# MATH 115, SUMMER 2012
# LECTURE 13

JAMES MCIVOR

Today we focus on the multiplicative aspects of the integers mod $p$.

## 1. Primitive roots in $\mathbb{Z}/m$

For this section, we work in the ring $\mathbb{Z}/m$, so "=" in this ring means congruent mod $m$ in integers. We are interested in a special type of unit, namely when $a^k = 1$. We make some preliminary observations:

- If $(a, m) \neq 1$, then $a^k \neq 1$ unless $k = 0$.
- So from now on consider $(a, m) = 1$; then $a$ is a unit, as we have seen before.
- For some $k \geq 0$, we must have $a^k = 1$. Reason: look at sequence $a, a^2, a^3 \ldots$. The ring is finte, so it repeats somewhere, say $a^m = a^n$, with $m < n$. Then set $k = n - m$, and we have $a^k = 1$.
- We might ask, when is the first point in that sequence that we get 1? That's called the order of $a$:

**Definition 1.** The **order** of the unit $a \in \mathbb{Z}/m$ is the smallest positive $h$ such that $a^h = 1$.

- Note, in some rings, units may have infinite order, but not in $\mathbb{Z}/m$ (or any finite ring).

**Proposition 1.** *If $a$ has order $h$, and $k$ is any positive integer, then $a^k = 1$ if and only if $h|k$.*

*Proof.* - Pick any $k > 0$ If $k < h$, then $a^k \neq 1$ by def of order
- divide: $k = hq + r$, with $0 \leq r < h$
- then $a^k = a^{hq+r} = (a^h)^q \cdot a^r = 1 \cdot a^r$.
- so $a^k = 1$ iff $a^r = 1$ iff $r = 0$, second iff because $r < h$ and def of order

□

**Proposition 2.** *The order of any unit in $\mathbb{Z}/m$ divides $\phi(m)$.*

- this follows from the previous one by Euler's lemma: $a^{\phi(m)} = 1$ so $h|\phi(m)$.

Is the order of a product the product of the orders of the factors? only when the two orders are coprime

**Proposition 3.** *If $a, b \in \mathbb{Z}/m$ have orders $g, h$, respectively, and $g$ and $h$ are coprime, then the order of $ab$ is $gh$.*

*Proof.* - let $r =$ order of $ab$. Since $(ab)^{gh} = 1$, we know $r|gh$. Want: $gh|r$
- since $(g, h) = 1$, enough to show $g|r$ and $h|r$ separately
- since $(g, h) = 1$, $g|r$ will follow from $g|hr$.
- but $a^{hr} = a^{hr}b^{hr}$ since $b^{hr} = (b^h)^r = 1$. this is equal to $(ab)^{hr} = ((ab)^r)^h = 1$.
- this shows $a^{hr} = 1$, so $g|hr$. Similarly for $b$. □

**Definition 2.** If $a$ is a unit in $\mathbb{Z}/m$, then it has a finite order $h$, which is a divisor of $\phi(m)$. If it's actually equal to $\phi(m)$, we call $a$ a **primitive root modulo** $m$.

You may remember we used this in the proof of Wilson's theorem. The useful fact for us there was: if $a$ is a primitive root mod $m$, then $\{a, a^2, \ldots, a^h\}$ forms a reduced residue system mod $m$.

**Example 1.1.** - 1 is never a primitive root
- mod 5, 2 and 3 are primitive roots, but 4 is not.
- mod 8, there are NO primitive roots!

So when can we find a primitive root? The answer is known exactly, and is in your book. For us, we'll only use that there are primitive roots for a prime modulus.

Before reading the proof, recall from last time (problem session) that we showed $x^k \equiv 1 \mod p$ has exactly $k$ solutions if $k|p-1$.

