Continuing the review of the simple (!?) case of number theory over $\mathbb{Z}$:

So far, we have sketched the connection between *prime numbers*, and *zeros of the zeta function*, given by Riemann's formula

$$\sum_{p^m < X} \log p \;=\; X \;-\; (b+1) \;-\; \lim_{T\to\infty} \sum_{|\mathrm{Im}\,(\rho)|<T} \frac{X^\rho}{\rho} \;+\; \sum_{n\geq 1} \frac{X^{-2n}}{2n}$$

with *finite* LHS, and *infinite* RHS... and noted that ideas from complex variables and Fourier analysis are needed to make this legitimate. A similar discussion applies to many other zeta functions and L-functions, such as those used by Dirichlet to prove the primes-in-arithmetic progressions theorem.

A different example (though connected to zeta functions and L-functions at a deeper level!) is Gauss' *Quadratic Reciprocity.*

Fermat's two-squares theorem: a prime number p is expressible as $p = a^2 + b^2$ if and only if $p = 1 \bmod 4$ (or $p = 2$):

Yes, one direction is easy: the squares mod 4 are $0, 1$. The ring of Gaussian integers $\mathbb{Z}[i]$ is *Euclidean*, so is a PID. The Galois norm N from $\mathbb{Q}(i)$ to $\mathbb{Q}$ is $N(a + bi) = a^2 + b^2$.

A prime is expressible as $p = (a + bi)(a - bi)$, if and only if it is *not* prime in $\mathbb{Z}[i]$, if and only if $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is *not* an integral domain. Compute

$$\mathbb{Z}[i]/p \approx \big(\mathbb{Z}[x]/\langle x^2 + 1\rangle\big)/p \approx \big(\mathbb{Z}[x]/p\big)/\langle x^2 + 1\rangle \approx \mathbb{F}_p[x]/\langle x^2 + 1\rangle$$

The latter *is not* an integral domain if and only if there is a fourth root of unity $\sqrt{-1}$ in $\mathbb{F}_p$. Since $\mathbb{F}_p^\times$ is *cyclic*, presence of $\sqrt{-1}$ is equivalent to $p = 1 \bmod 4$ (or $p = 2$. ///

$\mathbb{Z}[\sqrt{2}]$ is Euclidean, and the same argument shows

$$p \;=\; a^2 - 2b^2 \qquad \Longleftrightarrow \qquad 2 \text{ is a square mod } p$$

When is 2 a square mod p? (for $p > 2$)

A main feature of finite fields is the cyclic-ness of multiplicative groups, from which arises *Euler's criterion*

$$b \in \mathbb{F}_p^\times \text{ is a square} \qquad \Longleftrightarrow \qquad b^{\frac{p-1}{2}} = 1 \bmod p$$

Also, there is a handy connection between roots of unity and 2:

$$(1+i)^2 \;=\; 2i \qquad \Longrightarrow \qquad 2 \;=\; -i(1+i)^2$$

Computing in the ring $\mathbb{Z}[i]/p$ (!), using $\binom{p}{j} = 0$ for $0 < j < p$,

$$2^{\frac{p-1}{2}} \;=\; \Big(-i(1+i)^2\Big)^{\frac{p-1}{2}} \;=\; (-i)^{\frac{p-1}{2}} \frac{(1+i)^p}{1+i} \;=\; (-i)^{\frac{p-1}{2}} \frac{1+i^p}{1+i}$$

Quasi-astonishingly, this depends only on p mod 8, and

$$2 \text{ is a square mod } p \qquad \Longleftrightarrow \qquad p = \pm 1 \bmod 8$$

When is q a square mod p, for odd primes $p \neq q$?

Amazingly, the answer depends only on p mod $4q$.

The *quadratic symbol* is

$$\left(\frac{b}{p}\right)_2 = \begin{cases} 0 & \text{for } b = 0 \bmod p \\ 1 & \text{for } b \text{ nonzero square mod } p \\ -1 & \text{for } b \text{ nonzero non-square mod } p \end{cases}$$

Gauss' Law of Quadratic Reciprocity is

$$\left(\frac{q}{p}\right)_2 \cdot \left(\frac{p}{q}\right)_2 = (-1)^{\frac{(p-1)(q-1)}{4}}$$

This is arguably the historically-first non-trivial theorem in number theory.

Again, the cyclicness of $\mathbb{F}_p^\times$ shows that *exactly half* the non-zero things mod p are squares, and Euler's criterion

$$b \in \mathbb{F}_p^\times \text{ is a square} \quad \Longleftrightarrow \quad b^{\frac{p-1}{2}} = 1 \bmod p$$

also shows that $b \to \left(\frac{b}{p}\right)_2$ is a *group homomorphism* $\mathbb{F}_p^\times \to \{\pm 1\}$. For brevity, write $\chi(b) = \left(\frac{b}{q}\right)_2$.

The surprise is that *every* prime q is expressible, *systematically* in terms of roots of unity. Fix a group homomorphism $\psi(b) = e^{2\pi i b/q}$ on the *additive* group of $\mathbb{F}_q$. The quadratic *Gauss sum* mod q is

$$g(\chi) \;=\; \sum_{b \bmod q} \chi(b) \cdot \psi(b)$$

Obviously, this is a weighted average of q^{th} roots of unity, with weights ± 1 (or 0). Such Gauss sums with more general *characters* χ on $\mathbb{F}_p^\times$ are useful, too, but we just want the quadratic character for now.

