Math 312, lecture 10, 30/5/2018

Last time: Multiplicative order

Mod 7: $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$, $2^4 \equiv 2$, ...

$\text{ord}_7(2) = 3$

Lemma: Let $(a, m) = 1$. Then (1) $\exists k \geq 1$ s.t. $a^k \equiv 1 \ (m)$ ("periodicity exists")

(2) $a^r \equiv a^s \ (m)$ iff $r \equiv s \ (\text{ord}_m(a))$ ("$\text{ord}_m(a)$ is the period")

Summary: powers of a mod m (if $(a,m)=1$) form a periodic sequence, call period the "order" of a mod m.

Example: What is the order of 2 mod $2^n - 1$? $(n \geq 2)$

Note that $2^n \equiv 1 \ (2^n - 1)$ so $\text{ord}_m(2)$ $(m = 2^n - 1)$ divides n. Can it be a proper divisor?

Let $1 \leq k < n$. Can $2^k \equiv 1 \ (m)$ be true?

This would mean $2^k - 1 = (2^n - 1)c$ or $2^n - 1 \mid 2^k - 1$.

But $2^k - 1 < 2^n - 1$ so $2^n - 1 \nmid 2^k - 1$ and $2^k \not\equiv 1 \ (m)$

Conclusion: $\text{ord}_{2^n - 1}(2) = n$

Multiplicative order mod primes

("Fermat's little theorem")

Let p be a prime number. Among the residues $0 \le a < p$ only 0 is not invertible, i.e. $\mathcal{U}(p)$ consists of all $p-1$ non-zero residues.

Thm: (Fermat) Let $(a,p)=1$. Then $a^{p-1} \equiv 1 \ (p)$

(Ex. $2^3 \equiv 1 \ (7)$, $3 \mid 7-1$, $2^{10} \equiv 1 \ (11)$, $10 \mid 11-1$

Pf: let $A \equiv \prod_{x \in \mathcal{U}(p)} x \equiv (p-1)! \ (p)$

then $a^{p-1} \cdot A = \prod_{x \in \mathcal{U}(p)} (ax) \equiv \prod_{y \in \mathcal{U}(p)} y \equiv A$

↑ exactly $p-1$ invertible residues

The change of variable $y = ax$ is valid since it is reversible: have $x = \bar{a}y$.

A is invertible, (in fact $A \equiv -1 \ (p)$ by Wilson)

So $a^{p-1} A \equiv A \ (p) \Rightarrow a^{p-1} \equiv 1 \ (p)$

Cor: $\mathrm{ord}_p(a) \mid p-1$.

So, to find $\mathrm{ord}_p(a)$ enough to try divisors of $p-1$.

Example: $2^{10} \equiv 1 \ (11)$ by this thm

Note $2^2 = 4 \not\equiv 1 \ (11)$ $\quad (4 < 11)$

$2^5 = 32 = 33 - 1 \equiv -1 \ (11)$

$\not\equiv 1$

(Also $2^1 \not\equiv 1 \ (11)$)

But $\text{ord}_{11}(2)$ must divide 10, so it is 10.

Recall lemma: $a^r \equiv 1 \ (m)$ iff $\text{ord}_m(a) \mid r$

use it with $m = p$, $r = p - 1$.

Example: $2^6 \equiv 1 \ (7)$ also $2^3 \equiv 1 \ (7)$ but 3 has no further divisors so $\text{ord}_7(2) = 3$

Def: Call p a Sophie Germain prime if $q = 2p + 1$ is also prime. In this case call q a "safe prime".

Ex: $p = 2, \ q = 5$
$p = 3, \ q = 7$
$p = 5, \ q = 11$
$p = 11, \ q = 23$
⋮

Note: if (a, q) $\text{ord}_q(a) \mid q - 1$

but $q - 1 = 2p$, so $\text{ord}_q(a)$ is one of $1, 2, p, 2p$

if $a^1 \equiv 1 \ (p)$ then $a \equiv 1 \ (p)$

$a^2 \equiv 1$ but $a \not\equiv 1$ then $a \equiv -1 \ (p)$

bottom line: If q is a safe prime and $a \not\equiv -1, 0, 1 \bmod q$ then $\mathrm{ord}_q(a) \in \{p, 2p\}$?

---

i.e. every a has mult order of scale q

Cf. $\mathrm{ord}_{2^n-1}(2) = n \asymp \log(2^n - 1)$

Are there any safe primes / Sophie Germain primes?

- Not proved that there are ∞ly many
  (about as hard as having $p, p+2$ both prime)
- Believe: up to x about $\frac{Cx}{(\log x)^2}$ such primes

Tips

(1) Do excercises: - Textbooks (Rosen, Jones[2])
- Notes by Freitas-Gherga
- Practice sets by -"-

(2) Doing problems develops your intuitions