Welcome back to the online version of MTH 505!

Recap:

Linear Diophantine Equations

$$ax + by = c.$$

Euclidean Algorithm.

Modular Arithmetic $\mathbb{Z}/n\mathbb{Z}$

$a \in \mathbb{Z}/n\mathbb{Z}$ is invertible $\Leftrightarrow$ $\gcd(a,n) = 1$.

The group of units $(\mathbb{Z}/n\mathbb{Z})^\times$ has size $\phi(n) = \#\{0 \leq a < n : \gcd(a,n) = 1\}$

Euler's Totient Theorem:

$\forall\, a \in \mathbb{Z}$, $\gcd(a,n) = 1$, $a^{\phi(n)} \equiv 1 \bmod n$.

Special Case (Fermat's Little Theorem):

p prime, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \bmod p$.

Application: RSA Cryptosystem.

For $m, p, q, k \in \mathbb{Z}$ with $p \neq q$ primes,

$$m^{(p-1)(q-1)k+1} \equiv m \bmod pq$$

Chinese Remainder Theorem:

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$c \longmapsto (c, c)$$

If $\gcd(m,n) = 1$ then this is a BIJECTION, with inverse

$$(a, b) \longmapsto any + bmx$$
$$(mx + ny = 1).$$

Corollary: Restrict to invertible elements, get a bijection

$$(\mathbb{Z}/mn\mathbb{Z})^\times \longleftrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$
$$\phi(mn) = \phi(m)\phi(n)$$

Follows that
$$\phi(n) = n \prod_{p \mid n} \left(\frac{p-1}{p}\right).$$

$\square$

What next ?

Topics I want to get to:

- Quadratic Reciprocity
- Integer Points on Conics

Example: Pell's Equation

$$x^2 - dy^2 = 1$$

This will involve arithmetic in the ring $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$

An algorithm to find solutions comes from CONTINUED FRACTIONS.

To some extent, we will follow "Elements of Number Theory", by John Stillwell

---

Our first new topic will be the "Primitive Root Theorem"

Recall: for $a, n \in \mathbb{Z}$, $n \geq 1$, define

$$\mathrm{ord}_n(a) = \min\{r \geq 1 : a^r \equiv 1 \bmod n\}.$$

Example $n = 5$

a	0	1	2	3	4
$\mathrm{ord}_5(a)$	∞	1	4	4	2

$2,\ 2^2 = 4 \not\equiv 1,\ 2^3 = 8 \not\equiv 1,\ 2^4 = 16 \equiv 1$

$3 \not\equiv 1,\ 3^2 = \underset{4}{9} \not\equiv 1,\ 3^3 = 12 \equiv \underset{\not\equiv 1}{2},\ 3^4 = 6 \equiv 1$

$4 \not\equiv 1,\ 4^2 = \underset{\equiv 1}{16}$

Jargon: 2 & 3 are <u>primitive roots</u> mod 5 because they have maximum possible order mod 5.

Example $n = 8$

a	0	1	2	3	4	5	6	7
$\mathrm{ord}_8(a)$	∞	1	∞	2	∞	2	∞	2

There are <u>no</u> primitive roots mod 8 because no element has order $\phi(8) = 4$.

DEF: Euler's Totient Theorem says $\mathrm{ord}_n(a) \mid \phi(n)$.

If $\mathrm{ord}_n(a) = \phi(n)$ then we say "a is a <u>primitive root</u> mod n," in which case we can write

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{1, a, a^2, a^3, \dots, a^{\phi(n)-1}\}$$

[Remark: Then we can use powers of a to do computations.]

Two Questions:

1. When do Primitive Roots Exist?
2. How to find one?

Primitive Root Theorem:

$\exists$ primitive root(s) mod $n \iff$
$n = 1, 2, 4, p^k, 2p^k$ (p odd prime).

We won't prove the full theorem.
Instead we will prove

<u>Theorem</u>: Let p be prime. Then
there exist $\phi(p-1)$ primitive roots
mod p.

Test: $p=5$ is prime.
There should be $\phi(5-1) = \phi(4) = 2$
primitive roots mod 5.

Our next goal is to prove P.R.T.
There is no really short proof :(

I won't show you the quickest proof, but I will show you the BEST proof. We will need two lemmas.

- A polynomial of degree d with integer coefficients has $\leq d$ roots <u>mod p</u> for any prime p.

Remark: Primality is necessary!

x^2-1 has 4 roots mod 8.
Namely, $x = 1, 3, 5, 7$.

- A property of the totient:

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

Example : $n = 15$

Divisors $d = 1, 3, 5, 15$.

$\phi(1) = 1$

$\phi(3) = 2$

$\phi(5) = 4$

$\phi(15) = \phi(3)\phi(5) = 8$.

Hence $\phi(1) + \phi(3) + \phi(5) + \phi(15)$

$= 1 + 2 + 4 + 8$

$= 15$, as expected. ✓

This is not so hard if we think about reducing fractions to lowest terms.

$$\frac{1}{8}, \frac{2}{8}, \frac{3}{8}, \frac{4}{8}, \frac{5}{8}, \frac{6}{8}, \frac{7}{8}, \frac{8}{8}$$

$$\Downarrow$$

$$\frac{1}{8}, \frac{1}{4}, \frac{3}{8}, \frac{1}{2}, \frac{5}{8}, \frac{3}{4}, \frac{7}{8}, \frac{1}{1}$$

Counting fractions by denominators
gives 4 with denominator 8
2 with denominator 4
1 with denominator 2
1 with denominator 1

Observe: $4 = \phi(8)$
$2 = \phi(4)$
$1 = \phi(2)$
$1 = \phi(1)$ ✓

The proof will show that this works in general.

Theorem/Lemma: $\forall n \geq 1$,

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

Proof: Define two sets

$$F_n = \left\{ \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n} \right\}$$

$$F_n' = \left\{ \frac{k}{n} : 1 \le k \le n,\ \gcd(k,n) = 1 \right\}.$$

Observe $\# F_n = n$

$\# F_n' = \phi(n)$

We will show that

$$F_n = \coprod_{d \mid n} F_d'$$

disjoint union of sets.

Then it will follow that

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

We need to show three things:

① $F_n \subseteq \bigcup_{d \mid n} F_d'$

② $\bigcup_{d \mid n} F_d' \subseteq F_n$

$\left.\right\}$ $F_n = \bigcup_{d \mid n} F_d'$

③ $F_d' \cap F_e' = \emptyset$ when $d \neq e$.

(1) Given $k/n \in F_n$ we let

$\lambda = \gcd(k,n)$, $k = \lambda k'$, $n = \lambda n'$,

so that $\gcd(k', n') = 1$. Then

$$\frac{k}{n} = \frac{\lambda k'}{\lambda n'} = \frac{k'}{n'} \in F_{n'}'$$

Since $n' | n$ we get

$$\frac{k'}{n'} \in \bigcup_{d|n} F_d' .$$

(2) STAY TUNED !