Due date: 27.10.2020

Theorem (Chinese remainder theorem). *Let R be a commutative ring with unity and consider the ideals $I_1, \dots, I_n \subseteq R$, where $n \in \mathbb{Z}^+$. The map*

$$\varphi : R \to R/I_1 \times \cdots \times R/I_n$$
$$r \mapsto (r + I_1, \dots, r + I_n)$$

is a ring homomorphismus whose kernel is precisely $I_1 \cap \cdots \cap I_n$. If the ideals $I_1, \dots, I_n$ are pairwise comaximal,[1] then φ is surjective and $I_1 \cap \cdots \cap I_n = I_1 \cdot \cdots \cdot I_n$.

Note: For rings R_1, R_2 the operation $R_1 \times R_2$ denotes their direct product. Furthermore, given ideals I, J in a ring R the operations $I + J$ and $I \cdot J$ denote the usual ideal addition and product, respectively.

10. Exercise

Consider the extended definition[2] of a greatest common divisor (GCD): A *greatest common divisor* of a finite number of polynomials $f_1, \dots, f_n \in K[x]$, where K is a field and $n \geq 2$, is a polynomial $g \in K[x]$ with the following properties:

1. The polynomial g divides all polynomials $f_1, \dots, f_n$.
2. If h is another polynomial which divides all $f_1, \dots, f_n$, then h divides g.

When g satisfies these properties we write $g = \gcd(f_1, \dots, f_n)$.

The GCD of a finite number of polynomials exists and is unique up to multiplication by nonzero constants in K. Prove the following claims:

(a) The GCD generates the ideal spanned by the f_i, i.e.

$$\langle \gcd(f_1, \dots, f_n) \rangle = \langle f_1, \dots, f_n \rangle.$$

(b) For $n > 2$ the identity

$$\gcd(f_1, f_2, \dots, f_n) = \gcd(f_1, \gcd(f_2, \dots, f_n))$$

holds. This shows that we can compute the GCD of finitely many polynomials with the (two-input) algorithm `GCD_EUCLID`.

[1] Recall that ideals I, J of the ring R are comaximal if $I + J = R$.
[2] Cf. Definition 2.1.1 in the lecture notes.

11. Exercise

Let I be an integral domain and consider polynomials $a, b \in I[x]$ such that $b \neq 0$ and $m = \deg(a) \geq \deg(b) = n$. Show that there are uniquely defined polynomials $q, r \in I[x]$ such that $\operatorname{lc}(b)^{m-n+1}\, a = q \cdot b + r$ and either $r = 0$ or $\deg(r) < \deg(b)$.

12. Exercise

Let $m_1, \dots, m_n \in \mathbb{Z}$ be pairwise relatively prime integers and $n \in \mathbb{Z}^+$.

(a) Let $a_1, \dots, a_n \in \mathbb{Z}$. Show with the Chinese remainder theorem that there exists a solution $x \in \mathbb{Z}$ of the simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ &\vdots \\ x &\equiv a_n \bmod m_n \end{aligned}$$

such that x is unique modulo $\prod_{i=1}^{n} m_i$.

(b) Solve the following Chinese remainder problem, i.e. find a solution $x \in \mathbb{Z}$ of the system of simultaneous congruences

$$\begin{aligned} x &\equiv 62 \bmod 79 \\ x &\equiv 66 \bmod 83 \\ x &\equiv 72 \bmod 89. \end{aligned}$$

13. Exercise

Consider the polynomials

$$\begin{aligned} f &= x^7 - 3\,x^5 - 2\,x^4 + 13\,x^3 - 15\,x^2 + 7\,x - 1 \\ g &= x^6 - 9\,x^5 + 18\,x^4 - 13\,x^3 + 2\,x^2 + 2\,x - 1. \end{aligned}$$

Compute $h = \gcd(f, g)$ in $\mathbb{Z}[x]$ using the modular algorithm. Verify whether the integer factors of the resultant of f/h and g/h are unlucky primes in the modular approach to GCD computation.

14. Exercise

Let U be a unique factorization domain (UFD). Show that the polynomial ring $U[x]$ is a UFD as well. Can we conclude that the multivariate polynomial ring $K[x_1, \dots, x_n]$ is a UFD, where K is a field and $n \in \mathbb{Z}^+$?