Chapter 9 Lecture Notes

Greg Knapp

May 16, 2022

1 The Order of an Integer and Primitive Roots

1.1 Prologue

- Everything we're about to say follows from the fact that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a finite abelian group
- If you know things about finite abelian groups, put everything that we say in this chapter into that context in your mind

1.2 Motivation and Def of Order

- Recall how we started the term with Euler's theorem: If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \mod n$.
- We then went to explore how to compute $\varphi(n)$ and we got this cool formula:

$$\varphi(n) = n \cdot \prod_{p|n} 1 - \frac{1}{p}$$

- After that, we let ourselves get sidetracked by the fact that φ was multiplicative and we explored a bunch of other stuff
- We're going to return to where we started though: given $a, n \in \mathbb{Z}_{>0}$ with $(a, n) = 1$, which values of x yield $a^x \equiv 1 \mod n$?
- Let's return to our example from chapter 6 (use as warm-up exercise):

x	1	2	3	4	5	6	7	8
1^x	1	1	1	1	1	1	1	1
2^x	2	4	8	7	5	1	2	4
4^x	4	7	1	4	7	1	4	7
5^x	5	7	8	4	2	1	5	7
7^x	7	4	1	7	4	1	7	4
8^x	8	1	8	1	8	1	8	1

- Recall that $\varphi(9) = 6$
- We already know (by Euler's theorem) that column 6 will have all 1s
- But notice that for some elements, we hit 1 sooner.
- Also for some elements, we don't hit 1 until column 6.
- Let's temporarily define the order of an element to be the least positive x so that $a^x \equiv 1 \mod n$ (it's not clear at this point that this is a good definition)
- What are the orders of various elements?

  - Order of 1 is 1
  - Order of 2 is 6
  - Order of 4 is 3
  - Order of 5 is 6
  - Order of 7 is 3
  - Order of 8 is 2

- Notice that all of the orders are divisors of 6.
- Notice also that any row of an element of order 6 contains a reduced residue system
- How many of these observations can we make for other moduli?
- For any n, will column $\varphi(n)$ have all 1s?
- For any n, will there be elements of order $< \varphi(n)$?
- For any n will there be some element of order $= \varphi(n)$?
- For any n and $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, will the order of a divide $\varphi(n)$?
- For any n and $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ of order $\varphi(n)$, will $\{a^x : 1 \leqslant x \leqslant \varphi(n)\}$ be a reduced residue system modulo n?
- Let's look also at $n = 8$:

x	1	2	3	4
1^x	1	1	1	1
3^x	3	1	3	1
5^x	5	1	5	1
7^x	5	1	5	1

- $\varphi(8) = 4$
- Orders of elements are 1 and 2
- Note that column 4 contains all 1s
- Note that there are elements of order $< \varphi(n)$
- There is no element of order $= \varphi(n)$
- The order of every element divides $\varphi(n)$
- The last question doesn't apply
- Go back to our general question of "for which values of x is $a^x \equiv 1 \mod n$?"
- We can answer this question by cheating: Let $S = \{x : a^x \equiv 1 \mod n\}$
- S is nonempty because $\varphi(n) \in S$
- By the well-ordering principle, S has a least element
- **Def:** For any $a, n \in \mathbb{Z}_{>0}$ with $(a, n) = 1$, define the <u>order</u> of a modulo n to be the least integer x so that $a^x \equiv 1 \mod n$. We denote this number by $\mathrm{ord}_n(a)$

1.3 Examples

- From the previous examples, we have
  - $\text{ord}_8(1) = 1$ and $\text{ord}_9(1) = 1$
  - $\text{ord}_9(2) = 6$
  - $\text{ord}_8(3) = 2$
  - $\text{ord}_9(4) = 3$
  - $\text{ord}_8(5) = 2$ and $\text{ord}_9(5) = 6$
  - $\text{ord}_8(7) = 2$ and $\text{ord}_9(7) = 3$
  - $\text{ord}_9(8) = 2$
- There's not really a great pattern for us to draw on here.

