UCLA Mathematics 110A: selected solutions from homework #1

David Wihr Taylor

July 2, 2010

Introduction

When reading these solutions always keep in mind the common techniques being used. The point of homework, and subsequently these solutions, is to give you experience and competence in *solving* abstract algebra problems *on your own*! By this point you all have the capacity to memorize algorithms and the statements of theorema. However developing both an understanding of what a subject really means and how one can use it requires a more specialized type of effort. You must practice *problem solving* and also try to *abstract*, that is find the general themes inherent in, your solutions. I'll try to make my own ideas and strategies clear in the solutions that follow.

1 Problems from Section 1.1

The main result of this section is theorem 1.1. This is the familiar division algorithm that we all learn in grade school. You probably just memorized this many years ago and never gave much thought as to why it works. The main technical tool in its proof is to use the fact that every nonempty subset of the integers, which is bounded below has a *smallest* element.

1.1 Problem 1.1.7:

Claim: Let n be a positive integer. Prove that a and c leave the same remainder when divided by n if and only if $a - c = nk$ for some integer k.

Proof: We're proving an if and only if statement here, so we're going to have to write two arguments:

$\Rightarrow$ If a and c leave the same remainder when divided by n, then $a - c = nk$ for some integer k.

$\Leftarrow$ If $a - c = nk$ for some integer k, then a and c leave the same remainder when divided by n.

Remember, we only have theorem 1.1 and its corollary to work with, so we'll have to pay close attention to what it really says at each step of our proof.

$\Rightarrow$: Since we assume that a and c leave the same remainder when divided by n we can use the division algorithm to write

$$a = pn + r \qquad \text{and} \qquad b = qn + r \tag{1}$$

for integers $p, q, r \in \mathbb{Z}$. The we can compute the difference $a - c$ by using equations (1):

$$\begin{aligned} a - c &= pn + r - (qn + r) \\ &= (p - q)n \\ &= kn \end{aligned}$$

where we've let $n := p - q$. This is what we wanted to show, so we're finished with this part of the problem.

$\Leftarrow$: We're given that $a - c = nk$. We only have the division algorithm at our disposal, so let's write what it says about a and c:

$$a = pn + r \qquad \text{and} \qquad b = qn + s \tag{2}$$

for integers $p, q, r, s \in \mathbb{Z}$.

Now that we've done this let's form the expression $a - c$ and substitute equations (2) to see if the division algorithm says anything more about our situation.

$$\begin{aligned} a - c &= pn + r - (qn + r) \\ &= (p - q)n + (r - s) \end{aligned}$$

Since $n|(a - c)$ and $n|n(p - q)$ we have that $n|(r - s)$. That is, $r - s = \alpha n$ for some integer α. Finally we note that the division algorithm says that $0 \leq r, s < n$. Thus we have that

$$-n < r - s < n \qquad \text{and} \qquad r - s = \alpha n. \tag{3}$$

The only multiple of n between $-n$ and n is $0n$, namely the integer 0. Thus $r - s = 0$, or just $r = s$. We're done now because we've shown that a and c have the same remainder when divided by n.
□

2 Problems from Section 1.2

The new idea in this section is the notion of the greatest common divisor (g.c.d) of two integers a and b. The g.c.d. of a and b is denoted by the symbol (a, b). The powerful theorem 1.3 tells us that we can write the g.c.d of a and b in the useful form,

$$(a, b) = au + vb$$

for some integers u, v, with (a, b) being the smallest such positive linear combination. There are two main ideas in the proof. The first is that the set of all linear combinations of a and b has a positive element, and thus by the "well ordering axiom" for the integers, there must be a smallest positive linear combination, t. Then one applies the division algorithm to a divided by t and b divided by t successively and finds that t must be a common divisor. Then one shows that any other common divisor of a and b must divide t. Hence $t = (a, b)$.

Using this theorem there are several corollaries and theorems.

Finally, the section leads up to the Euclidean algorithm. This gives you a way to actually find the g.c.d. of two numbers. Furthermore the Euclidean algorithm actually gives you the u and v used in theorem 1.3.

2.1 Problem 1.2.26:

Claim: Let $a, b, c \in \mathbb{Z}$. The equation $ax + by = c$ has an integer solution if and only if $(a, b)|c$.

Proof: We proceed in two steps as before, proving first the "if" ($\Leftarrow$) and then the "only if" ($\Rightarrow$) parts of the above statement.

$\Rightarrow$: Supposing $ax + by = c$ has an integer solution, we recall the fact that $d := (a, b)$ divides both a and b. Thus it divides c. This is what we wanted to show!

$\Leftarrow$: Supposing the $d := (a, b)$ divides c we'd like to show that there are x and y in $\mathbb{Z}$ which solves the equation. Here we should do one of the few things possible given the information in the section: we should write $d = au + bv$, as given by theorem 1.3. Then since $c = \alpha d$ (because d divides c) we may write

$$c = a(\alpha u) + b(\alpha v)$$

. If we let $x = \alpha u$ and $y = \alpha v$ we're done.
□

2.2 Problem 1.2.36:

Claim: For every integer n, $(n+1, n^2 - n + 1) = 1$ or 3.

