

COMMENTS ON CHAPTER 9

March 17, 2008

This chapter is all about the set $U(R)$ of units of a commutative ring R . The main focus is on the set $U(\mathbb{Z}/m\mathbb{Z})$. This set consists of the units (also called “invertible elements”) of $\mathbb{Z}/m\mathbb{Z}$. Any general statement about $U(R)$ applies, in particular, to $U(\mathbb{Z}/m\mathbb{Z})$, since $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring. It is important to realize that $U(R)$ is closed under multiplication. Also, the inverse of each element in $U(R)$ is again in $U(R)$. (In fact, $U(R)$ is a *group*, but in this course we won’t study groups *per se*, so we have no need for the additional terminology here.) Here is a summary of the main results we have proved:

Theorem 1. *Suppose R is a commutative ring with exactly n units. Then $u^n = 1$ for each $u \in U(R)$.*

How does this general result play out with respect to $\mathbb{Z}/m\mathbb{Z}$? We assume always that $m \geq 1$. (The case $m = 1$ is exceptionally boring, but there’s no need to exclude it.) First of all, a congruence class $[a]_m$ has an inverse (that is, $[a]_m$ is in $U(\mathbb{Z}/m\mathbb{Z})$) if and only if $\text{GCD}(a, m) = 1$. For example,

$$U(\mathbb{Z}/15\mathbb{Z}) = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}.$$

More succinctly, $U/15\mathbb{Z} = \{\pm 1, \pm 2, \pm 4, \pm 7\}$. Since $\mathbb{Z}/15\mathbb{Z}$ has exactly 8 units, Theorem 1 guarantees that $u^8 = 1$ for every $u \in U(\mathbb{Z}/15\mathbb{Z})$.

The number of units of $\mathbb{Z}/m\mathbb{Z}$ is equal to the number of positive integers $a \leq m$ such that $\text{GCD}(a, m) = 1$. This number is called *Euler’s phi function* and is denoted by $\varphi(m)$. We know, for example, that $\varphi(p) = p - 1$ if p is a prime number. As a special case of Theorem 1 we have the following:

Corollary 2. *Let m be a positive integer, and let $u \in U(\mathbb{Z}/m\mathbb{Z})$. Then $u^{\varphi(m)} = [1]_m$.*

In terms of congruences, Corollary 2 says this:

Euler’s Theorem. *Let m be a positive integer, and let a be any integer such that $\text{GCD}(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

In the special case of a prime number, we get:

Fermat’s Theorem. *Let p be a prime number, and let a be any integer such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

In class, we proved the following important corollary:

Corollary to Fermat's Theorem. *Let p be a prime number, and let a be any integer. Then $a^p \equiv a \pmod{p}$.*

Proof. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$, by Fermat's Theorem; multiply both sides by a to get the desired formula. If $p \mid a$, then $a^p \equiv 0 \equiv a \pmod{p}$. Thus it's true in either case.

In Chapter 12 we will find out how to evaluate $\varphi(m)$ for large values of m . At this point, we can easily compute the number of units modulo a power of a prime. First, let's look at an example, say, $125 = 5^3$. The numbers on the list $1, 2, 3, \dots, 125$ that are *not* relatively prime to 125 are the multiples of 5, that is $5, 10, 15, 20, \dots, 125$. There are 25 multiples of 5 between 1 and 125. Therefore $\varphi(125) = 125 - 25 = 100$.

Proposition 3. *Suppose p is a prime number and m is a positive integer. Then $\varphi(p^m) = p^{m-1}(p - 1)$.*

Proof. On the list of integers $1, 2, \dots, p^m$, we have to throw out the ones that are *not* relatively prime to p^m . These are exactly the integers that are multiples of p , and there are exactly p^{m-1} of them, namely, $1 \cdot p, 2 \cdot p, \dots, p^{m-1} \cdot p$. Therefore the number of *non-units* is p^{m-1} , so the number of units is $p^m - p^{m-1}$, which equals $p^{m-1}(p - 1)$.

The order of a unit. Let R be a commutative ring, and let $u \in U(R)$. Assume that $U(R)$ is finite. Then we know, by Theorem 1, that there is a positive integer n such that $u^n = 1$. (For example, if $R = \mathbb{Z}/m\mathbb{Z}$ we can take $n = \varphi(m)$.) Of course, there may be a *smaller* positive integer q such that $u^q = 1$. For example, in $U(\mathbb{Z}/15\mathbb{Z})$, $(-1)^2 = 1$ and $2^4 = 1$. (In fact, it's not hard to see that $u^4 = 1$ for every $u \in U(\mathbb{Z}/15\mathbb{Z})$.) The *order* of an element of $U(R)$ is the *smallest* positive integer q such that $u^q = 1$. In the special case (the main case of interest) where $R = \mathbb{Z}/m\mathbb{Z}$, we call this number q the *order of u modulo m* . Here are the orders of the elements of $U(\mathbb{Z}/15\mathbb{Z})$.

