Math 300A Winter 2011

Assignment 9 Answers

DEFINITION: Given two integers m and n, an integer k is a **common divisor of m and n** if k divides m and also k divides n. (In other words, there are integers a and b so that m = ka and n = kb.)

DEFINITION: The **greatest common divisor of m and n** is a positive integer d such that d is a common divisor of m and n and any other divisor k of m and n also divides m. **The greatest common divisor of m and n is denoted by gcd(m,n).**

DEFINITION: Two integers m and n are said to be **relatively prime** if their greatest common divisor is 1.

Examples: The gcd(150, 45) is 15, since 150 = 2*3*5*5 and 45 = 3*3*5. The gcd(49, 39) = 1 since 49 = 7*7 and 39 = 3*13.

Problem 9-2: Prove this theorem that we have been using.

For any integers m and n, there is an integer q and an integer r, with $0 \le r < |m|$ so that n = qm + r.

Hint: Induction on n.

> **Correction and comment**: The integer m cannot be 0. Also, if the case for positive m and nonnegative n is proved, the case for negative m or n can be quickly proved from the positive case (as will be noted at the end). So the revised instructions for the problem were to prove the result for positive m and nonnegative n.
>
> **Answer**: The idea of the proof is that we can fix m (in class there was an example of m = 5) and then do an induction on n. Also, it suffices to prove the theorem for nonnegative n, as will be explained at the end of the proof.
>
> So we can rephrase what we want to prove thus:
>
> To prove: Given a positive integer m, for any nonnegative integer n, there are integers q and r, with $0 \le r < m$ so that n = qm + r.
>
> So m is fixed throughout the proof. We do an inducation on n.
>
> Base case: n = 0. In this case, n = 0m +0, so q = r = 0.
>
> Inductive step: Assume n = qm + r, with $0 \le r < m$ (inductive hypothesis).
>
> Prove: n+1 = q'm + r', with $0 \le r' < m$. (Note: we need a new q and a new r for this case.)
>
> Now we start with n + 1 = qm + r + 1 from the inductive hypothesis.
>
> If $0 \le r + 1 < m$, then we can take r' = r+1 and q' = q. If r < m-1, this is the case and we are done.
>
> In the remaining case of r = m-1, then r+1 = m. So in this case

$n + 1 = qm + r + 1 = qm + m = (q+1)m + 0$. So if we set $q' = q+1$ and $r' = 0$, we have proved what was needed in each case.

QED.

A *very optional* additional comment on the negative case for those who are interested: If $m > 0$ and $n < 0$, then we know from above that

$$-n = qm + r \text{ so } n = (-q)m + (- r).$$

This is the right form but now r is negative or zero. If $r = 0$, then $0 \le r < m$ and we are done. But if $-m < -r < 0$, we add m to r to get $0 < m - r < m$. So if we rewrite the equation as $n = (-q-1)m + (m- r)$. So this has the form $n = q'm + r$, with $q' = -q-1$ and $r' = m-r$.

For negative m, it is simpler. If m is negative and so $-m$ is postive, then for any n, $n = q(-m) +r$ and so $n = (-q)m + r$. is of the right form.

If these equations seem obscure, write out some simple examples.

Problem 9-3: Prove: If m, n, q, and r and integers, then the set of common divisors of m and n is the same as the set of common divisors of m and r.

What does this mean if $r = 0$. Is the theorem still true?

Conclude as a corollary: $\gcd(m,n) = \gcd(m,r)$.

Note: As clarified in an email, the integers here refer to the 9-2.

Answer: We want to show that any divisor of m and n is also a divisor of m and r and vice versa.

Let d be a divisor of m and n. Than means for some integers a and b, $m = da$ and $n = db$.

But we have $n = qm +r$, so $r = n =qm = da - qdb = d(a -qb)$, so r is divisible by d. And we already assumed that m is divisible by d.

In the other direction, assume that d divides both m and r, so $m = db$ and $r = dc$.

Then $n = qm + r = qdb+dc = d(qb+c)$, so n is divisible by d also.

QED.

Problem 9-4: Use the result of 9-3 for an algorithm to find the gcd of any two integers that does not require factoring them into prime factors.

Then use your algorithm on some non-obvious numbers, including some of at least 4 digits and preferably more.

Answer: This is called the **Euclidean Algorithm**.

First of all, for divisors are the same for positive or negative integers, so we assume that m and n are positive. If we wish to find a common divisor of m

and n, we use the division algorithm to write $n = qm + r$, with $0 \le r < m$ as before.

Because of 9-3, the gcd of m and n is the same as the gcd of m and r. If r = 0 above, then m divides n the gcd = m.

