p-adic integers and prime groups

As an arithmetic analogue of the tubular neighborhood, last time we defined the ring of p-adic integers to be the inverse limit $\varprojlim_n \mathbb{Z}/(p^n)$. Here is a concrete way to understand the p-adic integers.

Example 1. Instead of arranging the integers on a line in the usual order, let us classify them by their residues modulo $p, p^2, \ldots, p^n, \ldots$. We think that two integers x, y are closer if $x - y$ is more divisible by p. Because a p-adic integer is a sequence (a_n) where $a_{n+1} - a_n$ is divisible by p^n, the a_n's are getting closer and closer when n gets bigger and thus has a "limit" under this p-adic sense of distance. The p-adic integer ring $\mathbb{Z}_p$ simply consists of all these limits and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. In sum, a p-adic integer is a limit of integers under the p-adic distance.

To make more precise meaning of the p-adic distance, we shall discuss some basic algebraic properties of $\mathbb{Z}_p$. The following will not surprise you if you are familiar with the power series ring $\mathbb{C}[[t]]$.

Theorem 1. A nonzero element $x \in \mathbb{Z}_p$ can be uniquely written as $x = u \cdot p^k$, where $u \in \mathbb{Z}_p^\times$ is a unit and $k \geq 0$ is an integer.

Proof. Write $x = (x_n)$ and k be the largest power of p dividing x (equivalently, $x_k = 0$ but $x_{k+1} \neq 0$). Then we can find a unique element $u = (u_n) \in \mathbb{Z}_p$ such that $x = p^k u$. Moreover, $p \nmid u_n$, so $u_n \in \mathbb{Z}/(p^n)$ is a unit. □

So the arithmetic in $\mathbb{Z}_p$ is much easier than that in $\mathbb{Z}$. In particular,

Corollary 1. $\mathbb{Z}_p$ is a UFD and all its nonzero ideals are of the form (p^k). (0) and (p) are the only two prime ideals.

Exercise. The natural map $\mathbb{Z}_p \to \mathbb{Z}/(p^k)$ induces an isomorphism $\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}$.

The ring of p-adic integers $\mathbb{Z}_p$ is like a local version of $\mathbb{Z}$ obtained via throwing away all primes other than p. The usage of p-adic numbers is ubiquitous in modern number theory, reflecting the importance of the local-global point of view. $\mathbb{Z}_p$ has many similar properties as $\mathbb{Z}$ (integrally closed, prime decomposition, Krull dimension 1, ...), but it is much simpler than $\mathbb{Z}$ (local, complete, discrete valuation, ...). It allows us study arithmetic problems by studying one prime at a time and then tying the local information thus obtained together.

The following Hensel's lemma is the crucial property of $\mathbb{Z}_p$ as a result of the completion process.

Theorem 2 (Hensel's Lemma)**.** Let $f(x) \in \mathbb{Z}[x]$ and $\bar{a} \in \mathbb{F}_p$ be a simple root of the reduction $\bar{f}(x) = f(x) \bmod p \in \mathbb{F}_p[x]$. Then $\bar{a}$ lifts to a root $a \in \mathbb{Z}_p$ of $f(x)$.

Sketch of the proof. The key idea is to produce the solutions modulo p^k inductively from $\bar{a}$. Then taking the limit of these solutions gives a solution in $\mathbb{Z}_p$. □

Corollary 2. $\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$.

Proof. Consider the quotient map: $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times, \quad a \mapsto a \bmod p$. Clearly it is surjective and has kernel $1 + p\mathbb{Z}_p$. So it suffices to show the exact sequence

$$1 \to 1 + p\mathbb{Z}_p \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \to 1$$

splits, which follows from Hensel's lemma since we can lift each solution of $x^{p-1} = 1$ in $\mathbb{F}_p$ to a solution in $\mathbb{Z}_p$. □

Remark. The proof shows that all $(p-1)$th roots of unity exist in $\mathbb{Z}_p^\times$.

Now let us turn back to the analogy between knot groups and prime groups, the linking number and the Legendre symbol. Recall that we can interpret the linking number using covering spaces. Let $L \cup K$ be a link and X_2 be the double covering of the knot complement X_L corresponding to the map $\rho_2 : G_L \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Then $\rho_2([K]) = \mathrm{lk}(L, K) \bmod 2$.

