Theorem: Euler's Theorem

$G = U(\mathbb{Z}_n), |G| = \phi(n)$. If $x \in U(\mathbb{Z}_n)$, then $x^{|G|} = e$. If $\gcd(a, n) = 1$ then $a^{\phi(n)} = 1 \mod n$.

Note. It's the same thing as Fermat with $\mathbb{Z}_n^*$. The units of

How many elements in $U(\mathbb{Z}_n)$?

Definition: Euler's phi-function

$\phi(p) = p - 1$ in $U(\mathbb{Z}_p)$. $\phi(1) = 1$.

Example. $\phi(9) = 3$.

Proposition

$\phi(p^n) = p^{n-1}(p-1)$.

Example. $\phi(1000)$. Even numbers and multiples of 5 are factors. The units are the ones that don't have 2 or 5 as factors.

Example (solving congruence)**.** Solving $ax = b \mod m$, $a, b, m \in \mathbb{Z}$. "Congruence mod m": $ax - b = km$ for some $k \in \mathbb{Z}$. So $b = ax - km$.

$d = \gcd(a, m)$. So a is a multiple of d, m is a multiple of d. So $b = ax - km$ is multiple of d. So by contrapositive, if d doesn't divide b then there is no solution.

If we assume d/b. Define $b' = \frac{b}{d}, a' = \frac{a}{d}, m' = \frac{m}{d}$ all integers. Then

$$\begin{aligned} b' &= a'x - km' \\ a'x &= b' \mod m' \end{aligned}$$

This is better because let $a = 30, m = 42$, then $d = 6, a' = \frac{30}{6} = 5, m' = \frac{42}{6} = 7$. Then $\gcd(a', m') = 1$ always coprime!

Now, a' is a unit in $\mathbb{Z}_{m'}$. This means $a'x = b'$ has a unique solution in $\mathbb{Z}_{m'}$ by multiplying by the inverse.

Example (20.14)**.** $12x = 27 \mod 18$. $a = 12, b = 27, m = 18$. $d = 6$. Since d doesn't divide b, no solution.

$15x = 27 \mod 18$. $d = 3$. d/b. So $a' = 5, m' = 6, b' = 9$. So $5x = 9 \mod 6 \Rightarrow 5x = 3 \mod 6$. Since 5 and 6 are coprime, 5 is a unit in $\mathbb{Z}_6$. The inverse is also 5.

So
$$5 \times 5x = 5 \times 3 \mod 6 \Rightarrow x = 3 \mod 6.$$

What is the relationship between mod 18 and mod 6?

Since 18 is a multiple of 6, so mod 18 implies mod 6. So if $x = 3 \mod 6 \Rightarrow x = 3, 9, 15 \mod 18$. There are d solutions here, evenly spaced mod 18, similar to U_n complex root of unity..

If $c = 5 \mod 9$ what is $c \mod 2$? Not well-defined.

Corollary: 20.13

$ax = b \mod m, d = \gcd(a, m)$.

- If d doesn't divide b, no solutions.
- If d/b, there are d solutions $\mod m$, and they are evenly spaced.

Note. This allows us to find all solutions if we find one.

21

Question: Is a subring of a field always a domain?

Example. $\mathbb{Z} \leq \mathbb{Q}$. It's a subset, nonempty, closed under addition, subtraction, and multiplication. It is also a domain.

Suppose $S \leq F$ a field. S inherits commutativity and no zero divisors. However, $2\mathbb{Z} \leq \mathbb{Q}$ doesn't have identity.

Theorem

If S is a subring of a field and S has identity, then S is a domain.

Goal: start with a domain and try to find the smallest field that contains it. (This always works!). This smallest field is called the field of fractions of the domain.

Example. $\mathbb{Z}$ is a domain. $\mathbb{Z} \leq F$. What could F be? It can be $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2})$. There is a smallest one: $\mathbb{Q}$.

To say two fractions are equal without mentioning division: $ad = bc$.