1.4 Fact Collection

- Given $a, n \in \mathbb{Z}_{>0}$ with $(a, n) = 1$, let's reconsider the set $S = \{x > 0 : a^x \equiv 1 \mod n\}$
- Let's look at $n = 9$ and $a = 4$
- Exercise: what is S for these values of n and a?
- S ends up being the set of all multiples of $3 = \text{ord}_9(4) = \text{ord}_n(a)$
- There's a reason for this: the list of powers of 4 cycles through 3 different numbers and we hit 1 every 3 powers of 4
- More generally, we have
- **Thm:** Suppose $a, n \in \mathbb{Z}_{>0}$ with $(a, n) = 1$. Then for any $x \in \mathbb{Z}_{>0}$, $a^x \equiv 1 \mod n$ if and only if $\text{ord}_n(a) \mid x$
- Proof:
  - First suppose $\text{ord}_n(a) \mid x$
  - Then there exists $k \in \mathbb{N}$ so that $x = k \, \text{ord}_n(a)$
  - Hence, $a^x \equiv a^{k \, \text{ord}_n(a)} \equiv \left(a^{\text{ord}_n(a)}\right)^k \equiv 1 \mod n$
  - Next suppose that $a^x \equiv 1 \mod n$
  - (We want to show that x is a multiple of $\text{ord}_n(a)$ and we know that $\text{ord}_n(a)$ is the least power of a to yield 1 mod n...what do you think we might need to do for this?)
  - Use Euclidean division to write $a = q \, \text{ord}_n(a) + r$ where $0 \leqslant r < \text{ord}_n(a)$
  - Then
  $$1 \equiv a^x \equiv a^{q \, \text{ord}_n(a) + r} \equiv a^r \mod n$$
  - $\text{ord}_n(a)$ is the least positive power of a congruent to 1 mod n and since $0 \leqslant r < n$, we must have $r = 0$
  - Hence x is a multiple of $\text{ord}_n(a)$
- We now know that whenever $a^x \equiv 1 \mod n$, x is a multiple of $\text{ord}_n(a)$.
- But there's something that we can always plug in for x: $x = \varphi(n)$
- Hence, $\text{ord}_n(a) \mid \varphi(n)$
- So the order of an integer is always a divisor of $\varphi(n)$

- Moreover, we can say something a little bit better than just $a^x \equiv 1 \mod n$ whenever x is a multiple of $\mathrm{ord}_n(a)$
- Our table for powers of 4 mod 9 repeated: every time I had a power that was a multiple of 3, we got 1
- Every time we had a power that was one more than a multiple of 3, we got 4
- Every time we had a power that was two more than a multiple of 3, we got 7
- So it seems that if $x \equiv y \mod 3$, then $4^x \equiv 4^y \mod 9$
- More generally, we can say the following:
- Suppose that $a, n \in \mathbb{Z}_{>0}$ and $(a, n) = 1$. Then for any $x, y \in \mathbb{Z}_{>0}$, $a^x \equiv a^y \mod n$ if and only if $x \equiv y \mod \mathrm{ord}_n(a)$
- Proof:
  - First suppose that $x \equiv y \mod \mathrm{ord}_n(a)$.
  - WLOG, $x \geqslant y$
  - Then $x = y + k\,\mathrm{ord}_n(a)$ for some $k \geqslant 0$
  - So $a^x \equiv a^{y+k\,\mathrm{ord}_n(a)} \equiv a^y \mod n$
  - Now if $a^x \equiv a^y \mod n$, we can divide both sides by a^y again assuming $x \geqslant y$
  - Then $a^{x-y} \equiv 1 \mod n$, so $\mathrm{ord}_n(a) \mid x - y$
  - I.e. $x \equiv y \mod \mathrm{ord}_n(a)$

1.5 Primitive Roots

- Let's further explore the concept of numbers which have maximal order.
- We already know that for some n, there's no $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $\mathrm{ord}_n(a) = \varphi(n)$
- Can we classify for which n this property holds?
- If such an a exists, what can we learn about a?
- **Def:** Suppose n is a positive integer and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then a is a primitive root modulo n if $\mathrm{ord}_n(a) = \varphi(n)$
- For example, we saw that 9 has 2 and 7 as primitive roots
- We also saw that 8 has no primitive roots.
- Exercise: do 10,11,12, and 13 have primitive roots?
- **Ex:** Show that 3 is a primitive root mod 17
  - Naive method: compute 3^x for $1 \leqslant x \leqslant 16$.
  - Better method:
  - Note that $\varphi(17) = 16$ which has divisors 1,2,4,8,16
  - These are the possible orders of 3, so we compute

$$\begin{aligned} 3^2 &\equiv 9 \mod 17 \\ 3^4 &\equiv 81 \equiv 13 \mod 17 \\ 3^8 &\equiv 169 \equiv 16 \mod 17 \end{aligned}$$

  so the order of 3 must be 16. Hence, 3 is a primitive root.

