Math 3527 (Number Theory 1)

Lecture #26

Primitive Roots:

- Primitive Roots (In General)
- Primitive Roots in Finite Fields
- Primitive Roots in $\mathbb{Z}/m\mathbb{Z}$

This material represents §4.3.3 from the course notes.

Primitive Roots, I

The goal of this lecture is to discuss primitive roots in arbitrary rings, and to characterize the values of m for which there exists a primitive root modulo m.

Definition

If R is a commutative ring with 1 having finitely many units, an element $u \in R$ is a primitive root if every unit of R can be expressed as some power of u.

Equivalently, if there are n units in R, then an element is a primitive root precisely when its order is n.

Primitive Roots, II

<u>Examples</u>:

- If R is the ring $\mathbb{F}_2[x]$ modulo $x^2 + x + 1$, which we have previously established is a field, the elements $\overline{x}$ and $\overline{x+1}$ are primitive roots in R, since R has 3 units and each element has order 3 (their orders divide 3 by Euler's theorem, and neither element has order 1).
- If R is the ring $\mathbb{F}_3[x]$ modulo $x^2 + 1$, which is also a field, then the element $\overline{x+1}$ is a primitive root in R, since R has 8 units and $\overline{x+1}$ has order 8 (its order divides 8 by Euler's theorem, and $\overline{x+1}^4 = \overline{2}$ so its order does not divide 4).

Primitive Roots, III

Example: If R is the ring $\mathbb{F}_7[x]$ modulo x^2, show that the element $\overline{x+3}$ is a primitive root in R.

Primitive Roots, III

<u>Example</u>: If R is the ring $\mathbb{F}_7[x]$ modulo x^2, show that the element $\overline{x+3}$ is a primitive root in R.

- Note that R is not a field because x^2 is not irreducible.
- Indeed, the units in R are the elements that are relatively prime to x, which have the form $\overline{ax+b}$ where $b \neq 0$.
- To be a unit, there are 7 possible choices for a and 6 choices for b, so there are $7 \cdot 6 = 42$ total units in R.
- Thus to show $\overline{x+3}$ is a primitive root, we need to show it has order 42.
- By Euler's theorem, we know its order divides 42. Furthermore, by successive squaring, we can compute $\overline{x+3}^{21} = \overline{6}$, $\overline{x+3}^{14} = \overline{2}$, and $\overline{x+3}^{6} = \overline{2x+1}$.
- This means that the order of $\overline{x+3}$ cannot divide 21, 14, or 6, so it must be 42: it is therefore a primitive root.

Primitive Roots in Finite Fields, I

Our next goal is to prove that every finite field has a primitive root.

We first recall some basic properties of orders:

Proposition (Properties of Orders)

Suppose R is a commutative ring with 1 and u is a unit in R.

1. *If $u^n \equiv 1 \pmod{m}$ for some $n > 0$, then the order of u is finite and divides n.*
2. *If u has order k, then u^n has order $k/\gcd(n,k)$. In particular, if n and k are relatively prime, then u^n also has order k.*
3. *If $u^n \equiv 1 \pmod{m}$ and $u^{n/p} \not\equiv 1 \pmod{m}$ for any prime divisor p of n, then u has order n.*
4. *If u has order k and w has order l, where k and l are relatively prime, then uw has order kl.*

Proofs: The proofs are the same as in $\mathbb{Z}/m\mathbb{Z}$.

Primitive Roots in Finite Fields, II

We will first establish the following preliminary fact:

Proposition

Let R be a commutative ring with 1 having finitely many units. If M is the maximal order among all units in R, then the order of every unit divides M.

Proof:

- Suppose u has order M and let w be a unit of order k.
- If k does not divide M, there is some prime q which occurs to a higher power q^f in the factorization of k than the corresponding power q^e dividing M.
- Then u^{q^f} has order M/q^f while w^{k/q^e} has order q^e.
- Since these two orders are relatively prime, the element $u^{q^f} \cdot w^{k/q^e}$ has order $M \cdot q^{f-e}$, which is a contradiction because this is larger than M. Hence k divides M as claimed.

Primitive Roots in Finite Fields, III

Now we can prove our first main result:

Theorem (Primitive Roots in Finite Fields)

If F is a finite field, then F has a primitive root.

Our proof of the Theorem is nonconstructive: we will show the existence of a primitive root without explicitly finding one by exploiting unique factorization in the polynomial ring $F[x]$.

