Exercises for Chapter 3

Exercise 1 – [Wilson]

1. Let $\mathbb{F}_q$ be a finite field. Prove that

$$\prod_{\alpha \in \mathbb{F}_q^\times} \alpha = -1,$$

and in particular that if p is prime $(p-1)! \equiv -1 \bmod p$.

2. Conversely, show that $n \geq 2$ being an integer such that $(n-1)! \equiv -1 \bmod n$, then n is prime.

Exercise 2 – [Yun's algorithm]

Yun's algorithm is an efficient algorithm that computes not only the squarefree part but the full squarefree decomposition of a polynomial: if k is a field and if $P \in k[x]$ is nonconstant and monic, the squarefree decomposition of P is

$$P = f_1 f_2^2 \cdots f_m^m$$

where the f_i are monic squarefree pairwise coprime polynomials and $f_m \neq 1$. With the same notation the squarefree part of P is $f_1 \cdots f_m$. For instance, the squarefree decomposition of $x^4(x+1)^2(x-1)^2(x^2+1)^2(x^2+x+1)$ in $\mathbb{Q}[X]$ is $(x^2+x+1)(x^4-1)^2(1)^3(x)^4$. Thus f_i is the product of the irreducible monic polynomials that divide P exactly i times.

1. We first suppose that k has characteristic zero. Let $f_1, \ldots, f_m \in k[X]$ be monic squarefree and pairewise coprime polynomials. Let us put

$$f = f_1 \cdots f_m \quad \text{and} \quad g = \sum_{1 \leq i \leq m} c_i f_i' \frac{f}{f_i},$$

for some constants $c_i \in k$. Show that

$$\gcd(f, g - cf') = \prod_{c_j = c} f_j.$$

2. Consider the following algorithm. Given $f \in k[X]$ monic of degree $n \geq 1$, where k has still characteristic zero:

1. Put $i = 1$, $u = \gcd(f, f')$, $v_1 = f/u$ and $w_1 = f'/u$
2. While $v_i \neq 1$ do
   $h_i = \gcd(v_i, w_i - v_i')$, $v_{i+1} = v_i/h_i$, $w_{i+1} = (w_i - v_i')/h_i$, $i = i + 1$
   End do
3. Return $(h_1, \ldots, h_{i-1})$

Show that the final h_j give the squarefree decomposition of f: $f = h_1 h_2^2 \cdots h_{i-1}^{i-1}$.

3. Show that it uses $\tilde{O}(n)$ operations in k.

4. Suppose $f = abc^2d^4$ for monic distinct irreducible polynomials $a, b, c, d \in k[X]$. Follow in detail the different steps of the algorithm applied to this f.

5. Suppose from now on that $k = \mathbb{F}_q$ with $q = p^\ell$ and that $f \in k[X]$ monic and nonconstant has squarefree decomposition $f_1 f_2^2 \cdots f_m^m$. Show that the previous algorithm returns the correct answer if $m < p$.

6. Let $m \geq p$. Show that the algorithm when applied to f computes

$$h_i = \prod_{j \equiv i \bmod p} f_j$$

for $1 \leq i < p$ and $h_i = 1$ for $i \geq p$.

7. Modify the algorithm so as to work also for $m \geq p$.

8. Show that the modified algorithm takes $\tilde{O}(\ell n)$ operations in $\mathbb{F}_q$.

9. Trace the algorithm with $f = ab^2c^2d^6e^8 \in \mathbb{F}_2[X]$ where $a, b, c, d, e \in \mathbb{F}_2[X]$ are irreducible and pairwise coprime.

Exercise 3 – [Probability to be squarefree]

We want to prove that for a prime power $q = p^f$ and a positive integer $n \geq 2$, the probability for a random polynomial in $\mathbb{F}_q[X]$ of degree n to be squarefree is $1 - 1/q$ (Carlitz, 1932).

Let s_n denote the number of monic squarefree polynomials of degree n in $\mathbb{F}_q[X]$. Then $s_0 = 1$ and $s_1 = q$.

