1. Finite fields

Definition 1.1. Euler function $\phi(n) \stackrel{\text{def}}{=} \#\{a \le n \,|\, \gcd(a,n) = 1\}$
$(n \in \mathbf{Z}_{>0}, a \in \mathbf{Z}_{>0})$

Theorem 1.2. 1) $\phi(p^k) = p^k - p^{k-1}$ (p prime)
2) $\gcd(m,n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$
3) $\sum_{d|n} \phi(d) = n$

Proof. 1) straightforward ■
2) Consider the natural homomorphizm of abelian groups $r : \mathbf{Z}/(mn) \to \mathbf{Z}/(m) \times \mathbf{Z}/(n)$. Since m and n are relatively prime, $\ker(r) = 0$. The finite grops in both sides are of the same order mn, hence r is an isomorphism. Clearly the residues to the left which are relatively prime to mn correspond to the pairs of residues to the right, the first one being relatively prime to m, the second one to n ■
3) See Problem 1 ■

Theorem 1.3. Let K be a field, K^* its multiplicative group, $G \subset K^*$ a finite subgroup. Then G is cyclic.

Lemma. $\forall d$ the number of elements of order d in G equals either 0 or $\phi(d)$.

Proof of the Lemma. Indeed, suppose there exists an element $a \in G$ of order d. Then the elements $1, a, a^2, a^3, \ldots, a^{d-1}$ are all different and enjoy the equation $x^d = 1$. One may consider the equation $x^d = 1$ in G as the equation $x^d - 1 = 0$ in K, hence by Bézout theorem it has no more than d solutions which therefore are all listed above. In particular, all the elements of order d in G need to be on the list. Clearly a^i is of order d in $G \Leftrightarrow \gcd(i,d) = 1$. ■

Proof of the Theorem. Let $\#G = n$. Then $\sum_{d|n}$ (number of elements of order d in G) $= n$. By Theorem 1.2(3) $\sum_{d|n} \phi(d) = n$. So no term in the first sum equals zero, in particular there exists an element of order n. This means G is cyclic ■

Definition 1.4. Let K be a field. Consider the ring homomorphism $i : \mathbf{Z} \to K$, $1 \stackrel{i}{\mapsto} 1$. The nonnegative generator of the ideal $\ker(i)$ is called the characteristic $\mathrm{char}(K)$.

Remark 1. Alternatively speaking, $\mathrm{char}(K)$ is the minimal positive integer p such that $p \cdot 1 = 0$, or $\mathrm{char}(K) = 0$ if no such integer exists. Here we define $p \cdot 1 = \underbrace{(1 + 1 + \cdots + 1)}_{p \text{ times}}$.

Remark 2. Clearly the image of the homomorphism i is isomprphic to the ring $\mathbf{Z}/(\mathrm{char}(K))$. Since K has no zero divisors $\mathrm{char}(K)$, if nonzero, is a prime number.

Definition-Theorem 1.5. Suppose K is a field, $\mathrm{char}(K) = p$. The map $Fr : K \to K$, $x \overset{Fr}{\mapsto} x^p$ is called the absolute Frobenius map. It is a field homomorphism.

Proof. Clearly it suffices to prove that $(x + y)^p = x^p + y^p$. Since p is prime, all the binomial coefficients, first and last excluded, are divisible by p ■

Remark. Any field homomorphism is injective, hence Fr defines an isomorphism $K \overset{\to}{\sim} K^{(p)}$, $K^{(p)}$ being the subfield of K which consists of all p - powers. In particular, if $\#(K) < \infty$ then $K^{(p)} = K$. The field with this property is called perfect.

Example. Let p be a prime integer. Then the ring $\mathbf{Z}/(p)$ is a field because any nonzero residue mod p is invertible (see Problem 2). The notation is $\mathbf{F}_p$.

Pre-definition 1.6. A field L is called algebraically closed if any polynomial in one variable with coefficients in L splits to a product of factors of degree 1. Equally speaking, any such polynomial has a root in L.

Theorem 1.7. Let p be a prime integer, f some positive integer, $q = p^f$, Ω an algebraically closed field, $\mathrm{char}(\Omega) = p$. Then
1) The equation $x^q - x = 0$ has q different solutions in Ω. The set of these solutions is a subfield of Ω (the notation is $\mathbf{F}_q$).
2) For any prime p such Ω does exist. For any field K such that $\#(K) = q$ there exists an isomorphism $K \overset{\to}{\sim} \mathbf{F}_q$.
3) $\mathbf{F}_p$ in this sense is isomorphic to $\mathbf{F}_p$ from the previous example. $\mathbf{F}_q \supset \mathbf{F}_p$.

