to be prepared for 16.12.2014

Exercise 38. Solve the Chinese remainder problem

$$\begin{aligned} r &\equiv 62 \mod 79 \\ r &\equiv 66 \mod 83 \\ r &\equiv 72 \mod 89 \end{aligned}$$

over the integers both by the Lagrange and by the Newton method.

Exercise 39. Let D be a Euclidean domain. Prove the following lemma.

1. Let $m_1, \ldots, m_n \in D^\star$ be pairwise relatively prime and let $M = \prod_{i=1}^{n-1} m_i$. Then m_n and M are relatively prime.
2. Let $r, r' \in D$, and $m_1, m_2 \in D^\star$ be relatively prime. Then $r \equiv r' \mod m_1$ and $r \equiv r' \mod m_2$ if and only if $r \equiv r' \mod m_1 m_2$.

Exercise 40. Consider the two polynomials over $\mathbb{Z}$

$$\begin{aligned} f(x) &= 6x^5 + 2x^4 - 19x^3 - 6x^2 + 15x + 9 \\ g(x) &= 5x^4 - 4x^3 + 2x^2 - 2x - 2 \ . \end{aligned}$$

Compute $\gcd(f(x), g(x))$ by the modular algorithm.

Exercise 41. Compute the squarefree factorization of

1. $f(x) = x^6 - x^5 + x^3 - x^2$ over the field $\mathbb{Z}_3$.
2. $g(x) = x^7 + x^5 + x^4 + x^3 + x^2 + 1$ over $GF(9)$.

Exercise 42. Prove the following theorem [1]. Let K be a field of characteristic 0, and $a(x_1, \ldots, x_n) \in K[x_1, \ldots x_n]$. Then a is squarefree if and only if $\gcd\left(a, \frac{\partial a}{\partial x_1}, \ldots, \frac{\partial a}{\partial x_n}\right) = 1$.

[1] Theorem 4.4.2, F. Winkler, Polynomial Algorithms in Computer Algebra