1. Prove the recursive formula

$$\sum_{0 \leq 2k \leq n} q^k s_{n-2k} = q^n.$$

2. Prove that $s_n = q^n - q^{n-1}$ if $n \geq 2$ and conclude.

Exercise 4 – [Irreducible factors of $X^n - 1$ in $\mathbb{F}_q[X]$]

Let $q = p^f$ a prime power and $n \geq 2$ coprime to q. We define an equivalence relation $\sim$ on $\mathbb{Z}/n\mathbb{Z}$ by

$$x \sim y \iff \text{there exists } l \in \mathbb{Z} \text{ such that } y = xq^l.$$

Let $S_1, \ldots, S_r$ be the distinct equivalence classes of $\mathbb{Z}/n\mathbb{Z}$ with respect to $\sim$ and

$$b_i = \sum_{j \in S_i} x^j \in \mathbb{F}_q[X] \quad \text{for } 1 \leq i \leq r.$$

1. Consider $B \subseteq \mathbb{F}_q[X]/\langle T \rangle$ the Berlekamp algebra associated to the polynomial $T = X^n - 1$. Show that a basis of B is given by $b_1 \bmod T, \ldots, b_r \bmod T$.

2. Give a probabilistic algorithm which computes all irreducible factors of $X^n - 1$ in $\mathbb{F}_q[X]$ using an expected number of $\tilde{O}(n \log q)$ field operations in $\mathbb{F}_q$ (Prange, 1959).

Exercise 5 – [Irreducibility in $\mathbb{F}_q[X]$]

Let $q = p^f$ a prime power.

1. For any $d \geq 1$, show that $X^{q^d} - X \in \mathbb{F}_q[X]$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[X]$ whose degree divides d.

2. Let $f \in \mathbb{F}_q[X]$ of degree $n \geq 1$. Show that f is irreducible if and only if

(i) f divides $X^{q^n} - X$;

(ii) $\gcd(X^{q^{n/t}} - X, f) = 1$ for all prime divisor of n.

3. Assume that we know the prime divisors of n. Write an algorithm which tests the irreducibility of $f \in \mathbb{F}_q[X]$ using $\tilde{O}(n^{(\omega+1)/2} + n \log q)$ operations in $\mathbb{F}_q$. We shall admit here that if R is a commutative unitary ring and if $f, g, h \in R[X]$ with $f \neq 0$ monic, $\deg g$, $\deg h < \deg f = n$, there exists an algorithm which computes $g(h) \bmod f$ with $O(n^{(\omega+1)/2})$ operations in R.

4. Let $I(n, q)$ be the number of monic irreducible polynomials of degree n in $\mathbb{F}_q[X]$. Prove that

$$\frac{q^n - 2q^{n/2}}{n} \leq I(n, q) \leq \frac{q^n}{n}.$$

5. Prove that if n is prime, there are exactly $(q^n - q)/n$ distinct monic irreducible polynomials of degree n in $\mathbb{F}_q[X]$ and find a simple formula when n is a prime power.

6. Show that, using our previous algorithm, we can find a uniformly random

irreducible polynomial of degree n in $\mathbb{F}_q[X]$ using an expected number of $\tilde{O}(n^{(\omega+3)/2} + n^2 \log q)$ operations in $\mathbb{F}_q$.

7. Consider now the following algorithm (Ben–Or's generation of a uniformly random monic irreducible polynomial of degree n in $\mathbb{F}_q[X]$).

1. randomly choose a monic polynomial $f \in \mathbb{F}_q[X]$ of degree n;
2. for i from 1 to $\lfloor n/2 \rfloor$ put $g_i = \gcd(X^{q^i} - X, f)$ and if $g_i \neq 1$ then goto 1;
3. return f.

Show that Ben–Or's algorithm works correctly as specified and takes an expected number of $\tilde{O}(n^2 \log q)$ operations in $\mathbb{F}_q$.