**Theorem 1.** *If $p$ is a prime, there are $\phi(p-1)$ primitive roots mod $p$.*

*Proof.* - To be a primitive root, must have order $p-1$.
- Factor $p-1 = \prod q^\alpha$
——— Step 1 ———
- for each $q^\alpha$, how many elements of $\mathbb{Z}/p$ with that order?
- Answer: $q^\alpha - q^{\alpha-1}$.
- reason: since $q^\alpha | p-1$, there are exactly $q^\alpha$ solutions of $x^{q^\alpha} \equiv 1$ ( problem session last time)
- also, $q^{\alpha-1}|p-1$, so there are $q^{\alpha-1}$ solutions of $x^{q^{\alpha-1}} \equiv 1$.
- to have order $q^\alpha$, you must be a solution of the first congruence, but not the second.
- so there are $q^\alpha - q^{\alpha-1}$ elements of order $q^\alpha$
——— Step 2 ———
Now we produce at least one primitive root.
- For each prime $q_i$ in the factorization, can find an element $a_1$ of order $q_i^{\alpha_i}$, by step 1.
- look at these $a_i$'s - their orders are pairwise prime, so by Prop 3, their orders multiply when we take their product.
- Thus the element $a_1 \cdots a_r$ has order $q_1^{\alpha_1} \cdots q_r^{\alpha_r} = p-1$, so it's a primitive root.
——— Step 3 ———
Now we count the exact number of primitive roots.

First notice the following lemma: If $a$ has order $h$, and $(h,k) = m$, then $a^k$ has order $h/m$. In English, when you take a power, the new order is the old order divided by gcd(old order, power).
- reason: $(a^k)^n \equiv 1$ iff $h|kn$ iff $\frac{h}{m}|\frac{k}{m}n$ iff $\frac{h}{m}|n$. The smallest $n$ for which this holds is $\frac{h}{m}$ itself.
- Now we count the primitive roots. There is one, call it $g$, by step 2. By def of primitive root, $\{g, g^2, \ldots, g^{p-1}\}$ is a reduced residue system. For each of these elements $g^k$, it has order $p-1/(k, p-1)$, by the above lemma. So the order of $g^k$ is $p-1$ iff $(k, p-1) = 1$. There are $\phi(p-1)$ such numbers $k$.

□

Our interest will primarily be in prime modulus congruences, so the above result is good enough. But we saw at the beginning that there are some moduli for which there is NO primitive root (8 was our example).

In conclusion, you may find it interesting that only certain moduli have primitive roots:

**Theorem 2.** *The only numbers $m$ for which there is a primitive root mod $m$ are $m = 1, 2, 4$, or $m = p^\alpha$ or $2p^\alpha$, where $\alpha \geq 1$ and $p$ is an odd prime.*

*Proof.* If interested, see the end of 2.8 in your book. We will prove two of the preliminary results, including Euler's criterion, tomorrow. □

**Algebraic Interpretation:** (for those who've seen groups before) For any $m > 1$, the set of units in $\mathbb{Z}/m$ forms a group under multiplication. If there is a primitive root $g$ mod $m$, then this group of units is cyclic, with $g$ as a generator. In particular, we see that the group of nonzero elements of the field $\mathbb{Z}/p$ ($p$ prime) is a cyclic group. This is true for any finite field (there are others besides $\mathbb{Z}/p$), but not true, say for infinite fields such as $\mathbb{Q}$ or $\mathbb{R}$.

## Problem Session

(1) (NZM 2.8.7) Let $p > 2$ be prime. How many solutions to $x^{p-1} \equiv 1 \mod p$? To $x^{p-1} \equiv 2 \mod p$?

**Solution:** Solutions to $x^{p-1} \equiv 1$ are elements whose order divides $p-1$. Since $\phi(p) = p - 1$, the order of every (nonzero) element divides $p - 1$, so every unit works, giving $p - 1$ solutions. Since every element satisfies $x^{p-1} \equiv 1$, no element satisfies $x^{p-1} \equiv 2$, because $1 \not\equiv 2$.

(2) (NZM 2.8.9) Show that $3^8 \equiv -1 \mod 17$. Explain why this implies that 3 is a primitive root mod 17.

