MATH 656- Spring 2019 Class Notes

Scribe: Carolyn Rogers
April 10, 2019

April 15, 2019

1 Euler Tasks:

Task 29: $2^{11} - 1 = 2047 = 23 * 89$
↳ NOT prime

Conjecture 1: There are infinitely many primes where $2p+1$ is also prime. (Sophie Germain Primes)

Conjecture 2: There are infinitely many primes where $2^p - 1$is prime. (Mersenne Primes)

Conjecture 3: There are infinitely many n with $2^{2^n} + 1$ primes. (Fermat Primes)

* No one knows a proof of any of these conjectures.*

2 Task:

Create a table of exponents (mod 11).

Exponents

Bases \ a^k	1	2	3	4	5	6	7	8	9	10 (mod 11)
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

Observations:

- when $k = 10$ $(p-1)$, $a^k \equiv 1(mod\ 11)$.

  ↳ $a^{p-1} \equiv 1(mod\ p)$.→ *Fermat's Little Theorem*

- $a = 2, 6, 7, 8$ "don't repeat". All the values are unique.

- $a^5 \equiv \begin{cases} 1 & a = 3, 4, 5, 9 \\ 10 & a = 2, 6, 7, 8, 10 \end{cases}$

- $10^k \equiv \begin{cases} 1 & k \equiv 0(mod\ 2) \\ 10 & (\text{k} \equiv 1 \text{ (mod 2)} \end{cases}$
- $1, 3, 4, 5$, and 9 are the only numbers that appear when the base is not $2, 6, 7$,and 8.
- Once we encounter a 1, the row repeats.
- In the even columns, the numbers are "symmetric" if the columns were flipped between 5 and 6.

It is useful to know what power of something gives us 1 (mod_)

3 Chapter 7

Book Definition: a belongs to the exponent $h(mod\ m)$, if $a^h \equiv 1(mod\ m)$ and h is the least exponent this is true.

Example:

- 2 belongs to the exponent $10(mod\ 11)$
- 3 belongs to the exponent $5(mod\ 11)$

↳ We're going to call this the order of $a(mod\ m)$.

- The order of $2(mod\ 11)$ is 10.
- The order of $3(mod\ 11)$ is 5.

We write this as $ord_m(a)$

- $ord_{11}(2) = 10$, $ord_{11}(3) = 5$, $ord_{11}(10) = 2$.

Theorem 1: If the $ord_m(a) = h$ and $a^r \equiv 1(mod\ m)$, then $h|r$.

Proof. Write $r = hk + s$, (division with remainder), where $s < h$.

Then, $1 \equiv a^r \equiv a^{hk+s}(mod\ m)$
$\equiv a^{hk} \cdot a^s(mod\ m)$
$\equiv (a^h)^k \cdot a^s(mod\ m)$
$\equiv 1 \cdot a^s(mod\ m)$
So, $a^s \equiv 1(mod\ m)$
$s < h$. So, $s = 0$
Therefore, $h|r$.

□

Corollary 1: Since $a^{\varphi(m)} \equiv 1(mod\ m)$. If $gcd(a,m) = 1$. We have that the $ord_m(a)|\varphi(m)$, if $gcd(a,m) = 1$.

> **Example:** $\varphi(11) = 10$, so the order of every element should divide 10. $ord_{11}(2) = 10$, $ord_{11}(3) = 5$, $ord_{11}(10) = 2 \rightarrow$ all divide 10 ✓

Definition: a is a primitive root $(mod\ m)$ if $ord_m(a) = \varphi(m)$.

> **Example:** The primitive roots mod 11 are 2, 6, 7, 8.

> **Example:** $m = 8$
> If $gcd(a, 8) \neq 1$, then $a^k \equiv 1(mod\ 8)$ isn't possible.
> ↳ Only possibilities are 1, 3, 5, 7.
> $3^2 \equiv 1(mod\ 8)$, $ord_8(3) = 2 = ord_8(5) = ord_8(7)$
> $5^2 \equiv 25 \equiv 1(mod\ 8)$
> $7^2 \equiv 49 \equiv 1(mod\ 8)$
> Since $\varphi(8) = 4$, 8 has no primitive roots.

Theorem 2: If a is a primitive root $(mod\ m)$, then $a^1, a^2, a^3, ..., a^{\varphi(m)}$ are mutually in-congruent and form a reduced residue system $(mod\ m)$.

Proof. (By contradiction)

Suppose there exists $1 \leq r < s \leq \varphi(m)$, with $a^r \equiv a^s(mod\ m)$,
then, $a^r \equiv a^r(a^{s-r})(mod\ m)$
$1 \equiv a^{s-r}(mod\ m)$
So, $s - r > 0$ and $s - r < \varphi(m)$, but $a^{s-r} \equiv (mod\ m)$. This contradicts $\varphi(m)$ being the order of $a(mod\ m)$.

□

Theorem 3: If the $ord_m(a) = h$ and $gcd(h,k) = d$, then $ord_m(a^k) = \frac{h}{d}$.