Exercise 6 – [Gauss Lemma, Eisenstein criterion, cyclotomic polynomials]

1. Let R be a UFD and P, $Q \in R[X]$. Show that $\mathrm{cont}(PQ) = \mathrm{cont}(P)\mathrm{cont}(Q)$.

2. Let $P \in R[X]$ non constant and K the field of fractions of R. Show that P is irreducible in $R[X]$ if and only if it is primitive and irreducible in $K[X]$.

3. Show that $R[X]$ is also a UFD and describe the primes of $R[X]$.

4. Let $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Suppose that there exists a prime p such that

$$p \nmid a_n, \;\; p \mid a_i \text{ for } 0 \leq i \leq n-1 \text{ and } p^2 \nmid a_0.$$

Show that P is irreducible in $\mathbb{Q}[X]$.

5. Let p be a prime and $\Phi_p = (X^p - 1)/(X - 1) = 1 + X + \cdots + X^{p-1}$ the p-th cyclotomic polynomial. By a suitable variable changing, prove that Φ_p is irreducible in $\mathbb{Q}[X]$.

6. Let $n \geq 1$ and Φ_n the n-th cyclotomic polynomial defined by

$$\Phi_n = \prod_{\zeta \in \Omega_n} (X - \zeta),$$

where Ω_n is the set of primitive n-th roots of 1. Show that this definition is compatible with the previous one in the case n prime. Then prove that $\Phi_n \in \mathbb{Z}[X]$ and is irreducible in $\mathbb{Q}[X]$ for every n.

7. Let $n = pq$ where p and q are distinct odd primes. Prove that the n-th cyclotomic polynomial Φ_n (which is irreducible in $\mathbb{Q}[X]$) splits modulo any prime into at least two factors.

Exercise 7 – [Elementary approaches]

1. Let $P = X^{10} + X + 1$. Using Berlekamp algorithm, we find that the factorizations of P into monic irreducible factors over $\mathbb{F}_p$ for $p = 2, 3, 5$ respectively are:

$$\begin{aligned} P &\equiv (X^3 + X + 1)(X^7 + X^5 + X^4 + X^3 + 1) \mod 2 \\ P &\equiv (X - 1)(X^3 - X^2 - X - 1)(X^6 - X^5 + X^4 - X^3 + X + 1) \mod 3 \\ P &\equiv (X^2 - X + 2)(X^8 + X^7 - X^6 + 2X^5 - X^4 + 2X^2 + 2X - 2) \mod 5. \end{aligned}$$

What can we say of P in $\mathbb{Q}[X]$?

2. Let p and q be two odd primes. We assume that $q \equiv 2 \bmod 3$ and that p is a primitive root modulo q. Show that the polynomial

$$P = X^{q+1} - X + p$$

is irreducible in $\mathbb{Q}[X]$.

3. Show that this criterion does not work with $P = X^4 + 1$. More precisely, prove that P splits modulo p into 4 linear factors if $p = 2$ or $p \equiv 1 \bmod 8$, into two irreducible quadratic factors otherwise, and that P is irreducible in $\mathbb{Q}[X]$. Hint: make use of the quadratic reprocity law.

4. Consider now the polynomial

$$P = X^6 - 6X^4 - 2X^3 - 7X^2 + 6X + 1.$$

Show that if Q is a factor of P of degree less or equal to 3 then its coefficients are bounded in absolute value by 23.

5. Berlekamp algorithm shows that over $\mathbb{Z}/47\mathbb{Z}$ we have

$$P = (X - 22)(X - 13)(X - 12)(X + 12)(X^2 - 12X - 4),$$

where the five factors are irreducible in $\mathbb{Z}/47\mathbb{Z}[X]$. Thanks to this decomposition, find the factorization of P into a product of monic irreducible polynomials in $\mathbb{Q}[X]$.

Exercise 8 – [Swinnerton-Dyer polynomials]

Recall that the n-th Swinnerton-Dyer polynomial is defined by

$$P_n = \prod (X \pm \sqrt{2} \pm \sqrt{3} \pm \sqrt{5} \pm \cdots \pm \sqrt{p_n}),$$

where p_n is the n-th prime number and where the product runs over all 2^n possible combinations of sign $+$ and $-$ signs.

