Quick context!

Recall A prime $p > 2$ is regular if $p \nmid h_p$

$$h_p = |Cl(\mathbb{Q}(\zeta_p))|.$$

Fact: If p is regular, then

$x^p + y^p = z^p$ has no nontrivial integer solutions.

Theorem: p is regular if and only if

Borevich & Šafarevič

p does not divide the numerator of

B_k for $k = 2, 4, 6, \ldots, p-3$.

Example: 691 is not regular, because $\boxed{691} \mid B_{\boxed{12}}$.

What is the significance of 12?

$$Cl(\mathbb{Q}(\zeta_{691}))[691] \neq 0$$

Vector space over $\mathbb{F}_{691}$.

with an action of

$(\mathbb{Z}/691\mathbb{Z})^\times \simeq$ Galois group

Can decompose into characters of this group

Character space for $z \mapsto z^{11}$

is nonzero.

<u>Remark</u> Go much further $\rightsquigarrow$ Iwasawa main conjecture (Mazur & Wiles)
p-adic zeta function that exactly measures
p-part of class groups of cyclotomic extensions.

Ribet's converse to Herbrandt (next week).

This week: Introduction to modular forms + application to sums of squares.

(A good reference is Serre's Course in Arithmetic, Ch VII).