- Here's a nice feature of primitive roots:
- **Thm:** If n is a positive integer and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, then

$$S = \{a^j : 1 \leqslant j \leqslant \varphi(n)\}$$

  is a reduced residue system modulo n
- Pf:
  - We'll show two things:
    - All elements of S are relatively prime to n
    - All elements of S are distinct modulo n
  - Once we've done this, we'll know that we have a reduced residue system
  - For the first, note that $(a, n) = 1$ implies that $(a^j, n) = 1$, so we're done there
  - For the second, note that if $a^i \equiv a^j \mod n$ with $i \leqslant j$, we can divide both sides by a^i to get $1 \equiv a^{j-i} \mod n$
  - But then $j - i$ must be a multiple of $\mathrm{ord}_n(a) = \varphi(n)$
  - But $j - i < \varphi(n)$, so $j = i$
- Once we know that an integer has a primitive root, we want to know how many it has
- Suppose that a is a primitive root
- Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is generated by the powers of a
- So it would be nice to know what the order of a^u is for $1 \leqslant u \leqslant \varphi(n)$
- In fact, we can generally do this without the assumption that a is a primitive root.
- **Thm:** If $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\mathrm{ord}_n(a) = t$, and $u \in \mathbb{Z}_{>0}$, then

$$\mathrm{ord}_n(a^u) = \frac{t}{(t, u)}$$

- Proof:
  - Unfortunately unenlightening
  - Let $s = \mathrm{ord}_n(a^u)$
  - $v = (t, u)$
  - $t = t_1 v$
  - $u = u_1 v$
  - We know that $(t_1, u_1) = 1$
  - Because $t_1 = \frac{t}{(t,u)}$, we want to show that $s = \mathrm{ord}_n(a^u) = t_1$
  - We'll employ a common trick and show that $s \mid t_1$ and $t_1 \mid s$
  - First,

$$(a^u)^{t_1} = (a^{u_1 v})^{t/v} = a^{tu_1} \equiv 1 \mod n$$

    because $\mathrm{ord}_n(a) = t$
  - Hence, $s \mid t$
  - Next,

$$(a^u)^s \equiv 1 \mod n$$

    we get $t \mid us$

- Hence $t_1 v \mid u_1 v s$ implying that $t_1 \mid u_1 s$
  - But since $(t_1, u_1) = 1$, $t_1 \mid s$
  - Therefore, $t_1 = s$ and we're done.

- More interesting is the following corollary
- **Cor:** Suppose that r is a primitive root modulo n. Then r^u is a primitive root if and only if $(u, \varphi(n)) = 1$
- Proof:
  - By the previous theorem

$$\begin{aligned}\mathrm{ord}_n(r^u) &= \frac{\mathrm{ord}_n(r)}{(u, \mathrm{ord}_n(r))}\\ &= \frac{\varphi(n)}{(u, \varphi(n))}\end{aligned}$$

    which equals $\varphi(n)$ if and only if $(u, \varphi(n)) = 1$

- As a consequence, if n has a primitive root, then it has $\varphi(\varphi(n))$ primitive roots.
- **Ex:** 2 is a primitive root modulo 11. Find all primitive roots modulo 11
  - $\varphi(11) = 10$, so we want to look at raising 2 to powers which are relatively prime to 10.
  - These powers are 2^1, 2^3, 2^7, and 2^9 yielding $2, 8, 7$, and 6

2 Primitive Roots for Primes

2.1 Intro

- Goal: to provide a partial answer to the question of: which integers have primitive roots?
- Warm-up: starting at $n = 2$, which integers have primitive roots?
- Make a conjecture based on that
- Yes: 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, 22, 23, 25, 26, 27, 29
- Make a conjecture based on that
- No: 8, 12, 15, 16, 20, 21, 24, 28, 30
- Make a conjecture based on that
- It seems like the integers which have primitive roots are 2, 4, powers of odd primes, and 2 times powers of odd primes
- As with many things in math, it's best to start proving a conjecture with the easiest cases.
- The easiest cases are 2 and 4 and check, we've done those
- Next, we want to worry about powers of odd primes
- But there's actually something a little easier we can start with: odd primes

