to be prepared for 7th November

Exercise 21. Consider the ring $\mathbb{Z}$ of integers and an ideal I generated by finitely many numbers $a_1, \ldots, a_n$. As $\mathbb{Z}$ is a principal ideal domain there must be a single generator b for I.

1. Describe a procedure for finding b when arbitrary generators $a_1, \ldots, a_n$ of I are given as an input.
2. Compute a single generator for the ideal $I = \langle 33600, 784080, 214500 \rangle$.

Exercise 22. Consider the polynomials $U(x), V(x)$ computed by the extended Euclidean algorithm for the input polynomials $u(x), v(x)$ over $\mathbb{Q}$, i.e., $\gcd(u, v) = Uu + Vv$. Prove that, if $u = x^m - 1$ and $v = x^n - 1$, then the extended Euclidean algorithm provides polynomials U, V with integer coefficients. Find U and V when $u = x^{23} - 1$ and $v = x^{18} - 1$.

Exercise 23. For $m \in \mathbb{Z}$ let $\mathbb{Z}_m$ denote the group $\mathbb{Z}/m\mathbb{Z}$. Prove the following statement:

If $k, n \in \mathbb{Z}$ are relatively prime then $\mathbb{Z}_{kn} \cong \mathbb{Z}_k \oplus \mathbb{Z}_n$.

Exercise 24. 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 $\gcd(f(x), g(x))$

1. by passing to the quotient field;
2. by a polynomial remainder sequence.

Exercise 25. Consider the bivariate polynomials

$$\begin{aligned} f(x,y) &= x^2y^3 - 5xy^3 + 6y^3 - 6xy^2 + 18y^2 + 2xy - 4y - 12, \\ g(x,y) &= x^2y^3 + 3xy^3 - 10y^3 - 6xy^2 - 30y^2 - 4xy + 8y + 24. \end{aligned}$$

Compute the gcd of f and g by the modular algorithm. Take care of leading coefficients.