The Galois group of $\mathbb{Q}(e^{2\pi i/q})$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/q^\times$, and $\ell \in \mathbb{Z}/q^\times$ acts on q^{th} roots of unity by $\sigma_\ell : e^{2\pi i/q} \to e^{2\pi i\ell/q}$. Certainly the quadratic Gauss sum

$$g(\chi) \;=\; \sum_{b \bmod q} \chi(b) \cdot \psi(b)$$

lies in $\mathbb{Q}(e^{2\pi i/q})$. By a change of variables (replacing b by $\ell^{-1}b$),

$$\sigma_\ell\, g(\chi) \;=\; \sum_{b \bmod q} \chi(b) \cdot \psi(\ell b) \;=\; \sum_{b \bmod q} \chi(\ell^{-1}b) \cdot \psi(b)$$

$$=\; \chi(\ell) \cdot \sum_{b \bmod q} \chi(b) \cdot \psi(b) \;=\; \chi(\ell) \cdot g(\chi)$$

With hindsight, since χ is multiplicative, this *equivariance* is really *designed into* the Gauss sum.

Then $\sigma_\ell\,(g(\chi)^2) \;=\; \chi(\ell)^2 \cdot g(\chi)^2 \;=\; g(\chi)^2$, so by Galois theory $g(\chi)^2 \in \mathbb{Q}$!?!?

Claim: $g(\chi)^2 = q \cdot (-1)^{q-1}$

Compute directly, keeping track of the trick that $\chi(0) = 0$:

$$g(\chi)^2 \;=\; \sum_{a\neq 0, b\neq 0} \chi(a)\,\chi(b)\,\psi(a+b) \;=\; \sum_{a\neq 0, b\neq 0} \chi(ab)\,\chi(b)\,\psi(ab+b)$$

$$= \sum_{a\neq 0, b\neq 0} \chi(a)\,\psi((a{+}1)b) \;=\; \sum_{a\neq 0, -1,\; b\neq 0} \chi(a)\,\psi((a{+}1)b) + \chi(-1)\sum_{b\neq 0} 1$$

To simplify all this, use the *Cancellation Lemma:* for $\alpha : H \to \mathbb{C}^\times$ a group homorphism from a finite group H to $\mathbb{C}^\times$,

$$\sum_{h\in H} \alpha(h) \;=\; \begin{cases} |H| & \text{for } \alpha \text{ identically } 1 \\ 0 & \text{for } \alpha \text{ \textit{not} identically } 1 \end{cases}$$

Proven by change-of-variables: for α not trivial, let $\alpha(h_o) \neq 1$, and

$$\sum_{h\in H} \alpha(h) \;=\; \sum_{h\in H} \alpha(hh_o) \;=\; \alpha(h_o) \sum_{h\in H} \alpha(h)$$

So $(1 - \alpha(h_o)) \sum_{h\in H} \alpha(h) = 0$. ///

Thus, since $b \to \psi(c \cdot b)$ is a group hom $\mathbb{F}_q$ to $\mathbb{C}^\times$, non-trivial for $c \in \mathbb{F}_q^\times$, for $a+1 \neq 0$, we can evaluate inner sums over b:

$$\sum_{b\neq 0} \psi((a+1)b) \;=\; \sum_{\text{all } b} \psi((a+1)b) - \psi((a+1)0) \;=\; 0-1 \;=\; -1$$

Thus,

$$\sum_{a\neq 0,-1,\; b\neq 0} \chi(a)\,\psi((a+1)b) \quad+\quad \chi(-1)\sum_{b\neq 0} 1$$

$$=\; \sum_{a\neq 0,-1} \chi(a)\cdot(-1) \quad+\quad \chi(-1)\cdot(q-1)$$

$$=\; -\sum_{a\neq 0} \chi(a) + \chi(-1) + \chi(-1)\cdot(q-1) \;=\; 0 + \chi(-1)q \;=\; \chi(-1)q$$

That is, $g(\chi)^2 = \chi(-1)q$. ///

Using $g(\chi)^2 \;=\; \chi(-1)q$ and plugging into Euler's criterion: computing mod p in $\mathbb{Z}[e^{2\pi i/q}]$, noting that apparently q and $g(\chi)$ are invertible there (!),

$$\binom{q}{p}_2 \;=\; q^{\frac{p-1}{2}} \;=\; \left((-1)^{\frac{q-1}{2}} \cdot g(\chi)^2\right)^{\frac{p-1}{2}} \;=\; (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \frac{g(\chi)^p}{g(\chi)}$$

Again using $\binom{p}{j} = 0 \bmod p$ for $0 < j < p$,

$$g(\chi)^p \;=\; \sum_{b \bmod q} \chi(b)^p \cdot \psi(p \cdot b) \;=\; \sum_{b \bmod q} \chi(b) \cdot \psi(p \cdot b)$$

$$=\; \sum_{b \bmod q} \chi(bp^{-1}) \cdot \psi(b) \;=\; \binom{p}{q}_2 \cdot g(\chi) \bmod p$$

Thus, in $\mathbb{Z}[e^{2\pi i/q}]$ mod p,

$$\binom{q}{p}_2 \;=\; (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \frac{g(\chi)^p}{g(\chi)}$$

$$=\; (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \frac{\binom{p}{q}_2 \cdot g(\chi)}{g(\chi)} \;=\; (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \binom{p}{q}_2$$

Since these values are ± 1, their equality in $\mathbb{Z}[e^{2\pi i/q}]$ mod p for $p > 2$ gives their equality as numbers in $\{\pm 1\}$. ///