2.2 From the Top Down

- Goal: Every prime has a primitive root
- Rephrased: $(\mathbb{Z}\,/\,p\mathbb{Z})^\times \cong (\mathbb{Z}\,/\,(p-1)\mathbb{Z})$
- Note: at every step of this proof ask: "Why do we need a prime?"
- **Thm:** Let p be prime and let d be a positive divisor of $p-1$. Then the number of incongruent integers of order d modulo p is equal to $\varphi(d)$.
- (Warm-up) Question: How does this imply our goal?
  - If we show this, take $d = p-1$ (positive divisor of $p-1$)
  - Conclusion is that there are $\varphi(p-1)$ integers of order $p-1$
  - But that's $\varphi(p-1)$ primitive roots
  - Since $\varphi(p-1) \geqslant 1$, we have at least 1 primitive root
- Question: How does this fit into context that we already understand?
  - Recall: we showed that if an integer n has a primitive root, then there are $\varphi(\varphi(n))$ primitive roots.
  - Taking $n = p$ to be prime, this is $\varphi(p-1)$ primitive roots
  - So this was a result of the form "if there is one primitive root, then there are $\varphi(p-1)$" where we're about to show "there are $\varphi(p-1)$"
  - We're taking a result that was conditional and with a different strategy, we're going to show it unconditionally
  - But the original result was more general because it didn't just apply to primes
  - This is a lot like how math research operates: someone will prove "if A, then B" and someone else will show that B always holds in certain cases (independent of A) and finally someone will put a bunch of pieces together and classify exactly when B happens
- Partial proof of theorem:
  - For each $d \mid p-1$, let
    $$S_d = \#\left\{n \in \left(\mathbb{Z}\middle/p\mathbb{Z}\right)^\times : \mathrm{ord}_p(n) = d\right\}$$
    and let $F(d) = \#S_d$
  - Since the S_d are pairwise disjoint and every element of $(\mathbb{Z}\,/\,p\mathbb{Z})^\times$ lives in one S_d, we have
    $$\left(\mathbb{Z}\middle/p\mathbb{Z}\right)^\times = \bigcup_{\substack{d\mid p-1\\ d>0}} S_d$$
    and so
    $$p-1 = \#\left(\mathbb{Z}\middle/p\mathbb{Z}\right)^\times = \sum_{\substack{d\mid p-1\\ d>0}} F(d)$$
  - But recall that $p-1 = \sum_{d\mid p-1}\varphi(d)$, so now we have
    $$\sum_{d\mid p-1}\varphi(d) = \sum_{d\mid p-1} F(d)$$
  - If we can show that $F(d) \leqslant \varphi(d)$ for all $d \mid p-1$, then we will conclude that $F(d) = \varphi(d)$

- Why?
  - Example: $p = 7$.
  - We just showed that $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = F(1) + F(2) + F(3) + F(6)$
  - If we know $F(1) \leqslant \varphi(1)$, $F(2) \leqslant \varphi(2)$, etc. then when we add them all up, the only way for both sides to be equal would be if we actually had $F(1) = \varphi(1)$, etc.
  - Another way to see it is if we had $F(2) < \varphi(2)$, then we would have $\sum F(d) < \sum \varphi(d)$, which we don't
- Once we conclude that $F(d) = \varphi(d)$, we have that the number of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d is equal to $\varphi(d)$

- Question: how do we show that $F(d) \leqslant \varphi(d)$?
- Let's think about what it means to be an element of order d
- This means that $a^d \equiv 1 \mod p$ AND that $a^x \not\equiv 1 \mod p$ when $x < d$
- Thinking about $a^d \equiv 1 \mod p$ for a second, notice that $a^d \equiv 1 \mod p$ if and only if a is a "root mod p" of $x^d - 1$
- I.e. $a^d - 1 \equiv 0 \mod p$
- So we're trying to count certain roots of $x^d - 1$ mod p
- We've looked at polynomials mod p before
- In particular, we tried to do things like solve $x^2 - 5 \equiv 0 \mod 7$ before
- We also looked at $x^2 - 5 \mod 14$ (by breaking it up and using Sun-Tsu), but right now we're working with a prime modulus

2.3 Detour: Polynomials mod p

- Recall our new goal: When $d \mid p - 1$, there are no more than $\varphi(d)$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d
- Each element of order d is a root of $x^d - 1$
- Question: how many roots of $x^d - 1$ mod p are there?
- Warm-up: how many roots of $x^{p-1} - 1$ mod p are there?
- Answer: by FLT, we have $p - 1$ roots
- But maybe we still don't know the answer to the first question, so let's go somewhere a little more familiar
- Question: how many real roots does $x^d - 1$ have?
- Question: how many complex roots does $x^d - 1$ have?
- Most importantly, we use the degree of the polynomial as a good indicator of how many roots it could have
- **Thm:** (Lagrange) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with $a_0, \ldots, a_n \in \mathbb{Z}$ and degree at least 1. Then $f(x)$ has at most n incongruent roots mod p
- First note that we are using the fact that p is prime here! Recall that $x^2 - 4$ has four roots mod 15.
- Proof: Not super critical, can skip if no time. Uses induction on degree and the fact that linear polynomials have roots mod p
  - We can assume that $a_n \not\equiv 0 \mod p$

- Induct on the degree:
- $n = 1$ comes from the fact that a_1 is invertible mod p
- Now suppose that polynomials of degree $\leqslant n-1$ have $\leqslant$ degree roots
- Assume by contradiction that there is a polynomial, $f(x) = a_n x^n + \cdots + a_1 x + a_0$ of degree n with $n+1$ distinct roots mod p
- Write those roots as $c_0, \ldots, c_n$
- Then

