TD ACCQ 201

Julien Béguinot, Duong Hieu Phan

Télécom Paris

1 Reminder

Theorem 1 (Wilson)**.** *Let $p > 1$. p is prime if and only if*

$$(p-1)! + 1 = 0 \bmod p$$

Theorem 2 (Euler)**.** *Let φ be Euler indicator function and $n > 1$. If k is coprime with n then $k^{\varphi(n)} = 1 \pmod n$.*

Definition 1 (Legendre Symbol)**.** Let p be a prime odd number. The Legendre symbol (n/p) is defined as

$$\left(\frac{n}{p}\right) : \begin{cases} 0 \text{ if } p \text{ divides } n \\ +1 \text{ if } p \text{ does not divide } n \text{ and } n \text{ is a square mod } p \\ -1 \text{if } p \text{ is not a square mod } p \end{cases}.$$

Theorem 3 (Quadratic Residuosity)**.** *Let $a \in \mathbb{Z}, p \not| a$, p odd prime.*

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \pmod p.$$

Definition 2 (Jacobi Symbol)**.** Let $a \in \mathbb{Z}$ and $n \in 2\mathbb{N}+1$. We assume that $n = \prod_{i=1}^{k} p_i$. Then the Jacobi symbol generalizes the Legendre symbol as

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right).$$

It verifies the following properties:

- it is zero if and only if a and n are not co-prime
- it is multiplicative in a and in n
- if $a = b \,(\mathrm{mod} n)$ then $(a/n) = (b/n)$.
- $$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \qquad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \qquad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

Definition 3. Let A be a commutative ring. A GCD for A is a mapping $\mathrm{GCD} : (a, b) \in A^2 \mapsto d \in A$ such that

- d divides both a and b
- If e divides a and b then d divides d.

Definition 4. The fraction field of the integral ing A is the smallest field that contains A. For instance the fraction field of $\mathbb{Z}$ is $\mathbb{Q}$.

Definition 5. A unitary polynomial is a polynomial whose leading coefficient is equal to 1.

Definition 6. A polynomial with coefficient in a factorial ring A is said to be primitive if the greatest common divisors of its coefficient is 1.

Definition 7. A field K is said to be algebraicaly closed if every polynomial P of $K[X]$ of degree at least 1 admits at least one root in K.

Theorem 4. *The following assertions are equivalent:*
- *All non constant polynomials of $K[X]$ splits as a product of polyniomial of degree* 1 *in $K[X]$*
- *All non constant polynomials of $K[x]$ admits at least one root in K.*
- *All irreducible polynomials of $K[X]$ is of degree* 1.

Definition 8 (Field Extension)**.** An extension L of a field K is a field that contains K. The extension degree $[L : K]$ is the dimension of L seen as K-vectorial space. The extension L is said to be algebraic if all elements of L is the root of a polynomial in $K[X]$, else it is said to be transcendant.

Theorem 5. *The extension degree is multiplicative. Namely if $K \subseteq L \subseteq M$ then*

$$[K : M] = [K : L][L : M].$$

Definition 9 (Minimal Polynomial)**.** Let K be a field and L an algebraic extension of K. Let $a \in L$. The minimal polynomial $\mu_a \in K[X]$ of a over K is the unitary polynomial with minimal degree such that $\mu_a(a) = 0$. This polynomial is always irreducible.

Definition 10. The other roots of μ_a are termed the **conjugates** of a.

Definition 11 (Rupture/Splitting Field)**.** Let P be a polynomial over the field K, irreducible over K. A rupture field of K is a minimal extension L of K such that P has a root in a. A splitting field of P is a minimal extension L of K such that P splits has a product of factors of degree 1 in L. For instance $\mathbb{C}$ is a rupture/splitting field of $X^2 + 1 \in \mathbb{R}[X]$.

Theorem 6. *Let P be a polynomial over the field K, irreducible over K. The splitting field of P is unique up to isomorphism.*

Theorem 7. *Let $d = \deg \mu_a$. Let $K \subseteq M \subseteq L$ be a rupture field of μ_a, then $[M : K] = d$. We also write $M \triangleq K(a) = K[X]/(\mu_a)$ the smallest subfield of L containing a. In particular $K(a)$ can be seen as a K vectorial space with basis* $(1, a, \ldots, a^{d-1})$.