**Solution**: Note that the inverse of 3 mod 17 is 6, so the given congruece is the same as $3^5 \equiv -6^3 \mod 17$, which says $243 \equiv -216 \mod 17$. This can be checked directly. Now consider the order of 3 mod 17. It must divide $\phi(17) = 16$. So it can only be 2,4,8,16. If it's 2 or 4 or 8, this contradicts the first part. So 3 has order 16, hence is a primitive root mod 17.

(3) (NZM 2.8.18) Show that if $g$ and $g'$ are primitive roots mod $p$, then $gg'$ is not.

**Solution:** This is like a HW problem from last week. product of all $g^k$s $\equiv$ product of all $g'^k$s $\equiv -1$ by Wilson. But product of $(gg')^k$s is then $\equiv (-1)^2 = 1$, wheras if $gg'$) was a primitive root, product of $(gg')^k$s would be $\equiv -1$.

**Definition 3.** A composite number $m$ is a **Carmichael number** if for all units $a$ in $\mathbb{Z}/m$, we have $a^{m-1} \equiv 1 \mod m$.

Fermat's little theorem shows that every prime has this property. But the converse of FLT is not true, so there are also some composite numbers $m$ with $a^{m-1} \equiv 1 \mod m$. These Carmichael numbers are "almost primes".

(4) Prove that $m$ is a Carmichael number if and only if $m$ is squarefree (which means $m = p_1 \cdots p_r$, with the $p_i$ all *distinct* primes), and $p_i - 1 | m - 1$ for each $p_i$.

- easier direction: "$m$ squarefree and for each $p|m$, we have $p-1|m-1$" implies "$m$ is a Carmichael number"

- harder direction: "$m$ is a Carmichael number" implies "$m$ squarefree and for each $p|m$, we have $p - 1|m - 1$"

[Hint for 'Carmichael implies squarefree and...": factor $n$ into prime powers, then choose a primitive root for each prime power. Apply the CRT.]

**Solution:** First the "if": Suppose $m$ is as above. We have to show that for each $0 < a < m$ with $(a, m) = 1$, we have $a^{m-1} \equiv 1 \mod m$. We know $a^{p_i - 1} \equiv 1 \mod p_i$ for each $i$ by FLT. Since $p_i - 1 | m - 1$, we have also $a^{m-1} \equiv 1 \mod p_i$. So each $p_i$ divides $a^{m-1} - 1$, hence so does $m$.

The "only if" direction: suppose $m$ is a Carmichael number. $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ for some primes $p_i$. Choose a primitive root $a_i$ for each prime power $p_i^{\alpha_i}$ (this is possible by the final theorem of the lecture, though we didn't prove it). Each $a_i$ must be prime to $p_i$ because $a_i$ is a unit mod $p_i^{\alpha_i}$, but if $p_i | a_i$, then $p_i^{\alpha_i} | a_i^{\alpha_i}$, so $a_i^{\alpha_i} \equiv 0 \mod p_i^{\alpha_i}$, and this is impossible for units. Now we have these elements $a_i \mod p_i^{\alpha_i}$, and we use CRT to construct $a \mod n$ (note the $p_i^{\alpha_i}$ are pairwise coprime) such that $a \equiv a_i \mod p_i^{\alpha_i}$. Moreover, each $p_i \nmid a$, since $a \equiv a_i \mod p_i^{\alpha_i}$, so $a \equiv a_i \mod p_i$, and $(a_i, p_i) = 1$. Thus since $(a, n) = 1$, $a^{n-1} \equiv 1 \mod n$ since $n$ is a Carmichael number. Then $a^{n-1} \equiv 1 \mod p_i^{\alpha_i}$, too, so $a_i^{n-1} \equiv 1 \mod p_i^{\alpha_i}$, hence $\phi(p_i^{\alpha_i}) | n - 1$. But $\phi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i - 1}(p_i - 1)$, so we have

$$p_i^{\alpha_i - 1}(p_i - 1) | n - 1$$

Now $p_i^{\alpha_i}$ and $p_i - 1$ are coprime, so this means that they both divide $n - 1$. So $p_i - 1 | n - 1$. But also, $p_i^{\alpha_i - 1}$ can't divide $n - 1$ since $p_i$ doesn't, so $\alpha_i = 1$.