Proof. 1) Since Ω is algebraically closed, the polynomial $x^q - x$ has q roots in Ω. Its derivative equals $qx^{(q-1)} - 1 = -1$ hence all the roots are different. By definition the set of all roots coincides with the set $\{x \in \Omega \,|\, Fr^f(x) = x\}$, i.e. with the set of fixed points of the field homomorphism Fr^f, hence it is a subfield ■

2) The order of the additive group K^+ of K equals q. It annihilates any element of the

group, in particular $q \cdot 1 = 0$ hence $p \cdot 1 = 0$, so $\mathrm{char}(K) = p$. In Chapter 3 (Galois theory) we will prove that Ω exists and that for any field K of q elements there exists an inclusion $\sigma : K \hookrightarrow \Omega$. Let $L = \sigma(K)$. $\#(L)=\#(K)=q \Rightarrow \#(L^*) = q-1 \Rightarrow \forall x \in L^*\ x^{q-1} = 1 \Rightarrow x^q = x$. Clearly for $x = 0$ the same is true ■
3) The set of integer multiples of 1 in Ω is a subring of Ω isomorphic to $\mathbf{Z}/(p)$. Hence it is a subfield containing p elements and therefore coincides with $\mathbf{F}_p \subset \Omega$ by the argument above. The rest is clear from the definition of $\mathbf{F}_q$ ■

Theorem 1.8. 1) If $p = 2$ then all elements of $\mathbf{F}_q^*$ are squares.
2) If $p \neq 2$ then $(\mathbf{F}_q^*)^2$ is a subgroup of index 2 in $\mathbf{F}_q^*$. In this case $(\mathbf{F}_q^*)^2$ coincides with the kernel of the group homomorphism $\mathbf{F}_q^* \to \{\pm 1 \in \mathbf{F}_q^*\}$ which sends $a \mapsto a^{\frac{(q-1)}{2}}$.

Proof. 1) See the Remark after Definition 1.5 ■
2) Consider $\mathbf{F}_q$ as a subfield of the algebraically closed field Ω. Let $a \in \mathbf{F}_q$. The equation $x^2 = a$ has a solution in Ω. Then $(x^{q-1})^2 = (x^2)^{q-1} = a^{q-1} = 1$ (if $a \neq 0$) as $a \in \mathbf{F}_q$. Hence either $x^{q-1} = 1$ or $x^{q-1} = -1$. In the first case $x \in \mathbf{F}_q \Rightarrow a$ is a square, while in the second one x cannot be an element of $\mathbf{F}_q$ so a is a non-square. Since $\mathbf{F}_q^*$ is cyclic of order $q-1$ the image of its generator under the homomorphism above differs from 1, so the homomorphism is surjective ■

In what follows we restrict ourselves to the case of prime fields $K = \mathbf{F}_p$.

Definition 1.9. Let p be a prime, $p \neq 2$, a any residue mod p. The Legendre symbol $\left(\frac{a}{p}\right) \stackrel{\text{def}}{=} a^{\frac{p-1}{2}}$.

Remark. Clearly for $a \neq 0$ $\left(\frac{a}{p}\right) = \pm 1$. The Legendre symbol $\left(\frac{0}{p}\right)$ has no much sense but it is useful to set $\left(\frac{0}{p}\right) = 0$ for computations.

Theorem 1.10. 1) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
2) $\left(\frac{1}{p}\right) = 1$.
3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof. 1) - 3) are the direct consequences from the definition ■
4) Consider an algebraically closed field Ω which contains $\mathbf{F}_p$. Our goal is to calculate

$\sqrt{2}$ in Ω. Let ζ be a solution of the equation $\zeta^4+1=0$ (this is in fact a "primitive" 8-th power root of 1). Set $\tau=\zeta+\zeta^{-1}$. Then $\tau^2=2$ (for the proof see Problem 4). In order to check whether $\tau\in\mathbf{F}_p$ one should calculate τ^{p-1}. If $\tau^{p-1}=1$ (i.e. $\tau^p=\tau$) then $\tau\in\mathbf{F}_p$, hence $\left(\frac{2}{p}\right)=1$. Conversely if $\tau^p=-\tau$ then $\left(\frac{2}{p}\right)=-1$. Now recall that $Fr:\Omega\to\Omega$, $x\mapsto x^p$ is a field homomorphism, hence in Ω $\tau^p=(\zeta+\zeta^{-1})^p=\zeta^p+\zeta^{-p}$. To finish the proof see Problem 5 ■

Theorem 1.11 (Gauss reciprocity law). Let p,l be two prime integers different from 2 and from each other. Then $\left(\frac{p}{l}\right)\left(\frac{l}{p}\right)=(-1)^{\frac{p-1}{2}\frac{l-1}{2}}$.

