The Infinitude of Primes

Plan

1. Three proofs (Classical, Analytic, Topological)
2. p-adic numbers and $\hat{\mathbb{Z}}$.
3. The topological proof, recast.
4. Relation between topological and analytic proofs. (If I have time.)

§1 Three proofs.

Theorem There are infinitely many primes.

Remark The following proofs assume that every integer >1 factors (uniquely) into primes

proof 1 (Euclid). Assume there are only finitely many, say $p_1, \dots, p_r$. Consider

$$N = p_1 p_2 \cdots p_r + 1.$$

Then $N > 1$ and $p_i \nmid N$ for all $i = 1, \dots, r$. So N doesn't factor, contradiction. □.

proof 2 (Euler). Consider the series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s \in \mathbb{R}_{>0}$$

Then by unique factorization,

$$\zeta(s) = \prod_{p\text{-prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right)$$

$$= \prod_{p\text{-prime}} \frac{1}{1 - \frac{1}{p^s}} \qquad \text{(geometric series)}$$

wherever this product converges. If there are only finitely many primes, then it converges for $s = 1$. So done by:

Lemma The series

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n}$$

diverges.

proof

$$1 + \underbrace{\frac{1}{2}}_{\geq \frac{1}{2}} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{\geq \frac{1}{2}} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\geq \frac{1}{2}} + \cdots \geq \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots \longrightarrow \infty. \qquad \square.$$

proof 3 (Forstenberg) Put a topology on $\mathbb{Z}$ where the opens are unions of sets of the form

$$\{an+b \mid n\in\mathbb{Z}\}, \quad 0\neq a\in\mathbb{Z}, \ b\in\mathbb{Z}.$$

Note: (1) The intersection of any two of these sets is again of this form, so this is a topology.
(2) Any nonempty open is infinite.

Now assume there are only finitely many primes, say $p_1,\dots,p_r$. Then

$$S=\bigcap_{i=1}^{r}\left(\bigcup_{a=1}^{p_i-1}\{p_i n+a \mid n\in\mathbb{Z}\}\right)$$

is open; it is an intersection of finitely many opens. An element $N\in S$ is divisible by no prime, so

$$S=\{\pm 1\}.$$

This is a contradiction by (2) $\square$

Remark This is essentially Euclid's proof, rephrased using topology.

§2 p-adic numbers and $\hat{\mathbb{Z}}$.

Recall If $p>1$ is an integer (not necessarily prime), then every $0\leq N\in\mathbb{Z}$ can be written uniquely as

$$N=\sum_{i=0}^{n} a_i p^i, \quad a_i\in\{0,1,\dots,p-1\}, \text{ some } n$$

This is just the base-p expansion of N. $+,\times$ are given by carrying.

Def Now let p be prime. Define the ring of p-adic integers by

$$\mathbb{Z}_p=\left\{\sum_{i=0}^{\infty} a_i p^i \,\middle|\, a_i\in\{0,1,\dots,p-1\}\right\},$$

where $+,\times$ are given by carrying, possibly infinitely many times.

Remark $-1\in\mathbb{Z}_p$ because

$$\begin{aligned}
1+\sum_{i=0}^{\infty}(p-1)p^i &= 1+\left[(p-1)+(p-1)p+(p-1)p^2+\cdots\right]\\
&= \quad p+(p-1)p+(p-1)p^2+\cdots\\
&= \quad\quad p^2+(p-1)p^2+\cdots\\
&= \quad\quad\quad p^3+\cdots\\
&\ \ \vdots\\
&= 0.
\end{aligned}$$

Remark $\mathbb{Z}_p\twoheadrightarrow\mathbb{Z}/p^n\mathbb{Z}$ for any n. The map is $\sum_{i=0}^{\infty} a_i p^i \longmapsto \sum_{i=0}^{n-1} a_i p^i \pmod{p^n}$, with kernel $p^n\mathbb{Z}_p$. In fact,

$$\mathbb{Z}_p\cong\varprojlim_{n\geq 1}\mathbb{Z}/p^n\mathbb{Z}=\left\{(b_1,b_2,b_3,\dots)\in\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p^2\mathbb{Z}\times\mathbb{Z}/p^3\mathbb{Z}\times\cdots \,\middle|\, b_n\equiv b_{n-1}\pmod{p^{n-1}}\ \forall n\right\}.$$

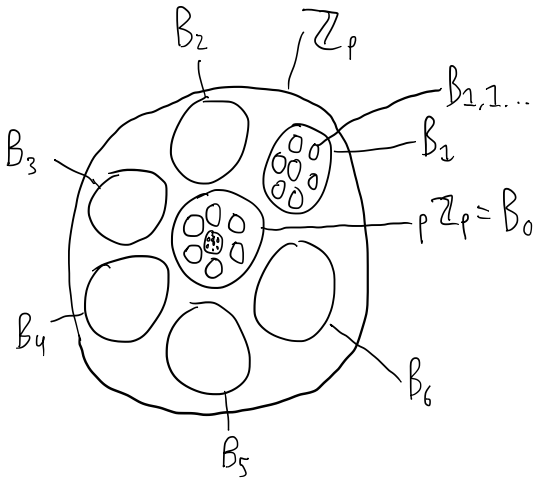
Put a topology on $\mathbb{Z}_p$ by declaring

$$B_{\alpha_0,\dots,\alpha_{n-1}} = \sum_{i=0}^{n-1} \alpha_i p^i + p^n \mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \;\middle|\; a_0 = \alpha_0,\ a_1 = \alpha_1,\ \dots,\ a_{n-1} = \alpha_{n-1} \right\} \quad (n \text{ not fixed.})$$

to be open. (This is Hausdorff, even metric, but that doesn't matter for this talk.)