Primitive Roots in Finite Fields, IV

Proof:

- Suppose M is the maximal order among all units in F, and let $|F|$ denote the number of elements in F.
- Then by the finite-field version of Euler's theorem, we know that $M \leq |F| - 1$, since $a^{|F|-1} = 1$ in F for every unit $a \in F$.
- By our preliminary Proposition, all units in F then have order dividing M.
- This means that the polynomial $x^M - 1$ has $|F| - 1$ roots in F.
- But this is impossible unless $M \geq |F| - 1$, since a polynomial of degree M can only have at most M roots in F.
- Hence we conclude $M = |F| - 1$, meaning that some element has order $|F| - 1$: this element is a primitive root.

Primitive Roots Modulo p^d, I

By applying the Theorem in the particular case where $F = \mathbb{Z}/p\mathbb{Z}$, we obtain the following very important consequence:

Corollary (Primitive Roots Modulo p)

For any prime p, there exists a primitive root modulo p.

We can then use the existence of a primitive root modulo p to show that there exist primitive roots modulo powers of p:

Proposition (Primitive Roots Modulo p^2)

If a is a primitive root modulo p for p an odd prime, then a is a primitive root modulo p^2 if $a^{p-1} \not\equiv 1 \pmod{p^2}$. In the event that $a^{p-1} \equiv 1 \pmod{p^2}$, then $a + p$ is a primitive root modulo p^2.

Primitive Roots Modulo p^d, II

Proof:

- Since a is a primitive root modulo p, if the order of a mod p^2 is r, then since $a^r \equiv 1 \pmod{p^2}$ certainly implies $a^r \equiv 1 \pmod{p}$, we see that $p-1$ divides r.
- Since $\varphi(p^2) = p(p-1)$, there are two possibilities: the order of a modulo p^2 is $p-1$ or it is $p(p-1)$.
- The order of a modulo p^2 will be $p-1$ if and only if $a^{p-1} \equiv 1 \pmod{p^2}$. This gives the first statement.
- For the second statement, suppose that $a^{p-1} \equiv 1 \pmod{p^2}$.
- The binomial theorem implies $(a+p)^{p-1} \equiv a^{p-1} - p\,a^{p-2} \pmod{p^2}$, since the other terms all have a p^2 in them.
- Since $a^{p-1} \equiv 1 \pmod{p^2}$, we see that $a^{p-2} - p\,a^{p-2} \not\equiv 1 \pmod{p^2}$, because $p\,a^{p-2}$ is not divisible by p^2.
- Therefore, we see that $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$, so by the argument above, $a+p$ is a primitive root modulo p^2.

Primitive Roots Modulo p^d, III

Example: Find a primitive root modulo 11^2.

Primitive Roots Modulo p^d, III

Example: Find a primitive root modulo 11^2.

- Per the Proposition, first we find a primitive root modulo 11, and then we use it to construct a primitive root modulo 11^2.
- We claim 2 is a primitive root modulo 11: since the order of 2 must divide $\varphi(11) = 10$, and $2^2 \not\equiv 1 \pmod{11}$ and $2^5 \not\equiv 1 \pmod{11}$, the order divides neither 2 nor 5, hence must be 10.
- Now, to find a primitive root modulo 11^2, we simply compute $2^{10} = 1024 \equiv 56 \pmod{11^2}$.
- Since this is not congruent to 1 modulo 11^2, our Proposition dictates that 2 is also a primitive root modulo 11^2.

Primitive Roots Modulo p^d, IV

Now we look at primitive roots modulo p^d for larger d. It turns out that primitive roots here are essentially the same as primitive roots modulo p^2:

Proposition (Primitive Roots Modulo p^d)

If a is a primitive root modulo p^2 for p an odd prime, then a is a primitive root modulo p^d for all $d \geq 2$.

Example: Since 2 is a primitive root modulo 11^2 as we just showed, it is also a primitive root modulo 11^d for all $d \geq 2$. (In particular, it is a primitive root modulo, say, 11^{100}.)

Primitive Roots Modulo p^d, V

Proof: Induction on d (base case $d = 2$ is trivial).