Proof: Here we don't know the specific integers (as usual) but we know they are related by another integer n. Here we must look to the later part of section 1.2 to find an appropriate theorem. It turns out the the corollary which the book uses to prove the Euclidean algorithm is exactly what we need. Recall that if $a = qm + r$ we have that $(a, m) = (a, r)$. Thus, to find the g.c.d., $(n+1, n^2 - n + 1)$ we only need write $n^2 - n + 1 = q(n+1) + r$ and compute $(n^2 - n + 1, r)$. Since r is smaller than $n + 1$ we hope that solving this equivalent problem will be easier. Thus we use long division of polynomials to find that

$$n^2 - n + 1 = (n-2)(n+1) + 3 \tag{4}$$

where $q = n - 2$ and $r = 3$. Hence we have that $(n+1, n^2 - n + 1) = (n^2 - n + 1, 3)$. Since the only divisors of 3 are 1 and 3, we're done!
□

3 Problems from section 1.3

This section has a very important theorem. It's the fundamental theorem of algebra, theorem 1.11. However, to prove this theorem the book needs theorem 1.8, which says that p is prime is equivalent to the statement: if $p|ab$ then $p|a$ or $p|b$. This is the essential property that primes have. If you do more abstract algebra (and ring theory) you'll end up thinking of this *as* the definition of a prime!

3.1 Problem 1.2.28:

Claim: Let p, q be primes larger than 5. Then $24|(p^2 - q^2)$.

Proof: Here we meet several useful tricks.

Trick #1: If we want to show that a given number a divides b, then we can write $b = na + r$ by the division algorithm. Now our problem is reduced to checking if $r = 0$. Sometimes we're given extra information about how a and b are related, which allows us to find out extra information about r, and this can help us prove that $r = 0$.

Trick #2: This is the fact that if you're given n consecutive integers, then exactly one of them is divisible by n. For example one of $m, n+1$ is even and one of $n, n+1, n+2$ is a multiple of 3.

Now we continue armed with these observations! This is what I meant by *abstraction* in the introduction. Here I could have just made these observations in the course of the following proof, but by recognizing that these ideas are useful in themselves allows me to solve other problems. I spoke about this in section at some length.

Consider that we can factor $p^2 - q^2 = (p+q)(p-q)$. Since p and q are greater than 5, we know that they are both odd numbers: $p = 2k + 1$ and $q = 2l + 1$. Notice that we've basically used trick #1 here. Then $p^2 = 4k^2 + 4k + 1$ and $q^2 = 4l^2 + 4l + 1$. Hence $p^2 - q^2 = 4(k^2 + k - l^2 - l) = 4(k(k+1) - l(l+1))$. Trick #2 says that one of k and $k+1$ is divisible by 2. It also says that one of l and $l+1$ is also. Hence we have that $8|p^2 - q^2$ because we've found three powers of 2 which factor out.

We now have to account for the factor of 3 which must divide $p^2 - q^2$. Now I go back to trick #1, using 3 in the place of a. I get that $p = 3k + r$ and $q = 3l + s$, where the pair $\langle r, s\rangle \in \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 2,2\rangle\}$ because p and q are prime and therefore have some remainder when divided by 3.

We next substitute for p and q to get that

$$p^2 - q^2 = 9k^2 + 6kr + r^2 - 9l^2 - 6ls - s^2$$

. It's our job to show that $r^2 - s^2$ is divisible by 3 since the rest of the terms are. Then we'll be done. We have that $r^2 - s^2 = (r + s)(r - s)$. If $r = s$ we're done because the difference is zero. If $r \neq s$ then we have that $r + s = 3$ and we're done. Hence $3|p^- q^2$. Then the fundamental theorem of arithmetic tells us that since 8 and 3 divide $p^2 - q^2$, 24 does as well.
□

4 Problems from section 2.1

For the first time in the book there is a new conceptual element. This is the notion of *congruence* and *equivalence relation*. This allows us to view all objects in some set which have some common property as all belonging to a subset of the original set. In the case of integers and modular arithmetic, we have that the subsets are those subsets of the integers such that the difference of any pair of elements is a multiple of a fixed number n. That is we look at those distinct subsets, with $0 \leq i \leq n - 1$,

$$S_{i,n} \subset \mathbb{Z} \quad \text{where} \quad r, s \in S_{i,n} \Leftrightarrow n|(s - r).$$

These $S_{i,n}$ are the congruence classes indexed by the notation $[i]$, where $0 \leq n - 1$, which is used in your book.

4.1 Problem 2.1.31

Claim: If $(a, n) = 1$, then there is an integer b such that $ab \equiv 1 \pmod{n}$.

Proof: Here we use the fact from section 1.2 which allows us to write (a, n) as a linear combination of a and n. That is there are some $x, y \in \mathbb{Z}$ such that

$$ax + yn = 1.$$

Then $ax = 1 + (-y)n$. This is the same as $ax \equiv 1 \pmod{n}$. If we let $b := x$ we're done.
□.

5 Conclusion

I may add more problems to this guide if a get a chance to write more up before your exam on Monday. Feel free to email me if you have any questions or you find any errors.

Regards from you TA,
David W. Taylor.