$u :$	1	2	4	7	8	11	13	14
order of $u :$	1	4	2	4	4	2	4	2

The next two results are very useful in computing the order of a unit of $\mathbb{Z}/m\mathbb{Z}$.

Proposition 4. *Let R be a commutative ring, let $u \in U(R)$, and let n be a positive integer. If $u^n = 1$, then the order of u is a divisor of n .*

We proved this in class, using the division algorithm, exactly as in the proof, in the book, of Proposition 2 on page 137.

Corollary 5. *Let $m \geq 1$, and let u be any integer such that $\text{GCD}(u, m) = 1$. Then the order of u modulo m is a divisor of $\varphi(m)$.*

For example, let's compute the order of 32 modulo 125. We know that the order has to be a divisor of $\varphi(125) = 100$. It makes sense to try exponents that are divisors of 100. Working in $\mathbb{Z}/125\mathbb{Z}$ (bravely omitting brackets and foolishly refusing to use a calculator), we note that $32^2 = 1024 = 24$, so $32^4 = 24^2 = 576 = 76 = -49$. Next, working toward 32^{10} , we compute $32^8 = (-49)^2 = (1 - 50)^2 = 1 - 100 + 50^2 = -99 = 26$. Now $32^{10} = 32^2 \cdot 32^8 = 24 \cdot 26 = (25 - 1)(25 + 1) = 25^2 - 1 = -1$. Finally,

$32^{20} = (-1)^2 = 1$. Now we know that the order of 32 is a divisor of 20, so it has to be on the list 1, 2, 4, 5, 10, 20. We have already observed that $32^4 \neq 1$ and $32^{10} \neq 1$, so the order of 32 cannot be a divisor of either 4 or 10. This rules out 1, 2, 4, 5 and 10, so the order of 32 is 20.

Playing fast and loose with exponents (pardon the bad grammar). Suppose R is a commutative ring, $u \in U(R)$ and n is a positive integer. We define $u^n = u \cdot u \cdot \dots \cdot u$ (n times). Also, by definition, $u^{-n} = (u^n)^{-1}$ and $u^0 = 1$. Thus u^m is defined for every integer m , positive, negative or zero. The following laws of exponents, familiar in the context of real numbers, are valid:

- Let $u \in U(R)$, and let m and n be arbitrary integers. Then the following equations are valid:

$$u^{m+n} = u^m u^n$$

$$u^{m-n} = u^m \cdot (u^n)^{-1}$$

$$(u^m)^n = u^{(mn)}$$

- Let $u, v \in U(R)$, and let m be any integer. Then $u^m v^m = (uv)^m$.

The proofs of these are too boring to be done in public, but feel free to use these equations whenever they are useful. (The last equation, involving u and v , actually requires commutativity. The others do not, since an element always commutes with all of its powers.)

The order of a power of a unit. In many situations we know the order of u , and we want to use this knowledge to figure out the order of u^d . We use the following very important result (Proposition 3 on page 137 of the book):

Theorem 6. *Let u be a unit of a commutative ring R , and suppose that u has order n . Then, for every integer d , the order of u^d is $\frac{n}{\text{GCD}(n,d)}$. In particular, the order of u^d is always a divisor of the order of u .*

We proved this in class. Note that d can be a negative integer. In fact, it is easy to see that u and u^{-1} have the same order. For example, u^{-37} and u^{37} have the same order. Thus negative exponents don't really matter much in these considerations.

Let's use this information to compute the orders of some units of $\mathbb{Z}/125\mathbb{Z}$, starting with the fact that 32 has order 20, as shown above.

- The order of 32^2 is $\frac{20}{\text{GCD}(20,2)} = \frac{20}{2} = 10$.
- The order of 32^3 is $\frac{20}{\text{GCD}(20,3)} = \frac{20}{1} = 20$.
- The order of 32^5 is $\frac{20}{\text{GCD}(20,5)} = \frac{20}{5} = 4$. We can work "backwards" too, to figure out, for example, the order of 2. Let n denote the order of 2. By Theorem 6, the order of 2^5 is a divisor of the order of 2. Since $2^5 = 32$, and since we know that 32 has order 20, we see that $20 \mid n$. Of course $n \mid 100$, by Corollary 5. Therefore the order of 2 has to be either 20 or 100. If it were 20, then $32^4 = (2^5)^4 = 2^{20} = 1$, which is false. Therefore the order of 2 is 100.