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0) \\ &= a_n(x-c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + xc_0^{n-2} + c_0^{n-1}) + a_{n-1}(x-c_0)(x^{n-2} + x^{n-3}c_0 + \cdots + xc_0^{n-3} + c_0 \\ &= (x-c_0)g(x) \end{aligned}$$

- For some polynomial $g(x)$ with degree $\leqslant n-1$
- But notice that
$$0 \equiv f(c_i) \equiv (c_i - c_0)g(c_i) \mod p$$
and dividing by $c_i - c_0$ gives that c_i is a root of $g(x)$
- But now $g(x)$ has at least n roots and degree $\leqslant n-1$, contradiction

* Question: where did we use the fact that p was prime in this proof?
* From here, we can now say something about the polynomial $x^d - 1$ mod p when $d \mid p-1$
* (This is the type of polynomial where we wanted to count its roots)
* **Thm:** Let p be prime and let d be a divisor of $p-1$. Then $x^d - 1$ has exactly d incongruent roots mod p
* Proof:
  - Since $d \mid p-1$, there exists $e \in \mathbb{Z}$ so that $de = p-1$
  - Then
  $$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1) = (x^d - 1)g(x)$$
  - We already know that x^{p-1} has exactly $p-1$ distinct roots
  - We know that $g(x)$ has at most $d(e-1) = p-1-d$ roots
  - But this means that $x^d - 1$ has to take up the rest of the slack, giving $x^d - 1$ at least $(p-1) - (p-1-d) = d$ roots
  - Since $x^d - 1$ has at most d roots, we're done

2.4 Return to the proof

* Recall that for $d \mid p-1$ we had $F(d)$ equal to the number of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d
* We wanted to show that $F(d) \leqslant \varphi(d)$ because that would imply $F(d) = \varphi(d)$
* Lemma: $F(d) \leqslant \varphi(d)$
* Proof:
  - If $F(d) = 0$, then we certainly have $F(d) \leqslant \varphi(d)$
  - Otherwise $F(d) \geqslant 1$ and we have that there exists an element of order d
  - Say $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order d

- Then the integers $a, a^2, a^3, \ldots, a^d$ are incongruent mod p because if not, then $a^i \equiv a^j \mod p$ with $1 \leqslant i < j \leqslant d$, so $1 \equiv a^{j-i} \mod p$, implying that $\text{ord}_p(a) \leqslant j - i \leqslant d - 1 < d$ contradiction
- Moreover, each of those powers of a is a root of $x^d - 1$ mod p because

$$(a^i)^d - 1 \equiv (a^d)^i - 1 \equiv 0 \mod p$$

- Since $x^d - 1$ has exactly d roots mod p and since $a, a^2, \ldots, a^d$ gives d roots mod p, every root of x^d is congruent to a power of a
- Since every element of order d is a root of $x^d - 1$, every element of order d is a power of a
- But recall that

$$\text{ord}_p(a^j) = \frac{d}{(j, d)}$$

so that the only powers of a which have order d are the ones with $(j, d) = 1$
- Hence, there are $\varphi(d)$ powers of a that have order d
- Hence, there are $\varphi(d)$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ that have order d

- Recall: this tells us that there are $\varphi(p-1)$ primitive roots mod p!

3 The Existence of Primitive Roots

- We're not going to do much with this section
- It's worth stating the main result though:
- **Thm:** There is a primitive root modulo n if and only if one of the following holds true:
  1. $n = 2$
  2. $n = 4$
  3. $n = p^t$ for an odd prime p and $t \geqslant 1$
  4. $n = 2p^t$ for an odd prime p and $t \geqslant 1$
- How do you get there?
- First prove that primitive roots mod p are connected to primitive roots mod p^2: if r is a primitive root mod p, then all but one element of $\left(\mathbb{Z}/p^2\mathbb{Z}\right)$ which are congruent to r mod p are primitive roots mod p^2
- As a corollary, if r is a primitive root mod p, then either r or $r + p$ is a primitive root mod p^2
- Next, prove that if r is a primitive root mod p^2, then it's a primitive root mod p^k for $k \geqslant 2$
- Next, show that all of the above categories have primitive roots: only need to check the $2p^t$ case and it's possible to check that if r is a primitive root mod p^t and r is odd, then r is a primitive root mod $2p^t$. If r is a primitive root mod p^t and r is even, then $r + p^t$ is a primitive root mod p^t.
- For the other direction, check powers of 2 and show that 2^k when $k \geqslant 3$ does not have a primitive root because the order of every element is a divisor of $\varphi(2^k)/2$
- Finally, show that if there's a primitive root mod n, then n has to have one of the above forms
- Note that this gives us an algorithm for finding primitive roots:
  - Find a primitive root, r mod p (say, using the week 6 group work problem)
  - Lift that primitive root to a primitive root mod p^2 (either r or $r + p$ will work) and you get that it's a primitive root mod p^t for free