- Suppose a is a primitive root modulo p^d and that it has order r modulo p^{d+1}: thus, $a^r \equiv 1 \pmod{p^{d+1}}$. Note that Euler's theorem implies that r divides $\varphi(p^{d+1}) = p^d(p-1)$.
- Since a is a primitive root modulo p^d we see that r is divisible by $\varphi(p^d) = p^{d-1}(p-1)$, so
- Thus, the only possibilities are $r = p^{d-1}(p-1)$ and $r = p^d(p-1)$: we just need to eliminate the first possibility.

Primitive Roots Modulo p^d, VI

Proof (continued):

- We want to show that a cannot have order $p^{d-1}(p-1)$.
- By Euler's theorem, $a^{p-1} \equiv 1 \pmod{p}$ so we can write $a^{p-1} = 1 + kp$ for some integer k.
- Then, since a is a primitive root modulo p^2, we also know that k is not divisible by p (as otherwise a would have order $p-1$ modulo p^2).
- Expanding with the binomial theorem yields $(a^{p-1})^{p^{d-1}} = (1+kp)^{p^{d-1}} = 1+p^{d-1} \cdot kp + p^{d+1} \cdot$[other terms]. But this is $\not\equiv 1$ modulo p^{d+1}, since k is not divisible by p.
- Hence $a^{p^{d-1}(p-1)} \not\equiv 1 \pmod{p^{d+1}}$, so a must have order $p^d(p-1) = \varphi(p^{d+1})$, meaning a is in fact a primitive root.

Primitive Roots Modulo p^d, VII

Example: Find a primitive root modulo 7^{2020}.

Primitive Roots Modulo p^d, VII

Example: Find a primitive root modulo 7^{2020}.

- Per our Propositions, we first find a primitive root modulo 7. Then we use it to construct a primitive root modulo 7^2, which will then also be a primitive root modulo 7^d for any $d \geq 2$ (and in particular, modulo 7^{2020}).
- Note that $2^3 \equiv 1 \pmod 7$, so 2 is not a primitive root.
- But $3^3 \equiv 6$ and $3^2 \equiv 2 \pmod 7$, so 3 is a primitive root.
- Furthermore, we can see that $3^6 \equiv 43 \pmod{49}$.
- Hence 3 is also a primitive root modulo 49, and therefore also modulo 7^{2020}, as required.

Primitive Roots Modulo m, I

Now that we have treated the case of odd prime powers, we can also easily handle one other case:

Proposition (Primitive Roots Modulo $2 \cdot p^d$)

If a is a primitive root modulo p^d for p an odd prime, then a is a primitive root modulo $2p^d$ if a is odd, and $a + p^d$ is a primitive root modulo $2p^d$ if a is even.

<u>Proof</u>:

- If a is odd, then $a, a^2, \dots, a^{\varphi(p^d)}$ are odd and distinct modulo p^d, so they remain invertible and distinct modulo $2p^d$.
- But since $\varphi(2p^d) = \varphi(p^d)$, the elements $a, a^2, \dots, a^{\varphi(p^d)}$ exhaust all of the distinct unit residue classes modulo $2p^d$.
- Thus, a is a primitive root modulo $2p^d$.
- If a is even, then $a + p^d$ is odd, and so by the argument above, we see $a + p^d$ is a primitive root modulo $2p^d$.

Primitive Roots Modulo m, II

Example: Find a primitive root modulo $2 \cdot 11^{100}$.

- From before, we know that 2 is a primitive root modulo 11^{100}. Since 2 is even, the Proposition implies that $2 + 11^{100}$ is a primitive root modulo $2 \cdot 11^{100}$.

Example: Find a primitive root modulo $2 \cdot 7^{2020}$.

- From before, we know that 3 is a primitive root modulo 7^{2020}. Since 3 is odd, the Proposition implies that 3 is also a primitive root modulo $2 \cdot 11^{100}$.

Primitive Roots Modulo m, III

By putting together all of our results, we can finish the characterization of the moduli that have primitive roots:

Theorem (Primitive Roots Modulo m)

There exists a primitive root modulo m if and only if $m = 1, 2, 4$, or $m = p^k$ or $2p^k$ for an odd prime p and some $k \geq 1$.

Primitive Roots Modulo m, III

By putting together all of our results, we can finish the characterization of the moduli that have primitive roots:

Theorem (Primitive Roots Modulo m)

There exists a primitive root modulo m if and only if $m = 1, 2, 4$, *or* $m = p^k$ *or* $2p^k$ *for an odd prime p and some* $k \geq 1$.

