Exercise 1: The number of coefficients required for Half-GCD (4 points)

Prove Lemma II.3.17: Let \( k \in \mathbb{N}, (f, g) \) and \((f^*, g^*)\) in \((F[x] \setminus \{0\})^2\) coincide up to \(2k\), and \(k \geq \deg f - \deg g \geq 0\). Define \( q, r, q^*, g^* \in F[x] \) for a field \( F \) by division with remainder:
\[
f = qg + r, \quad \deg r < \deg g,
\]
\[
f^* = q^*g^* + r^*, \quad \deg r^* < \deg g^*.
\]
Then, \( q = q^* \), and either
- \((g, r)\) and \((g^*, r^*)\) coincide up to \(2(k - \deg q)\), or
- \(r = 0\), or
- \(k - \deg q < \deg g - \deg r\).

Exercise 2: Bounds on the intermediate values in the EEA (4 points + 4 bonus points)

We consider the Extended Euclidean Algorithm for integer polynomials \( f, g \in \mathbb{Z}[x] \) of degree bounded by \( n \) and coefficients of absolute value less than \( 2^\tau \) as presented in the lecture. As usual, define \( s_i, t_i, \rho_i, r_i, q_i \) as
\[
\rho_0 := \text{LC}(f), \quad r_0 := \text{normal}(f), \quad s_0 := \rho_0^{-1}, \quad t_0 := 0,
\]
\[
\rho_1 := \text{LC}(g), \quad r_1 := \text{normal}(g), \quad s_1 := 0, \quad t_1 := \rho_1^{-1}
\]
and, for \( 1 \leq i \leq \ell \) (with \( \ell \) the index such that \( r_\ell \neq 0 \) and \( r_{\ell+1} = 0 \)),
\[
q_i := r_{i-1} \text{ quo } r_i, \quad \rho_{i+1} := \text{LC}(r_{i-1} \text{ rem } r_i), \quad r_{i+1} := \text{normal}(r_{i-1} \text{ rem } r_i),
\]
\[
s_{i+1} := (s_{i-1} - q_is_i)/\rho_{i+1}, \quad t_{i+1} := (t_{i-1} - q_it_i)/\rho_{i+1}.
\]
Prove that, for each fixed \( i \), there exists a value \( \mu_i \in \mathbb{Z} \) with \( \mu = 2^{O(n(\tau + \log n))} \) such that
\[
\mu_is_i, \mu_it_i, \mu_i\rho_i, \mu_ir_i, \mu_iq_i \in \mathbb{Z}[x]
\]
with coefficients of bitsize \( O(n(\tau + \log n)) \).

Proceed as follows:

1. Use that \( r_i \) is monic and there exists a \( \lambda_i \in \mathbb{Q} \) such that
\[
\lambda_i r_i = \text{Sres}_{n_i}, \quad \lambda_is_i = u_{n_i} \quad \text{and} \quad \lambda_it_i = v_{n_i},
\]
where the \( u_{n_i} \) and \( v_{n_i} \) are the cofactors of the subresultant \( \text{Sres}_{n_i} := \text{Sres}_{n_i}(f, g) \) for \( n_i := \deg r_i \).
2. Recall that

\[ R_i = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix} = R_0 \cdot \prod_{j=1}^{i} Q_j, \quad \text{where} \]

\[ R_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} \quad \text{and} \quad Q_j = \begin{pmatrix} 0 & 1 \\ \rho_{j+1}^{-1} & -q_j \rho_{j+1}^{-1} \end{pmatrix}. \]

and, in particular, \[ \left| \begin{array}{cc} s_i & t_i \\ s_{i+1} & t_{i+1} \end{array} \right| = (-1)^{i-1}(\rho_0 \cdots \rho_i)^{-1}. \]

Use these identities to derive a bound on the bitsize of numerator and denominator of the \( \rho_i \).

3. Prove that \( f = q \cdot g \) with \( f, g \in \mathbb{Z}[x] \) and \( q \in \mathbb{Q}[x] \) implies that there exists a \( \lambda \in \mathbb{Z} \) with \( |\lambda| < 2^\tau \) such that

\[ \lambda \cdot q \in \mathbb{Z}[x] \quad \text{and} \quad \|\lambda q\|_{\infty} = 2^{O(n+\tau)}. \]

4. Use the fact that \( r_{i-1} = q_i r_i + \rho_{i+1} r_{i+1} \) and the previous result to derive a bound on the size of \( q_i \).

**Exercise 3: Modular GCD computation (4 points)**

Let \( f, g \in \mathbb{Z}[x] \) be integer polynomials of degree bounded by \( n \) and coefficients of absolute value less than \( 2^\tau \), let \( p \) be prime such that \( p \nmid \text{LC}(f) \) and \( p \nmid \text{LC}(g) \), and define \( d := \deg \gcd(f, g) \) to be the degree of the GCD of \( f \) and \( g \).

1. Show that

\[ \gcd(f, g) \equiv \gcd(\bar{f}, \bar{g}) \mod p \quad \text{if and only if} \quad p \nmid \text{sres}_d(f, g), \]

where \( \bar{f} \) and \( \bar{g} \) are the modular images of \( f \) and \( g \) in \( \mathbb{Z}/p\mathbb{Z}[x] \).

2. Develop a modular algorithm to compute under guarantee the degree \( d \) of \( \gcd(f, g) \in \mathbb{Z}[x] \) and determine its bit complexity in terms of \( n \) and \( \tau \).

**Exercise 4: A bit of number theory (4 points)**

We define, for \( n, r \in \mathbb{Z} \) with \( \gcd(n, r) = 1 \), the order of \( n \) in \( \mathbb{Z}/r\mathbb{Z} \) as

\[ o_r(n) := \min\{k \geq 1 : n^k \equiv 1 \mod r\} \]

and Euler’s totient (or phi) function as

\[ \varphi(r) := \#\{k \leq r : \gcd(k, r) = 1\}. \]

Prove the following statements:

1. \( o_r(n) \mid \varphi(r) \).

2. If \( o_r(n) > 1 \), then there exists a prime \( p \) with \( p \mid n \) and \( o_r(p) > 1 \).

Merry Christmas and a happy new year!