  - If $n = p^t$ you're done
  - If $n = 2p^t$ and your primitive root is odd, you're done
  - If $n = 2p^t$ and your primitive root is even, add p^t and you're done

- **Ex:** Find a primitive root modulo $2 \cdot 17^5$
  - First, find a primitive root modulo 17
  - We showed that 3 is a primitive root modulo 17 previously by checking the power of 2 powers of 3 ($3^1, 3^2, 3^4, 3^8$) and seeing that they were not 1 mod 17, so 3 must be a primitive root modulo 17
  - Next, check to see if 3 is a primitive root modulo 17^2
  - $\varphi(17^2) = 17 \cdot 16$
  - We need to check some extra powers of 3 mod 17^2: 3^{16}, 3^{17}, $3^{2\cdot 17}$, $3^{4\cdot 17}$, and $3^{8\cdot 17}$
  - Once we see that these are not 1 mod 17^2, we conclude that 3 is a primitive root mod 17^2
  - We now get for free that 3 is a primitive root mod 17^5
  - Since 3 is odd, 3 is still a primitive root mod $2 \cdot 17^5$

4 Discrete Logarithms and Index Arithmetic

4.1 Intro to definition

- In the real numbers, what does $\log_b(a)$ mean?
- Here are some questions to help you determine what $\log_b(a)$ should mean when working in modular arithmetic.
  - The following questions work modulo 9:
    * What should $\log_2(2)$ be?
    * What should $\log_2(4)$ be?
    * What should $\log_2(8)$ be?
    * What should $\log_2(7)$ be?
    * Can you come up with another reasonable answer to the previous question? What about a third answer? A fourth?
    * What should $\log_5(1)$ be?
    * What should $\log_5(5)$ be?
    * What should $\log_5(7)$ be?
    * What should $\log_7(7)$ be?
    * What should $\log_7(4)$ be?
    * What should $\log_7(5)$ be?
    * Why doesn't $\log_7(a)$ make sense as a function defined on $(\mathbb{Z}/9\mathbb{Z})^\times$?
  - Does there exist a base b so that $\log_b$ is a well-defined function on $(\mathbb{Z}/8\mathbb{Z})^\times$? If yes, give a table of values of $\log_b(n)$ for $n \in (\mathbb{Z}/8\mathbb{Z})^\times$. If no, why not?

4.2 Definition

- Let r be a primitive root modulo m. Then for any $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, there exists unique x so that $1 \leqslant x \leqslant \varphi(m)$ and $r^x \equiv a \mod m$. Define the index base r (or discrete logarithm base r) of a modulo m to be x. Denote this by $\mathrm{ind}_r(a)$.
- We like to reserve log for real numbers, so we stick with ind here.

- Since ind is essentially a log and since we explored properties in the beginning-of-the-section questions, you probably find the following proposition plausible
- **Thm:** Let m be a positive integer with primitive root r and let $a, b \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then
  1. $\text{ind}_r(1) \equiv 0 \mod \varphi(m)$
  2. $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \mod \varphi(m)$
  3. $\text{ind}_r(a^k) \equiv k\,\text{ind}_r(a) \mod \varphi(m)$
- Proof:
  - $\text{ind}_r(1) = \varphi(m)$
  - $r^{\text{ind}_r(ab)} \equiv ab \mod m$
  - Also, $r^{\text{ind}_r(a)+\text{ind}_r(b)} \equiv r^{\text{ind}_r(a)} \cdot r^{\text{ind}_r(b)} \equiv ab \mod m$
  - Since we then have that $r^{\text{ind}_r(ab)} \equiv r^{\text{ind}_r(a)+\text{ind}_r(b)} \mod m$, we conclude that $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \mod \varphi(m)$.
- **Ex:** Find all solutions of the congrunce $7x^3 \equiv 4 \mod 9$

$$\begin{aligned}
\text{ind}_2(7x^3) &\equiv \text{ind}_2(2) &\mod 6\\
\text{ind}_2(7) + 3\,\text{ind}_2(x) &\equiv 1 &\mod 6\\
4 + 3\,\text{ind}_2(x) &\equiv 1 &\mod 6\\
3\,\text{ind}_2(x) &\equiv 3 &\mod 6\\
\text{ind}_2(x) &\equiv 1 &\mod 2\\
\text{ind}_2(x) &\equiv 1, 3, 5 &\mod 6\\
x &\equiv 2^1, 2^3, 2^5 &\mod 9
\end{aligned}$$

4.3 Applications

- In general, computing $\text{ind}_r(a)$ is HARD
- Hard enough that the security of the ElGamal cryptosystem and Diffie-Hellman public key exchange rely on the difficulty of the problem