Let p and q be two odd primes. Let us first work out the arithmetic analogue $\rho_2 : G_{\{q\}} \to \mathbb{Z}/2\mathbb{Z}$. Class field theory classifies all number fields with abelian Galois groups. The following can be derived easily using class field theory.

Theorem 3. The maximal abelian extension of $\mathbb{Q}$ unramified outside p is $\mathbb{Q}(\zeta_{p^\infty}) = \cup_n \mathbb{Q}(\zeta_{p^n})$.

In the exercise last time we have known that $\mathbb{Q}(\zeta_{p^\infty})$ does satisfies the unramified outside p condition and class field theory furthermore ensures that it is the maximal one. It follows that

$$G_{\{q\}}^{\mathrm{ab}} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty}/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/(p^n))^\times = \mathbb{Z}_p^\times.$$

Using the structure of $\mathbb{Z}_p^\times$, we construct the natural quotient map

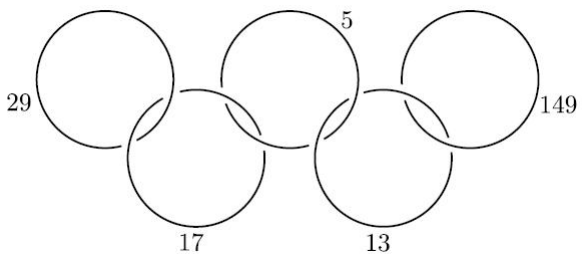
$$\rho_2 : G_{\{q\}} \to G_{\{q\}}^{\mathrm{ab}} \to \mathbb{F}_q^\times \to \mathbb{Z}/2\mathbb{Z}.$$

ρ_2 should corresponds to a quadratic extension of $\mathbb{Q}$ unramified outside q. What is it? Let us assume for simplicity that q is congruent to 1 modulo 4. Then the natural option $K = \mathbb{Q}(\sqrt{q})$ is in fact a quadratic extension unramified outside q. In fact, its number ring is $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{q}}{2}]$ with discriminant $d_K = q$. Now we can similarly define the **mod 2 linking number** to be $\mathrm{lk}_2(q, p) := \rho_2(\sigma_p)$, where $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$ is the Frobenius automorphism associated to p.

Theorem 4. $(-1)^{\mathrm{lk}_2(q,p)} = \left(\frac{q}{p}\right)$.

Proof. Notice that $\mathrm{lk}_2(q, p) = 0$ is equivalent to $\rho_2(\sigma_p) = \mathrm{Id}$, or $\sigma_p(\sqrt{q}) = \sqrt{q}$. By the definition of the Frobenius automorphism, this is equivalent to $\sqrt{q} \in \mathbb{F}_p^\times$, or $q \in (\mathbb{F}_p^\times)^2$, which happens exactly when $\left(\frac{q}{p}\right) = 1$. □

So the Legendre symbol tells us how primes are "linked" together. This extra strucutre shows the advantage of viewing primes as knots in a 3-dimensional space rather than plain points on the line. Here is a picture of five primes "linked" as the Olympic rings.



We summarize the analogy obtained as follows.

G_L	$G_{\{q\}}$
$G_L^{\mathrm{ab}} \cong \mathbb{Z}$	$G_{\{q\}}^{\mathrm{ab}} \cong \mathbb{Z}_q^\times \cong \mathbb{F}_q^\times \times (1+q\mathbb{Z}_p)$
$\rho_2 : G_L \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$	$\rho_2 : G_{\{q\}} \to \mathbb{F}_q^\times \to \mathbb{Z}/2\mathbb{Z}$
$\rho_2([K]) = \mathrm{lk}_2(L,K)$	$\rho_2(\sigma_p) = \mathrm{lk}_2(q,p)$
$\mathrm{lk}(L,K) = \mathrm{lk}(K,L)$	$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$
$h_2^{-1}(K) = \begin{cases} K_1 \cup K_2, & \mathrm{lk}_2(L,K) = 0, \\ \mathfrak{K}, & \mathrm{lk}_2(L,K) = 1 \end{cases}$	$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2, & \left(\frac{q}{p}\right) = 1 \\ \mathfrak{p}, & \left(\frac{q}{p}\right) = -1 \end{cases}$

We finally tie up the beautiful story of the seemingly unrelated linking number and the Legendre symbol. And it takes only three weeks. This is so amazing, isn't it? Next time we will start a new story line: the analogy between Alexander polynomials and Iwasawa theory.