of the quotient $(f - f(u))/(x - u)$.

12. Let $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ be the finite field with 5 elements.

    (a) Compute a polynomial $f \in \mathbb{F}_5[x]$ of degree at most 2 satisfying

    $$f(0) = 1, \quad f(1) = 2, \quad f(2) = 4. \tag{1}$$

    (b) List all the polynomials $f \in \mathbb{F}_5[x]$ of degree at most 3 satisfying (1). How many of degree at most 4 are there? Generalize your answer to polynomials of degree at most n for $n \in \mathbb{N}$.

13. Let $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ be the finite field with 7 elements, and $m = x(x+1)(x+6) = x^3 + 6x \in \mathbb{F}_7[x]$.

    (a) Let $J \subset \mathbb{F}_7[x]$ be the set of all the polynomials $h \in \mathbb{F}_7[x]$ solving the interpolation problem

    $$h(0) = 1,\ h(1) = 5,\ h(6) = 2.$$

    Compute the unique polynomial $f \in J$ of least degree.

    (b) Find a surjective ring homomorphism $\chi : \mathbb{F}_7[x] \to \mathbb{F}_7^3$ such that $\ker(\chi) = \langle m \rangle$, and compute $\chi(f)$ and $\chi(x^2 + 3x + 2)$.

    (c) Show that $J = f + \ker(\chi)$.

14. Let $r = x^3 + x^2 \in \mathbb{F}_5[x]$.

    (a) List all polynomials $f \in \mathbb{F}_5[x]$ of degree at most 5 satisfying

    $$f(a) = r(a)\ \forall a \in \mathbb{F}_5?$$

    (b) How many polynomials $f \in \mathbb{F}_5[x]$ of degree at most 6 satisfy the equality above?

15. Let F be a field, and $u_0, \ldots, u_{n-1} \in F$ such that $u_i \neq u_j$ if $i \neq j$. For $i = 0, \ldots, n-1$, set $\ell_i = \prod_{j=0,\, j\neq i}^{n-1} \frac{x-u_j}{u_i-u_j} \in F[x]$.

    (a) Show that $\sum_{i=0}^{n-1} \ell_i = 1$.

    (b) Let $u_n \in F$ be another point different from $u_0, \ldots, u_{n-1}$. Show how one can obtain the Lagrange interpolants $\ell_0^*, \ldots, \ell_n^*$ corresponding to $u_0, \ldots, u_n$ from $\ell_0, \ldots, \ell_{n-1}$.

16. What is the least nonnegative integer f with $f \equiv 2 \bmod 3,\ f \equiv 3 \bmod 5$, and $f \equiv 2 \bmod 7$?

17. How many common solutions $f \in \mathbb{Z}$ with $0 \leq f < 10^6$ do the following congruences have

    $$f \equiv 2 \bmod 11,\ f \equiv -1 \bmod 13,\ f \equiv 10 \bmod 17?$$

18. Let F be a field, $u_0, \ldots, u_{n-1} \in F$ distinct, $m = (x-u_0)\ldots(x-u_{n-1}) \in F[x]$, and $f \in F[x]$. Prove that $fm' \equiv \sum_{i=0}^{n-1} \frac{f(u_i)m}{x-u_i} \bmod m$, where m' is the derivative of m.