Proof. The proof is close to that of the Theorem 1.10. Consider an algebraically closed field Ω of characteristic p. The proof consists of two steps: we first calculate the $\sqrt{l}$ in Ω and then check whether $(\sqrt{l})^p=\sqrt{l}$ or $(\sqrt{l})^p=-\sqrt{l}$.

Definition 1.12. Let $\zeta\in\Omega$, $\zeta^l=1$, $\zeta\neq 1$. The Gaussian sum $\tau(\zeta)\stackrel{\text{def}}{=}\sum\limits_{a \bmod l}\left(\frac{a}{l}\right)\zeta^a$.

Remark. It is easy to prove that $\tau(\zeta)$ up to a sign does not depend on the choice of ζ. The proof of the statements below will not depend on the choice of ζ so we will use notation τ instead of $\tau(\zeta)$.

Lemma 1. $\tau^2=(-1)^{\frac{l-1}{2}}l$.

Proof. $\tau^2=\sum\limits_{a,b \bmod l}\left(\frac{ab}{l}\right)\zeta^{a+b}=\sum\limits_{c \bmod l}\zeta^c\sum\limits_{t \bmod l}\left(\frac{t(c-t)}{l}\right)$. The term corresponding to $t=0$ in the inner sum is zero, so $\tau^2=\sum\limits_{c \bmod l}\zeta^c\sum\limits_{t \bmod l,\, t\neq 0}\left(\frac{-t^2}{l}\right)\left(\frac{1-ct^{-1}}{l}\right)$. $\left(\frac{-t^2}{l}\right)=\left(\frac{-1}{l}\right)=(-1)^{\frac{l-1}{2}}$, so $(-1)^{\frac{l-1}{2}}\tau^2=\sum\limits_{c \bmod l}\zeta^c S_c$, where $S_c=\sum\limits_{t \bmod l,\, t\neq 0}\left(\frac{1-ct^{-1}}{l}\right)$. Clearly if $c=0$ then $S_c=l-1$ being the sum of $l-1$ copies of $\left(\frac{1}{l}\right)=1$. If $c\neq 0$ then the "numerator" in the sum runs over all residues mod l, 1 mod l being excluded. Hence $S_c=\sum\limits_{s \bmod l}\left(\frac{s}{l}\right)-\left(\frac{1}{l}\right)=-1$ (the sum to the left equals zero as the number of squares in $\mathbf{F}_l^*$ equals the number of non-squares). Finally, $(-1)^{\frac{l-1}{2}}\tau^2=l-1-\sum\limits_{c \bmod l,\, c\neq 0}\zeta^c=l-1-(\frac{1-\zeta^l}{1-\zeta}-1)=l$ as $\zeta^l-1=0$ by definition of ζ ■

Lemma 2. $\tau^p = \left(\frac{p}{l}\right)\tau$

Proof. $\tau^p = \sum\limits_{a \bmod l} \left(\frac{a}{l}\right)\zeta^{ap}$. In fact, in Ω the p-th power of the sum equals the sum of the p-th powers of its terms while the Legendre symbol does not change after taking its p-th power. Hence $\tau^p = \sum\limits_{c \bmod l} \left(\frac{cp^{-1}}{l}\right)\zeta^c = \left(\frac{p^{-1}}{l}\right)\tau = \left(\frac{p}{l}\right)\tau$ ■

Remark. The proof of Lemma 2 is based on the property $\mathrm{char}(\Omega) = p$ which we never did use in the proof of Lemma 1.

Proof of the Theorem (based on the Lemmas). See Problem 6 ■

Problems (the deadline for the Problems 1-6 is Tuesday, September, 24th).

1. Prove that $\sum\limits_{d|n} \phi(d) = n$ (derive the statement from Theorem 1.2 1)-2)).
2. Let p be a prime. Prove that any nonzero residue mod p is invertible.
3. Let $n > 1$ be a positive integer. Suppose that all the binomial coefficients $\binom{n}{i}$, first and last excluded, are divisible by n. Prove that n is prime.
4. Let Ω be a field, $\zeta \in \Omega$, $\zeta^4 + 1 = 0$, $\tau = \zeta + \zeta^{-1}$. Prove that $\tau^2 = 2$ (where $2 \stackrel{\mathrm{def}}{=} 1 + 1$).
5. For ζ as in Problem 5 prove that $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ if $p \equiv 1$ or $p \equiv 7 \bmod 8$ and $\zeta^p + \zeta^{-p} = -\zeta - \zeta^{-1}$ if $p \equiv 3$ or $p \equiv 5 \bmod 8$.
6. Derive Theorem 1.11 from Lemma 1 and Lemma 2.