tags: number-theory

def: Euler ϕ-function

$$\phi(n) = \left|(\mathbb{Z}/n)^\times\right|$$

express $n \in \mathbb{N}$ in terms of Euler's ϕ-function

$$n = \sum_{d|n} \phi(d)$$

(Each element of $\mathbb{Z}/n$ is a generator of one of the subgroups $\mathbb{Z}/d$ with $d|n$.)

Refs: Serre: A course in arithmetic, § I.1, Lemma 1

Chevalley-Warning-Theorem

Let $\mathbb{F}_q$ be a finite field (q a power of p).
The common vanishing locus of polynomials $f_\alpha \in \mathbb{F}_q[x_1, \ldots, x_n]$ of sufficiently small degree has cardinality a multiple of p. Sufficiently small means that $\sum_\alpha \deg(f_\alpha) < n$.

Refs: Serre: A course in arithmetic, § I.2, Theorem 3

prove: Every conic over a finite field has a rational point.

A conic in $\mathbb{P}^n_{\mathbb{F}_q}$ is defined by a quadratic form f in n variables ($n \geq 3$). As $\deg(f) = 2 < n$, the Chevalley-Warning-Theorem implies that f has more zeroes than just the trivial zero.

Refs: Serre: A course in arithmetic, § I.2, Corollary 2

squares in $\mathbb{F}_q$ (q a power of p)

If $p \neq 2$,

$$\begin{array}{c} 1 \to (\mathbb{F}_q^\times)^2 \to \mathbb{F}_q^\times \to \{\pm 1\} \to 1 \\ x \mapsto x^{\frac{q-1}{2}} \end{array}$$

If $p = 2$, all elements of $\mathbb{F}_q$ are squares.

Refs: Serre: A course in arithmetic, § I.3, Theorem 4

.

tags: philosophy

```
What good is it to argue about whether HOLISM or REDUCTIONISM
is right?
```

```
The proper way to understand the matter is to transcend the question,
by answering MU.
```