4.4 Power Residues

- More generally than our last example, we can talk about solving equations of the form $x^k \equiv a \mod m$
- Before we try to solve this, it's worth asking: is there a solution?
- For which a do there exist solutions to $x^k \equiv a \mod m$?
- We've already asked this for $k = 2$: this was the study of quadratic residues
- **Def:** Let m and k be positive integers and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then a is a kth power residue of m of there exists an $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ so that $x^k \equiv a \mod m$
- Recall Euler's Criterion: a is a quadratic residue mod p (prime) if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

- **Thm:** Let m be a positive integer with a primitive root. If k is a positive integer and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, then a is a kth power residue of m if and only if

$$a^{\varphi(m)/(k,\varphi(m))} \equiv 1 \mod m$$

  If there are solutions, then there are exactly $(k, \varphi(m))$ solutions.

- Proof:
  - Let r be a primitive root of m.
  - There is a solution to $x^k \equiv a \mod m$ if and only if there is a solution to $k\,\mathrm{ind}_r(x) \equiv \mathrm{ind}_r(a) \mod \varphi(m)$
  - Now this is a linear equation in the "variable" $\mathrm{ind}_r(x)$
  - It has solutions if and only if $(k, \varphi(m)) \mid \mathrm{ind}_r(a)$ and if it does, we get $(k, \varphi(m))$ solutions
  - But $(k, \varphi(m)) \mid \mathrm{ind}_r(a)$ if and only if $(\varphi(m)/(k, \varphi(m)))\,\mathrm{ind}_r(a) \equiv 0 \mod \varphi(m)$ which occurs if and only if $a^{\varphi(m)/(k,\varphi(m))} \equiv 1 \mod m$
  - We're done
- **Ex:** Is 5 a sixth power modulo 17? If so, how many solutions are there to $x^6 \equiv 5 \mod 17$?
  - To do this, compute $5^{16/(6,16)} \mod 17$
  - So we want $5^8 \mod 17$
  - Successively squaring gives

$$\begin{aligned} 5^2 &\equiv 25 \equiv 8 \mod 17 \\ 5^4 &\equiv 64 \equiv 13 \mod 17 \\ 5^8 &\equiv 169 \equiv 16 \mod 17 \end{aligned}$$

  - So 5 is not a 6th power residue
- Let p be an odd prime. Show that every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a pth power residue
  - Approach 1: Need to check $a^{\frac{p-1}{(p,p-1)}} \mod p$, but oh yeah, that's 1 by FLT, so check
  - Approach 2: $a^p \equiv a \mod p$, so a is a pth power residue.

5 Primality Tests Using Orders

6 Universal Exponents

6.1 Intro

- We've now seen a couple of things related to exponents and we can add a third complicating factor: universal exponents
- Here are some facts:
  - If $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, then $a^{\varphi(m)} \equiv 1 \mod m$
  - Every $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ has an order: that is, a least value of x so that $a^x \equiv 1 \mod m$. The order of a is a divisor of $\varphi(m)$
  - Sometimes, m has a primitive root: i.e. a base r so that the *smallest* positive x with $r^x \equiv 1 \mod m$ is $x = \varphi(m)$.
  - Sometimes, m doesn't have a primitive root.
- Let's visually explore what it means to have a primitive root:

x	1	2	3	4	5	6
1^x	1	1	1	1	1	1
2^x	2	4	8	7	5	1
4^x	4	7	1	4	7	1
5^x	5	7	8	4	2	1
7^x	7	4	1	7	4	1
8^x	8	1	8	1	8	1