Picture

$p = 7$



Remark $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ as rings, because, if $N \geq 0$, $N = \sum_{i=0}^{\infty} a_i p^i$ in base p, then N defines a p-adic integer with the same expansion. If $N < 0$, then $-N > 0$, and we know how to interpret $-N$ and -1 as p-adic integers, hence also $N = (-1)(-N)$.

Remark $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. In fact, every basic open $B_{\alpha_0,\dots,\alpha_{n-1}}$ contains an integer, namely $\sum_{i=0}^{n-1} \alpha_i p^i$.

Remark $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p$. (The outer ring in the picture.) $\mathbb{Z}_p^\times = \bigcup_{\alpha=1}^{p-1} B_\alpha$ is open.

Def Let $\hat{\mathbb{Z}}$ be the ring

$$\hat{\mathbb{Z}} = \varprojlim_{N \in \mathbb{Z}_{>0}} \mathbb{Z}/N\mathbb{Z} = \left\{ (b_1, b_2, b_3, \dots) \in \mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \cdots \;\middle|\; b_n \equiv b_m \pmod{m} \text{ if } m \mid n \right\}$$

"compatible sequences."

Remark The Chinese remainder theorem implies that if $N = p_1^{n_1} \cdots p_r^{n_r}$, then

$$\mathbb{Z}/N\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/p_i^{n_i}\mathbb{Z}$$

as rings. This can be upgraded to

$$\hat{\mathbb{Z}} \cong \prod_{\text{all } p} \left(\varprojlim_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z} \right) = \prod_{\text{all } p} \mathbb{Z}_p,$$

as rings. In particular, $\hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$.

Now define a topology on $\hat{\mathbb{Z}}$ by declaring

$$B_{N,a} = \left\{ (b_1, b_2, b_3, \dots) \in \hat{\mathbb{Z}} \;\middle|\; b_N = a \right\} \quad (\text{here } N \geq 1,\ a \in \mathbb{Z}/N\mathbb{Z})$$

to be open for any N and a.

Remark The iso

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$$

is a homeo. Recall that the product topology on $\prod_{i\in I} X_i$ is s.t. the basic opens are

$$\prod_{i\in S} U_i \times \prod_{i\notin S} X_i, \text{ for } \underline{\text{finite}} \text{ subsets } S\subseteq I.$$

We give $\prod_p \mathbb{Z}_p$ this product topology.

Remark $\mathbb{Z}\hookrightarrow\hat{\mathbb{Z}}$ as rings, $a\mapsto(a \bmod 1, a \bmod 2, a \bmod 3,\dots)$, and $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$.

§3 Topological proof, recast.

proof 3' Assume there are only finitely many primes. Since $\mathbb{Z}_p^\times$ is open in $\mathbb{Z}_p$,

$$\hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times \text{ is open in } \prod_p \mathbb{Z}_p = \hat{\mathbb{Z}} \quad (\text{This is } \underline{\text{false}} \text{ if there are infinitely many } p!)$$

Now $\hat{\mathbb{Z}}^\times = \{(b_1, b_2, b_3,\dots)\in\hat{\mathbb{Z}} \mid \underbrace{b_N \in (\mathbb{Z}/N\mathbb{Z})^\times}_{\Leftrightarrow (b_N, N)=1} \ \forall N>0\}$. Therefore $\hat{\mathbb{Z}}^\times\cap\mathbb{Z} = \{b\in\mathbb{Z} \mid (b,N)=1 \ \forall N>0\} = \{\pm 1\}$.

But $\mathbb{Z}$ is an infinite dense subset of $\hat{\mathbb{Z}}$, so its intersection with any nonempty open is infinite. Contradiction!

Remark Why is this a recasting of proof 3? Well, consider the topology $\mathbb{Z}$ gets as a subspace of $\hat{\mathbb{Z}}$. The basic opens are

$$B_{N,a}\cap\mathbb{Z} = \{b\in\mathbb{Z} \mid b\equiv a \pmod N\} = \text{arithmetic progression.}$$

So this is Furstenberg's topology, and $\hat{\mathbb{Z}}^\times\cap\mathbb{Z}$ = the intersection of opens in $\mathbb{Z}$ from Furstenberg's proof.

§4 Relation to Euler's proof.

Fact One can define a measure μ_p on $\mathbb{Z}_p$ so that

$$\mu_p(B_{a_0,\dots,a_{n-1}}) = p^{-n}.$$

Similarly one can define μ on $\hat{\mathbb{Z}}$ s.t.

$$\mu(B_{N,a}) = \frac{1}{N}.$$

Then $\mu_p(\mathbb{Z}_p)=1$, $\mu(\hat{\mathbb{Z}})=1$, and

$$\mu = \prod_p \mu_p.$$

Then we compute:

$$\begin{aligned}
\mu(\hat{\mathbb{Z}}^\times) &= \prod_p \mu_p(\mathbb{Z}_p^\times) \\
&= \prod_p \mu_p(\mathbb{Z}_p \setminus p\mathbb{Z}_p) \\
&= \prod_p \left(\mu_p(\mathbb{Z}_p) - \mu_p(p\mathbb{Z}_p)\right) \\
&= \prod_p \left(1 - \tfrac{1}{p}\right) \\
&= \left[\prod_p \frac{1}{1-\frac{1}{p}}\right]^{-1} \\
&= \zeta(1)^{-1}.
\end{aligned}$$

Euler's proof tells us $\zeta(1)^{-1} = 0$. But if $\hat{\mathbb{Z}}^\times$ were open, it would have measure > 0. So Euler's argument can be used to give us the desired contradiction in $\hat{\mathbb{Z}}$ as well.