Examples:

- Since $27 = 3^3$ is an odd prime power, there is a primitive root modulo 27.
- Since $33 = 3 \cdot 11$ is not of the required form, there is no primitive root modulo 33.
- Since $64 = 2^6$ is not of the required form, there is no primitive root modulo 64.
- Since $2662 = 2 \cdot 11^3$ is twice an odd prime power, there is a primitive root modulo 2662.

Primitive Roots Modulo m, IV

We have already shown the existence of primitive roots in all of the listed cases except $m = 1, 2, 4$ (but these cases are trivial). All we have left to do is show that a primitive root cannot exist for other m. Before giving the proof, we establish a simple Lemma:

Lemma

If there exists a primitive root r modulo m, then the congruence $u^2 \equiv 1 \pmod{m}$ has only the two solutions $u = \pm 1 \pmod{m}$.

Proof:

- If $u^2 \equiv 1 \pmod{m}$ then u is a unit, so since r is a primitive root, we can write $u = r^d$ for some $0 \le d < \varphi(m)$.
- Then $u^2 \equiv r^{2d} \equiv 1 \bmod m$, so since r has order $\varphi(m)$ there are only two possible d, namely $d = 0$ and $d = \varphi(m)/2$.
- Thus there are only two possible u (namely $u = \pm 1$).

Primitive Roots Modulo m, V

Proof (of main Theorem):

- We will show that if m is not of the given form, then there are more than two solutions to $u^2 \equiv 1 \pmod{m}$, which by the Lemma will show that m cannot have a primitive root.
- First, suppose $m = 4p$ for some prime p (including $p = 2$). Then $x \equiv \pm 1$ and $x \equiv \pm(2p-1)$ have $x^2 \equiv 1 \pmod{4p}$.
- Second, suppose $m = pq$ for some distinct primes p and q: by the Chinese Remainder Theorem, there are four solutions to $x^2 \equiv 1 \pmod{pq}$, obtained by solving the congruences $x \equiv \pm 1 \pmod{p}$ and $x \equiv \pm 1 \pmod{q}$ simultaneously.
- To finish the argument, note that if r is a primitive root modulo m and $d|m$, then r is a primitive root modulo d.
- Running this backwards, we see that if m is divisible by $4p$ or by pq, then m has no primitive root.
- This encompasses all of our required cases, so we are done.

Primitive Roots Modulo m, VI

For completeness, we restate a result we showed previously about the number of primitive roots modulo m:

Proposition (Number of Primitive Roots)

If there exists a primitive root modulo m, then there are precisely $\varphi(\varphi(m))$ primitive roots modulo m.

Proof:

- Suppose that there is a primitive root u modulo m.
- The units modulo m are represented by $u^1, \ldots, u^{\varphi(m)}$, so it suffices to determine which of these have order $\varphi(m)$.
- Since the order of u^k is $\varphi(m)/\gcd(k, \varphi(m))$, we see that u^k is a primitive root if and only if k is relatively prime to $\varphi(m)$.
- There are $\varphi(\varphi(m))$ such k, so there are $\varphi(\varphi(m))$ primitive roots modulo m.

Primitive Roots Modulo m, VII

Examples:

- The number of primitive roots modulo 41 is equal to $\varphi(\varphi(41)) = 16$ since 41 is a prime number, hence there are primitive roots mod 41.
- The number of primitive roots modulo 23^{2020} is equal to $\varphi(\varphi(23^{2020}) = 10 \cdot 22 \cdot 23^{2018}$, since 23^{2020} is an odd prime power.
- The number of primitive roots modulo 2662 is equal to $\varphi(\varphi(2662)) = 440$ since $2662 = 2 \cdot 11^3$ is twice an odd prime power, hence there are primitive roots mod 2662.
- The number of primitive roots modulo 24^{2020} is equal to 0, because $24^{2020} = 2^{6060}3^{2020}$ is not of the correct form.

Summary

We gave a general definition of a primitive root in a ring and proved that every finite field has a primitive root.

We discussed primitive roots modulo powers of primes, and gave procedures for finding primitive roots modulo p^d and $2p^d$.

We proved that there is a primitive root in $\mathbb{Z}/m\mathbb{Z}$ if and only if $m = 1, 2, 4$, or $m = p^k$ or $2p^k$ for an odd prime p and some $k \geq 1$.

Next lecture: Modular Arithmetic in $\mathbb{Z}[i]$.