NUMBER THEORY

ISHAN LEVY

By the Chinese Remainder Theorem, $\mathbb{Z}/n\mathbb{Z}$ decomposes into its prime factors, so understanding the group $\mathbb{Z}/n\mathbb{Z}^\times$ amounts to understanding $\mathbb{Z}/p^n\mathbb{Z}^\times$ for p, n.

Theorem 0.1. *The multiplicative group of a finite field is cyclic.*

Proof. let q be the order of the field, and consider the polynomial $x^{q-1} - 1$. Every nonzero element is a root of the polynomial. Let $o(n)$ be the number of elements of order n. Then $\sum_{d|r} o(d) = r$ for $r|q-1$ as $x^r - 1$ divides $x^{q-1} - 1$ and so splits into linear factors. $\sum_{d|r} \phi(d) = r$ and so by Möbius inversion, $o(d) = \phi(d)$ and the group is cyclic. $\square$

Let's examine prime powers.

Theorem 0.2. *The multiplicative group of $\mathbb{Z}/p^n\mathbb{Z}$ is cyclic when p is an odd prime, and is $\mathbb{Z}/2^{n-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ when $p = 2$.*

Proof. Let K_r^m be the kernel of $\mathbb{Z}/p^m\mathbb{Z}^\times \to \mathbb{Z}/p^r\mathbb{Z}^\times$. Now since for $p > 2$, $(1+p)^{p^{n-1}} \equiv 1 + p^n \pmod{p)^{n+1}}$, $1+p$ generates K_1^n, and the maps $K_1^{n+1} \to K_1^n$ send the generator to the generator. Thus $\mathbb{Z}/p^m\mathbb{Z}^\times$ is an extension of $\mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}^\times$ by a cyclic group of order p^{n-1} so it must be cyclic (explicitly one can obtain a generator by Hensel lifting a solution of $x^{p-1} = a$, where a generates K_1^n).

For $p = 2$, I first claim that $a \in \mathbb{Z}/2^n\mathbb{Z}^\times, n \geq 3$ is a square mod 2^n iff it is 1 mod 8. Clearly this condition is necessary, and to see the converse, we can lift a root off the polynomial $x^2 - a$ from $\mathbb{Z}/2^n\mathbb{Z}$ to $\mathbb{Z}/2^{n+1}\mathbb{Z}$ for $n \geq 3$ by noticing that $(x + 2^{n-1}y)^2 \cong x^2 + 2^n y \pmod{2^{n+1}}$. Thus it suffices to show that K_3^m is cyclic. Now the argument from before works for $m \geq 2$, namely $(1 + 2^3)^{2^{m-3}} \equiv 1 + 2^m \pmod{2^{m+1}}$. $\square$

Lemma 0.3 (Euler's Criterion)**.** *Let p be an odd prime. Then the Legendre symbol $(\frac{a}{p})$ is given by $a^{\frac{p-1}{2}}$ mod p.*

Proof. This follows from Theorem 0.1. $\square$

Theorem 0.4. $(\frac{2}{p}) = \chi(p)$, *where χ is the character mod 8 whose kernel is ± 1.*

Proof. Consider the Gauss sum $\tau(a) = \sum_{x \in \mathbb{Z}/8\mathbb{Z}^\times} \chi(x)\omega^a x$ where ω is a primitive 8^{th} root of unity. Then one easily sees $\chi(a)\tau(a) = \tau(1)$. Moreover, for any prime p, one has $\tau(1)^p \equiv \tau(p) \equiv \chi(p)\tau(1)$ in some prime above p. But we compute that $\tau(1)^2 = 8$, so that by Euler's Criterion $(\frac{8}{p}) = \tau(1)^{p-1} = \chi(p)$. $\square$

Theorem 0.5 (Quadratic Reciprocity). *If p, q are odd primes, and $p^* = (\frac{-1}{p})p$, then $(\frac{p^*}{q}) = (\frac{q}{p})$.*

Proof. Let ω be a primitive p^{th} root of unity in $\overline{\mathbb{F}}_p$. Consider the Gauss sum $\tau(a) = \sum_{k \in \mathbb{Z}/p\mathbb{Z}^\times} (\frac{k}{p})\omega^{ak}$. Again, one has $(\frac{a}{p})\tau(a) = \tau(1)$. Modulo q, we have $\tau(1)^q \equiv \tau(q) \equiv (\frac{q}{p})\tau(1)$. This time however, one computes that $\tau(1)^2 = p^*$, so that by Euler's Criterion, $(\frac{p^*}{q}) = \tau(1)^{q-1} = (\frac{q}{p})$. $\square$

Lemma 0.6. *$a^2 + b^2 = -1$ always has a solution mod p.*

Proof. a^2 and $-b^2 - 1$ take on $\frac{p+1}{2}$ values, so two must coincide. $\square$