> **Example:** $ord_{11}(2) = 10 = h$
> Let $k = 6$
> $gcd(10, 6) = 2$
> $ord_{11}(2^6) \equiv ord_{11}(9) = \frac{10}{2} = 5$ ✓
> $*2^6 \equiv 9(mod\ 11)$

Proof. Write $j = ord_m(a^k)$

(goal: prove that $j = \frac{h}{d} = h_1$)
Write: $h_1 = \frac{h}{d}$, $k_1 = \frac{k}{d}$
Since $j = ord_m(a^k)$
$1 \equiv (a^k)^j \equiv a^{kj}(mod\ m)$
Since $ord_m(a) = h_1$, we know $h|kj$.
Then, $h_1|k_1j$ (divided out the gcd from each)
and $gcd(h_1, k_1) = 1$. So, $h_1|j$.

Now, compute
$$\begin{aligned}(a^k)^{h_1} &\equiv a^{kh_1}(mod\ m)\\ &\equiv a^{k_1h_1d}(mod\ m)\\ &\equiv a^{hk_1}(mod\ m)\\ &\equiv (a^h)^{k_1}(mod\ m)\\ &\equiv 1(mod\ m)\end{aligned}$$

So, $(a^k)^{h_1} \equiv 1 (mod\ m)$
So, $ord_m(a^k)|h_1$. Thus, $j|h_1$
So, $j = h_1 \Rightarrow ord_m(a^k) = \frac{h}{d}$

□

Corollary 2: If g is a primitive root $(mod\ m)$, then g^r is a primitive root $(mod\ m)$ if and only if $gcd(r, \varphi(m)) = 1$.

Proof. The order of $g^r = \frac{ord_m(g)}{gcd(r, ord_m(g))} = \frac{\varphi(m)}{gcd(r, \varphi(m))}$

This equals $\varphi(m)$ exactly when $gcd(r, \varphi(m)) = 1$.

□

Example: If g is a primitive root $(mod\ 11)$, then g^r is a primitive root $(mod\ 11)$.

If $gcd(r, 10) = 1$, then $r = 1, 3, 7, 9$. Try this with $g = 2$...
$2^3 \equiv 8$ ✓
$2^7 \equiv 7$ ✓
$2^9 \equiv 6$ ✓
$8, 7$ and 6 are all primitive roots.

Corollary 3: If m has a primitive root, then it has $\varphi(\varphi(m))$ primitive roots.

Proof. If g is a primitive root, then g^r is a primitive root whenever $gcd(r, \varphi(m)) = 1$.
The number of such things is $\varphi(\varphi(m))$.

□

Example: $\varphi(\varphi(11)) = \varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4$.
So, 11 has 4 primitive roots.

When do we have at least one primitive root?
↳ Answer: m has a primitive root if and only if m is a prime or twice a prime.

Theorem 4: Every prime has a primitive root.

Proof. Let p be a prime. Then $ord_p(a)|p-1$. Let $N(h) = \#\{a(mod\ p)|ord_p(a) = h\}$
(count the number of residues $(mod\ p)$, with $ord_p(a) = h$)

Example: If $p = 11$
$N(2) = 1\ \{10\}$
$N(5) = 4\ \{3, 4, 5, 9\}$
$N(10) = 4\ \{2, 6, 7, 8\}$
$N(1) = 1\ \{1\}$

Now, $\Sigma_{h|p-1} N(h) = p - 1$
Goal: prove $N(p-1) \neq 0$ (Then has a primitive root)
Claim that $N(h)$ is either 0 or $\varphi(h)$. If it's not zero, then at least one thing has order h, call it b.
$b^h \equiv 1 (mod\ p)$.
Now, consider $x^h \equiv 1\ (mod\ p)$
$x^h - 1 \equiv 0\ (mod\ p)$

This polynomial has at most h distinct roots. $b^1, b^2, b^3, ..., b^h$ all satisfy this equation because
$(b^i)^h - 1 \equiv (b^h)^i - 1$
$\equiv 1 - 1 \equiv 0 (mod\ p)$.
So, these are all of the solutions to this equation.
How many of these have order h?
b^i has order h iff $gcd(i, h) = 1$.
So, there are $\varphi(h)$ many such i.
$N(h) = 0$ or $\varphi(h)$
Now, $p - 1 = \Sigma_{h|p-1} N(h)$
If $N(h) < \varphi(h)$, then $p - 1 = \Sigma_{h|p-1} N(h) < \Sigma_{h|p-1} \varphi(h) = p - 1$
Recall: $\Sigma_{d|n} \varphi(d) = n \rightarrow$ Contradiction!
So, $N(h) = \varphi(h)$ (ALWAYS!)
$N(p - 1) = \varphi(p - 1)$ and $\varphi(p - 1) \geq 1$.
So, p has at least one element of order $p - 1$.
So, p has a primitive root.
(In fact it has $\varphi(p - 1)$ many.)

$\square$