x	1	2	3	4
1^x	1	1	1	1
3^x	3	1	3	1
5^x	5	1	5	1
7^x	5	1	5	1

- 9 has a primitive root, meaning that "the first time a column has all 1s is when you get to column $\varphi(9)$"
- 8 does not have a primitive root. It's not obvious that this is true, but this is the same as saying "the first time a column has all 1s is *before* you get to column $\varphi(8)$."
- In general, what is "the first column where you get all 1s?"
- Note that you get all 1s in column $\varphi(m)$ by Euler's Theorem
- Hence, by the well-ordering principle, there is a first column where you get all 1s.
- **Def:** Let m be a positive integer. A universal exponent of m is a positive integer U so that $a^U \equiv 1 \mod m$ for every $a \in (\mathbb{Z}/m\mathbb{Z})^\times$
- **Ex:** 4 is a universal exponent of 5
- **Ex:** 4 is a universal exponent of 10
- **Ex:** $\varphi(m)$ is a universal exponent of m
- **Ex:** $m = 600 = 2^3 \cdot 3 \cdot 5^2$
  - Since $\varphi(m) = 4 \cdot 2 \cdot 4 \cdot 5 = 160$, we know that for any $a \in (\mathbb{Z}/200\mathbb{Z})^\times$, we have $a^{160} \equiv 1 \mod 200$.
  - We can do better though
  - Note that $a^{\varphi(8)} \equiv 1 \mod 8$ and for any multiple of $\varphi(8)$, too
  - Also $a^{\varphi(3)} \equiv 1 \mod 3$ and for any multiple of $\varphi(3)$ too
  - Finally, $a^{\varphi(25)} \equiv 1 \mod 25$ and for any multiple of $\varphi(25)$ too
  - So if we could find a number U that is a multiple of 4, 2, and 20, then we would have $a^U \equiv 1 \mod 8, 3, 25$ and by Sun-Tsu, $a^U \equiv 1 \mod 600$
  - We could take $U = 4 \cdot 2 \cdot 20 = 160$, but that seems silly
  - Let's take $U = \operatorname{lcm}(4, 2, 20) = 20$. We now know that $a^{20} \equiv 1 \mod 600$
  - That's a far cry better
  - But maybe we can do better still?
  - Because we know that $a^2 \equiv 1 \mod 8$ for all $a \in (\mathbb{Z}/8\mathbb{Z})^\times$.
  - So we can actually take $U = \operatorname{lcm}(2, 2, 20) = 20$
  - Okay, so it didn't work that time, but it was worth a try.
- More generally, we want to find the minimal universal exponent modulo n. Denote this with $\lambda(n)$
- **Question:** When is $a^U \equiv 1 \mod n$ for all $a \in n$?
- If $n = p_1^{e_1} \cdots p_g^{e_g}$, then this happens if and only if $a^U \equiv 1 \mod p_i^{e_i}$ for all a and i.
- **Ex:** Show that if n has a primitive root, then $\lambda(n) = \varphi(n)$.
- As a result, $\lambda(p^t) = \varphi(p^t)$ when p is an *odd* prime
- Result from section 9.3 that we didn't really cover $\lambda(2^t) = 2^{t-2}$ when $t \geqslant 3$

- **Thm:** Suppose that $n \in \mathbb{Z}$ with $n > 1$. Factor n into primes as $n = 2^{e_0} p_1^{e_1} \cdots p_g^{e_g}$ where $p_1, \ldots, p_g$ are distinct odd primes, $e_0 \geqslant 0$, and $e_1, \ldots, e_g \geqslant 1$. Then the minimal universal exponent modulo n is $\lambda(n) = \operatorname{lcm}(\lambda(2^{e_0}), \varphi(p_1^{e_1}), \ldots, \varphi(p_g^{e_g}))$. Moreover, there exists an $a \in \mathbb{Z}$ so that $\operatorname{ord}_n(a) = \lambda(n)$.
- "Proof:"
  - Define $M = \operatorname{lcm}(\lambda(2^{e_0}), \varphi(p_1^{e_1}), \ldots, \varphi(p_g^{e_g}))$
  - Note that because M is a multiple of $\varphi(p_i^{e_i})$, we have $b^M \equiv 1 \mod p_i^{e_i}$ for all b and i
  - Hence, by Sun Tsu's theorem, $b^M \equiv 1 \mod n$ for all b
  - So M is a universal exponent
  - To show that M is the least universal exponent, we find an $a \in \mathbb{Z}$ with order M
  - First, find a primitive root r_i mod $p_i^{e_i}$ for each $p_1, \ldots, p_g$
  - Using Sun Tsu's theorem, solve the system

$$\begin{aligned} a &\equiv 5 \mod 2^{e_0} \\ a &\equiv r_1 \mod p_1^{e_1} \\ &\vdots \\ a &\equiv r_g \mod p_g^{e_g} \end{aligned}$$

  - Show that if $a^N \equiv 1 \mod n$, then $\lambda(p_i^{e_i}) \mid N$ for $0 \leqslant i \leqslant g$
  - Hence $M \mid N$
  - So the order of a must be M.
  - Also any universal exponent is a multiple of N
  - Hence, M is the minimal universal exponent.
- Remember those problems at the very beginning of 347 that were like "show that $n^5 - n$ is divisible by 5"?
- **Ex:** Show that any integer n not divisible by 2, 3, or 5 has $n^{12} - 1$ divisible by 180.
  - A universal exponent for $180 = 2^2 \cdot 3^2 \cdot 5$ is $\operatorname{lcm}(\lambda(4), \lambda(9), \lambda(5)) = \operatorname{lcm}(2, 6, 4) = 12$
  - Hence any $n \in (\mathbb{Z} / 180\mathbb{Z})^\times$ satisfies $n^{12} \equiv 1 \mod 180$, i.e. $n^{12} - 1$ is divisible by 180.