Here's another little tidbit that we proved in class:

Proposition 7. *Let R be a commutative ring with exactly n units. If u is a unit of order n , then the list $1, u, u^2, \dots, u^{n-1}$ is a list of all units of R (with no repetitions). Conversely, if v is any element such that the list $1, v, v^2, \dots, v^{n-1}$ is a list of all units of R , with no repetitions, then v has order n .*

Well, maybe we didn't prove the "Conversely" statement, so let's do that now. Since there are no repetitions, and since 1 is on the list, we know that v^1, v^2, \dots, v^{n-1} are all different from 1. Since $v^n = 1$ by Theorem 1, we see that the order of v is exactly n .

For example, since we showed that 2 has order 100 modulo 125, we know that $1, 2, 2^2, \dots, 2^{99}$ is a list of all 100 units of $\mathbb{Z}/125\mathbb{Z}$. Then, using Theorem 5, we can easily read off the order of *every* element of $U(\mathbb{Z}/125\mathbb{Z})$. Suppose, for example, that we want an element u of order 5. We can take $u = 2^{20} = 32^4 = -49$.

Warning. You can't always find an element like the element u in $U(\mathbb{Z}/m\mathbb{Z})$, whose powers run through all of the units. For example, there is no such element in $\mathbb{Z}/15\mathbb{Z}$, since every element has order 1, 2 or 4.

Comments on the exercises. Be sure that you know how to do *all* of the problems in Sections 9A and 9B. Most of them are quite straightforward adaptations of examples we have worked in class. Here are comments on a few:

9A: The correct answer to E4 (v) is something like "2 is not a unit modulo 1, so it does not have an order."

In E4, since you know, from E3 (i), that 2 has order 10, every unit of $\mathbb{Z}/11\mathbb{Z}$ occurs on the list $1, 2, 2^2, 2^3, \dots, 2^9$. Then use Theorem 6 to get the order of *each* of the 10 units.

E8: Of course you must assume that $\text{GCD}(a, r) = 1$ and $\text{GCD}(a, s) = 1$, or else the problem does not make sense. Let f be the least common multiple of d and e . You have to show (i) $a^f \equiv 1 \pmod{m}$; and (ii) if $1 \leq t < f$ then $a^t \not\equiv 1 \pmod{m}$. Showing (i) is easy (and it's something you have done several times already). To verify (ii), suppose that $a^t \equiv 1 \pmod{m}$ and look for a contradiction. Then $a^t \equiv 1 \pmod{r}$ (Why?), so by Proposition 3 $d \mid t$. Similarly, $e \mid t$. Now use the fact, proved in class, that the least common multiple of two integers is a divisor of *every* common multiple of the two integers. Finish the problem.

E12: Proposition 3 (in the book) gives you a formula for the order of a^f , and you know that this order is 1 (since the order of 1 is 1 (duh!)). Now what?

E16: You are trying to show that $n \equiv -1 \pmod{41}$. Go back to basics. What does it mean to say that $n^2 \equiv 1 \pmod{41}$? By the way, 41 is prime; this should be helpful.

E18: 97 is prime. (Trust me.) What is $\varphi(97)$?

9B: E1 and E2 are silly problems. The smart-alecky (and perfectly correct) answer is: "They are true because Fermat's Theorem is true." There's no reason to run through the list to see that Fermat's Theorem gives the correct answer in a specific situation, since it has been proved in complete generality. These are not problems; they are suggestions for you to work on your own, in order to see how Fermat's Theorem plays out in a specific situation. This is, in fact, a useful thing to do.

E3: I think what is intended is something like this (in the case $p = 11$): $2^{10} = 1$, so $2^{-1} = 2^{10}2^{-1} = 2^{10-1} = 2^9 = 2^5 \cdot 2^4 = (-1) \cdot 16 = -5 = 6$. The verification is

that $2 \cdot 6 = 12 = 1$. I leave it to you to decide whether or not Fermat's Theorem is actually useful in finding the inverse of a unit, when the modulus is reasonably small. My opinion is "no".

E7: This is the Corollary to Fermat's Theorem. Feel free to use this result on the other exercises.

E8: We did this in class, using the Corollary to Fermat's Theorem.

E12: The expression equals $\frac{3n^5+5n^3+7n}{15}$, and your mission is to show that this is an integer. That is, you must show that $3n^5 + 5n^3 + 7n \equiv 0 \pmod{15}$.

E17: In addition to the hint in the back of the book, use the fact in the penultimate sentence of the comment on E8.

E18: The commas before "hence" in (ii) and (iii) should be semicolons (at least according to the rules of grammar and punctuation that I learned in the 1950's).