to be prepared for December 5

Exercise 36. Given the polynomials

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

compute their gcd $h \in \mathbb{Z}[x]$. Check whether the integer factors of the resultant of f/h and g/h are unlucky primes in the modular approach to gcd computation.

Exercise 37. How many factors does $u(x) = x^4 + 1$ have in $\mathbb{Z}_p[x]$, p a prime? (Hint: Consider the cases $p = 2,\ 8k+1,\ 8k+3,\ 8k+5,\ 8k+7$ separately).

Exercise 38. Compute the factorization of

$$p(x) = 112x^4 + 58x^3 - 31x^2 + 107x - 66$$

modulo 3 and modulo 11.

Exercise 39. Let $a(x) = 5x^3 + 9x^2 - 146x - 120 \in \mathbb{Z}[x]$. Lift the factorization of $a(x)$ mod 3 to a factorization mod 27. Check whether the result gives a factorization of $a(x)$ in $\mathbb{Z}[x]$.

Exercise 40. Apply the algorithm `FACTOR_BH` for factoring the integral polynomial

$$a(x) = 2x^6 - 6x^5 - 101x^4 + 302x^3 + 148x^2 - 392x - 49.$$

As the prime use 5. All the coefficients of factors of a are bounded in absolute value by 12.