1. Prove that $P_n \in \mathbb{Z}[X]$ for every $n \geq 1$.

2. Factor P_2 modulo 2, 3 and 5. and prove that P_2 is irreducible.

3. Prove that P_n is irreducible in $\mathbb{Q}[X]$ for every $n \geq 1$. Hint: consider $K = \mathbb{Q}(\sqrt{2}, \ldots, \sqrt{p_n})$ and use Galois theory.

4. Let p be a prime number and $n \geq 1$. Prove that all irreducible factors modulo p of P_n have degree at most 2 and if p does not divide the discriminant of P_n, they are either all linear or all quadratic.

Exercise 9 – [Linear Hensel step]

Let $p \in \mathbb{Z}_{>1}$. In Hensel step algorithm, we replace $sg + ht \equiv 1 \bmod m$ by $sg + ht \equiv 1 \bmod p$. In step 1 we perform computations modulo mp instead of m^2 and step 2 is omitted completely.

1. Prove that the output specifications for f, g^* and h^* hold if m^2 is replaced by pm.

2. Let $f \in \mathbb{Z}[X]$ and $g, h, r, s \in \mathbb{Z}[X]$ such that $f \equiv gh \bmod p$ and $sg + ht \equiv 1 \bmod p$. Using the previous linear Hensel step, write an algorithm which computes a factorization of f modulo p^l for some $l \geq 1$.

3. Compare the complexity of this new algorithm to the complexity of the algorithm which makes use of the usual quadratic Hensel step.

Exercise 10 – [Hensel lifting]

Let $f = X^{15} - 1 \in \mathbb{Z}[X]$.

1. Take a nontrivial factorization $f \equiv gh \bmod 2$ with $g, h \in \mathbb{Z}[X]$ monic and of degree at least 2.

2. Compute g^* and $h^* \in \mathbb{Z}[X]$ such that

$$f \equiv g^* h^* \bmod 16, \quad \deg g^* = \deg g, \quad g^* \equiv g \bmod 2.$$

3. Can you guess some factors of f in $\mathbb{Z}[X]$?

Exercise 11 – [Hensel lifting]

Let $f = 14X^4 + 15X^3 + 42X^2 + 3X + 1 \in \mathbb{Z}[X]$.

1. Find a suitable prime p such that $f \bmod p$ is squarefree and has degree 4.

2. Compute the irreducible factorization of $f \bmod p$ in $\mathbb{F}_p[X]$. Choose

two factors $g, h \in \mathbb{Z}[X]$ that are coprime modulo p such that h is monic and irreducible modulo p and $f \equiv gh \bmod p$. Determine $s, t \in \mathbb{Z}[X]$ with $sg + th \equiv 1 \bmod p$.

3. Execute two Hensel steps to obtain a factorization $f \equiv g^* h^* \bmod p^4$ with $g \equiv g^* \bmod p$ and $h \equiv h^* \bmod p$. Can you derive a factorization of f in $\mathbb{Q}[X]$ from it?

Exercise 12 – [Examples in number fields]

Let us see here some illustrations of the algorithm (seen in course) which gives the factorization of a polynomial over a number field. For this, if you are lazy or tired, you can obtain factorizations in $\mathbb{Q}[X]$ with the help of a computer.

1. Factor

$$P = x^3 - (7 - 3\sqrt{2})X + 5\sqrt{2} - 6$$

into a product of monic irreducible polynomials of $K[X]$ where $K = \mathbb{Q}(\sqrt{2})$.

2. Same question with $K = \mathbb{Q}(\sqrt{-3})$ and

$$P = X^3 + \frac{1 - 5\sqrt{-3}}{2}X^2 + \frac{3 - 5\sqrt{-3}}{2}X - 1 - 5\sqrt{-3}.$$

3. Same question with $K = \mathbb{Q}(\alpha)$ where α is a root of $X^3 - X^2 - 9X + 8$ and

$$P = X^3 - (6\alpha - 9)X^2 + (5\alpha^2 - 33\alpha + 13)X - 5\alpha + 30.$$