2 Exercices

Exercice 1. *Let $G \subset K^*$ be a finite subgroup of the group of invertible of the field K. Prove that G is a cyclic group. As a consequence $\mathbb{Z}_p^*$ is cyclic.*

Solution 1. Let $n \triangleq |G|$ be the order of the considered subgroup. n is uniquely decomposed as a product of primes $n = \prod_{i=1}^{q} p_i^{\nu_i}$ We write $G \triangleq \{g_1, \ldots, g_n\}$. Let $m \triangleq \mathrm{LCM}(\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_n))$ and $\mathrm{ord}(g_j) = \prod_{i=1}^{q} p_i^{\nu_{i,j}}$. Then $m = \prod_{i=1}^{q} p_i^{\max_j \nu_{i,j}}$ we first show that $m = n$.
- By Lagrange theorem $\mathrm{ord}(g_i)|n$ i.e. for all $i \in \{1, \ldots, q\}, j \in \{1, \ldots, n\}$ we have $\nu_{ij} \leqslant \nu_i$. It follows that $m \leqslant n$.
- Let $P(X) = X^m - 1$. Then all the n distinct g_i a roots of P so $n \leqslant m$.

So far we proved that $m = n$. It remains to exhibit an element of order m in G. By construction of the LCM for all i there exist an index j_i such that the p_i-adic valuation of $\operatorname{ord}(g_{j_i})$ is equal to the p_i-adic valuation of m i.e. $\operatorname{ord}(g_{j_i}) = p_i^{\nu_i} u_i$. But then $\operatorname{ord}(g_{j_i}^{u_i}) = p_i^{\nu_i}$. Then $\prod_{i=1^q} g_{j_i}^{u_i}$ is of order $\prod p_i^{\nu_i} = m$. We used the lemma that $\operatorname{ord}(ab) = \operatorname{LCM}(\operatorname{ord}(a), \operatorname{ord}(b))$.

Exercice 2. *Let $n \geqslant 2$ and $a_1, \ldots, a_n$ distinct elements of $\mathbb{Z}$. Show that $P(X) = (X - a_1)\ldots(X - a_n) - 1$ is irreducible in $\mathbb{Z}[X]$.*

Solution 2. Assume $P = QR$ with $Q, R \in \mathbb{Z}[X]$. Then for all k,

$$P(a_k) = Q(a_k)R(a_k) = -1.$$

In particular,

$$Q(a_k) + R(a_k) = 0.$$

Hence the polynomial $Q + R$ has at least n roots. If $\deg(Q + R) < n$ then $Q + R = 0$ and $P = -Q^2$. This is absurd since then P is always negative while its limit in $+\infty$ is clearly $+\infty$. This implies that $\deg(Q + R) = n$. But then either Q or R is constant equal to ± 1. This shows that P is irreducible over $\mathbb{Z}[X]$.

Exercice 3 (Gauss Lemma)**.** *The product of two primitive polynomial in $\mathbb{Z}[X]$ is primitive. A polynomial $P \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$ is and only if it is irreducible in $\mathbb{Q}[X]$ and primitive in $\mathbb{Z}[X]$. We show Gauss lemma in a step by step proof.*

- *Show that the product of two primitive polynomial in $\mathbb{Z}[X]$ is primitive.*
- *Prove that $c(PQ) = c(P)c(Q)$ for $P, Q \in \mathbb{Z}[X]$ where $C(P)$ is the GCD of the coefficent of the polynomial.*
- *Concludes the proof.*

Solution 3.

- We first show that if the prime number p divides all the coefficient of PQ then it necessarily divides all the coefficient of P or the coefficient of Q. If we project P, Q, PQ to $\mathbb{Z}_p$ we obtain that $0 = \bar{PQ} = \bar{P}\bar{Q}$. Since $\mathbb{Z}_p$ is integral $\mathbb{Z}_p[X]$ is integral so either $\bar{P} = 0$ or $\bar{Q} = 0$. As a consequence the product of two primitive polynomials is primitive.
- Now we can show that $C(PQ) = c(P)c(Q)$. For $\mathbb{Z}[X]$ we can define the content as the GCD of all the coefficient. Let $\tilde{P} = \frac{1}{c(P)}P \in Z[X]$ and $\tilde{Q} = \frac{1}{c(Q)}Q \in \mathbb{Z}[X]$ then $c(\tilde{P}) = c(\tilde{Q}) = 1$. Let $R = \tilde{P}\tilde{Q}$ we have $c(R) = 1$. Indeed if by absurd p divides $c(R)$ then it divides all the coeeficient of R os by the previous remark it divides all the coeefficent of $\tilde{P}$ (or $\tilde{Q}$). But $\tilde{P}$ is primitive which is a contradiction. This implies that $c(PQ) = c(P)c(Q)$.
- Let R be ireducible in $\mathbb{Z}[X]$ we show it is irreducible in $\mathbb{Q}[X]$. By the absurd if $R = PQ$ where $P, Q \in \mathbb{Q}[X]$ then by taking α the product of the denominator of the coefficent of P and β the product of the denominator of the coeffient of Q we have $\alpha \in \mathbb{Z}[X]$ and $\beta Q \in \mathbb{Z}[X]$. It follows that

  $$\alpha\beta R = (\alpha P)(\beta Q) = P_1 Q_1 = c(P_1)(\frac{1}{c(P_1)}P_1)c(Q_1)(\frac{1}{c(Q_1)}Q_1) = c(P_1)c(Q_1)P_2Q_2.$$

  Then

  $$\alpha\beta R = \alpha\beta c(R) P_2 Q_2$$

  i.e.

  $$R = c(R)P_2Q_2.$$

  But R is irreducible in $\mathbb{Z}[X]$ and $P_2, Q_2 \in \mathbb{Z}[X]$ so necesssarly P_2 or Q_2 is a constant which concludes the proof. Further if R be ireducible in $\mathbb{Z}[X]$ it is necessarily primitive. The other direction of the implication is clear.