Theorem 0.7. *Every integer is the sum of 4 squares.*

Proof. Consider the ring $\mathbb{H}_\mathbb{Z} = \mathbb{Z}[i, j, k, \frac{1+i+j+k}{2}]$ in the quaternions. It has an anti-involution, called conjugation, so if two numbers are sums of 4 squares, so are their products. Thus we only need to show primes are sums of 4 squares. To do this, note that this ring is Euclidean, and so every left ideal is principle. If $p \in \mathbb{Z}$ is a prime, the proof that $p|\bar{b}b \implies p|b$ or $p|b$ for Euclidean domains goes through. Now by the lemma, $p|a^2 + b^2 + 1$, so $p|(a + bi + j)(a - bi - j)$ and if p is prime, then $p|(a \pm bi \pm j)$, a contradiction. Thus something has norm p, and so either $p = x^2 + y^2 + z^2 + w^2$ or $4p = x^2 + y^2 + z^2 + w^2$ with x, y, z, w odd. But the latter cannot happen by looking mod 8.

Here is an alternative proof. By the lemma, we have $N(a + bi) + 1 \equiv 0 \pmod p$, and so we would like to search for solutions by noticing that $N((a + bi)(c + di)) + N(cj + dk) = 0 \pmod p$. But we would like to have control on the 1 and i coefficients mod p, so we can add $pe + pfi$, and look for (c, d, e, f) that satisfy make the left hand side equal to p. We can look at the lattice of (c, d, e, f), and note that it is given by the matrix $\begin{pmatrix} p & 0 & d & c \\ 0 & p & c & -d \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Thus the volume is p^2. We can notice that the open ball of radius $\sqrt{2p}$ has volume $2\pi^2 p^2 > 16p^2$ so there is a nonzero element of norm $< 2p$, which must have norm p. $\square$

Theorem 0.8. *Let k be a finite field of size q and characteristic p, and let f_i be polynomials in n variables so that the sum of their degrees is less than $n(q-1)$. Then their size of their common zeroes is congruent to 0 mod p.*

Proof. The characteristic function for the common zeroes is $\prod(1 - f_i^{q-1})$, so we need to compute the sum of this function over k^n. To do this, note that the sum of x^d over the finite field is equal to $-\delta_{d|q-1}$ for $d > 0$, so that since every term in the product has some power that is less than $q - 1$, the sum is 0. $\square$

1. Discriminants

Let R^n be a free R-module, and let f be a bilinear form $R^n \otimes R^n \to R$. f is adjoint to a map $R^n \to (R^n)^*$, which we can take the n^{th} wedge power of to get a map adjoint to a map $R \otimes R \to R$, where $\bigwedge^n(R^n)$ has been identified with R. by choosing any generator $a \in R$ and looking at the image of $a \otimes a$, we get a well defined element of $R/(R^\times)^2$ called the **discriminant** of f. If the original module is not free, but still has rank n, we can still get a **discriminant ideal** by taking the ideal generated by the discriminants of all free submodules of rank n. We can apply this in the case of an extension of number fields L/K to the rings of integers, where f is a bilinear map $a, b \mapsto \mathrm{tr}(ab)$. If $\mathcal{O}_L$ is a free $\mathcal{O}_K$ module (which is the case if $\mathcal{O}_K$ is a PID for example), then the discriminant is a well defined element of $\mathcal{O}_K/(\mathcal{O}_K^\times)^2$. Otherwise, there is only a well-defined discriminant ideal. Note the definition also makes sens in orders and localizations of the ring of integers.

If $a_1, \ldots, a_n$ are a basis of $\mathcal{O}_L$, the discriminant can be described as $\det(\mathrm{tr}(a_i a_j))$. If the extension is Galois, then note that this is equal to $\det(g_i(a_j))^2$, where g_i is some numbering of elements of the Galois group. This is because if you multiply $(g_i(a_j))$ and its transpose, you get $(\mathrm{tr}(a_i a_j))$.

Theorem 1.1. *A prime $\mathfrak{p} \in \mathrm{Spec}(O_K)$ ramifies in $\mathrm{Spec}(\mathcal{O}_L)$ iff $\mathfrak{p}$ divides the discriminant of $\mathcal{O}_L/\mathcal{O}_K$.*

Proof. First, note we can localize at $\mathfrak{p}$ so that everything is a PID, and so that the extension of rings is simple, generated by some α of degree n. Now, we can take $\alpha^i, i < n$ to be our basis, and let α_j be the Galois conjugates of α. The argument for Galois extensions shows that the discriminant is given by $\det((\alpha_i^j)^2)$. This is a Vandermonde matrix, and so it vanishes mod $\mathfrak{p}$ iff two of the α_i are equal mod $\mathfrak{p}$ iff $\mathfrak{p}$ ramifies. $\square$