Exercice 4 (Eisenstein)**.** *Let $P(X) = a_n X^n + \ldots + a_1 X + a_0$ be a polynomial in $\mathbb{Z}[X]$. Let p be a prime number such that*

- $p|a_i$ *for* $i = 0, \ldots, n-1$
- $p \not| a_n$
- $p^2 \not| a_0$

then $P(X)$ *is irreducible in* $\mathbb{Q}[X]$*. If further* $GCD(a_0, \ldots, a_n) = 1$ *then it is irreducible in* $\mathbb{Z}[X]$*.*

Solution 4. By absurd. If P is reducible in $\mathbb{Q}[X]$ then it is reducible in $\mathbb{Z}[X]$. Let $P = QR$ with $Q, R \in \mathbb{Z}[X]$ of degree at least 1. We consider the projection in $\mathbb{Z}_p$. We have $\bar{P} = \bar{a_n}X^n = \bar{Q}\bar{R}$. So necessarily $\bar{Q} = \bar{q_a}X^a$ and $\bar{R} = \bar{r_{n-a}}X^{n-a}$ where $n > a > 1$. So $\bar{q_0} = \bar{r_0} = 0$. But then $p|r_0$ and $p|q_0$ so $p^2|p_0$.

Exercice 5. *Show that* $3X^2 + 25X + 10$ *is ireducible in* $\mathbb{Q}[X]$

Solution 5. Apply Eisenstein with $p = 5$.

Exercice 6. *Show that in* $\mathbb{Q}[X]$ *there exists irreducible polynomials of all degrees* $n \geqslant 1$*.*

Solution 6. Apply Eisenstein to $P_n(X) = X^n - 2$ and $p = 2$.

Exercice 7. *Let* p *be a prime number. Let* $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$*. Show that* $\Phi_p(X)$ *is irreducible in* $\mathbb{Z}[X]$*.*

Solution 7.

$$X\Phi_p(X+1) = (X+1)^p - 1$$

so

$$\Phi_p(X+1) = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}.$$

The result then folloows from Eisenstein lemma.

Exercice 8. *Compute* $\left(\frac{2585}{5031}\right), \left(\frac{122}{237}\right)$*.*

Solution 8. Use the relation on Jacobi coefficient to reduce the numerator and denomiator by successive euclidean division.

Exercice 9. *Determine when* $q = 3, 11$ *is a square modulo* p*.*

Solution 9. We use the quadratic residue criterium from Euler. For example for $q = 3$. We know that q is a square modulo p if and only if $(3/p) = 1$. But $(3/p) = (p/3)(-1)^{\frac{p-1}{2}}$. If $p - 1 = 4k$ then we need $(p/3) = 1$ i.e. $p = 3k' + 1$. It follows by Euclide lemma that in this case we need $p = 12k'' + 1$. If $p - 3 = 4k$ then we need $(p/3) = -1$ i.e. $p = 3k' + 2$. By the chinese reminder theorem we copnclude that necessarily $p = 3(3^{-1}(4))3 + 4(4^{-1}(3))2 + 12k'' = 9 + 4 + 12k'' = 1 + 12k'''$. In any case we obtain that 3 is a square modulo p if and only if p is equal to 1 modulo 12. Apply the same method to $q = 11$.

Exercice 10 (Finite Fields Cannot Be algebraically Closed)**.** *Show that a finite field cannot be algebraically closed.*

Solution 10. Let $K = \{\alpha_1, \ldots, \alpha_q\}$. Then $P(X) = 1 + \prod_{i=1}^{q}(X - \alpha_i)$ has no roots in K.

Exercice 11 (D'Alembert's Theorem)**.** *Prove that* $\mathbb{C}$ *is algebraically closed.*

Solution 11.

Finally I give this nice results that is out of the scope of the class but has a nice proof by Ram Murty.

Theorem 8 (Cohn's Criterion)**.** *Let* $b \in \mathbb{N}$*,* $b \geqslant 2$*, and* $P(X) = \sum a_k X^k$ *with* $a_k \in 0, \ldots, b-1$*. If* $P(b)$ *is a prime integer then* P *is irreducible in* $\mathbb{Z}[X]$ *and as a consequence over* $\mathbb{Q}[X]$*.*