But we note that now, whatever, n was, the maximum of m and r is m.

Then if we apply the division algorithm to m , we get $m = q_1 r + r_1$, with $r_1 < r$.

So now the divisors of m and n are the same as the divisors of m and r which are the same as the devisors of r and r_1. And we note that max of r and $r_1 < m-1$.

So we continue with $r = q_2 r_1 + r_2$. Again the divisors of m and n are the same as the divisors of $r_1 + r_2$. And now the max of $r_1 + r_2$ is less than m – 2.

So at each stage, the remainder, which began as a number < m decreases by at least 1. So in no more than m steps, the remainder will be 0.

At this point we have $r_k = q_k r_{k-1} + 0$. And the divisors of m and n will be the same as the divisors of r_{k-1} and 0. But this is the same as the set of divisors of r_{k-1} since any integer divides 0. So we conclude that r_{k-1} itself (a divisor of r_{k-1}) divides m and n, and any common divisor of m and n is a divisor of r_{k-1}. So r_{k-1} must be the gcd of m and n.

Example 1: Let n = 150 and m = 45. Then

150 = 3*45 + 15

45 = 3*15 + 0

15 is the gcd of 150 and 45.

Example 2. Let n = 3744 and m = 390. Then

3744 = 9*390 + 234
390 = 1*234 + 156
234 = 1 * 156 + 78
156 = 2*78 + 0

So 78 is the gcd. In fact 3744 = 48*78 and 390 = 5*178.

Problem 9-5:

Any function X from N to R defines a sequence of real numbers, $X_1, X_2, \ldots$

The number A is defined to be the limit of X_n as $n \to \infty$ if this is true:

For every $\varepsilon > 0$, there is a positive ~~integer~~ N so that for all $n > N$, $|X_n - A| < \varepsilon$.

Notation: $\lim_{n\to\infty} X_n = A$

Comment: It is not necessary to assume N is an integer, since if we have any non-integer N with this property, then the integer N' obtained by rounding up N to an integer in the segment [N, N+1] will satisfy the integer definition.

> **PROVE**: If $X_n = \dfrac{2n-1}{n}$, then $\lim_{n\to\infty} X_n = 2$.
>
> **Answer**. We begin by computing the "error":
>
> $|X_n - A| = |2 - (1/n) - 2| = 1/n$.
>
> Then given an $\varepsilon > 0$, the goal is to make this error $< \varepsilon$, so in particular we need $(1/n) < \varepsilon$. Bu t this is true if $1/\varepsilon < n$.
>
> Then for this $\varepsilon > 0$, let $N = 1/\varepsilon$, then for any $n > N$, $1/n < 1/N$, so $|X_n - A| = 1/n < 1/N < \varepsilon$. Thus the definition is satisfied

Problem 9-6:

Suppose that Z_n is a sequence for which this is true: There is a positive integer N such that for every $\varepsilon > 0$, for all $n > N$, $|Z_n - A| < \varepsilon$.

What would an example of such a Z_n be? What can you prove about Z_n that must be true.

> **Answer**. This definition says that for all $n > N$ that for that particular n, $|Z_n - A| < \varepsilon$ for any $\varepsilon > 0$. But this means that it must be true that $|Z_n - A| \le 0$, for if the number were positive, there would be a positive ε that would be smaller. But also $|Z_n - A| \ge 0$ since it is an absolute value, so it must = 0 and $Z_n = A$.
>
> And this is true for an $n > N$, so this only happens if the sequence is constant beyond a certain point: in other words, for all $n > N$, $Z_n = A$.
>
> An example would be any constant sequences or any sequence such as 1, 2, 3, 3, 3, 3, 3, ... with 3 for all remaining terms.

Problem 9-7:

(a) Write what it means for a number A *not* to be the limit of X_n as $n \to \infty$. In other words, what is the negation of the definition in 9-5.

> **Answer**: A is not a limit of X_n as $n \to \infty$ if there exists an $\varepsilon > 0$ such that for every N there is some $n > N$ such that $|X_n - A| \ge \varepsilon$.

In other words, there is a subseqence that stays a fixed distance away from A.

(b) If the sequence $Y_n = (-1)^n$ for all positive integers n, prove that there is no number A that is the limit of Y_n as $n \to \infty$.

Answer: Pick any A and we show it is not a limit. This includes the case when A = 1 or -1 but all other numbers as well. The idea of the proof is that we observe that any A is either at distance ≥ 1 from +1 or from -1. So an infinite number of the Y_n must be at this distance from A. (In this case, either all the odd ones or all the even ones, or maybe both if A is a number like 12.)

Since the distance between +1 and -1 is 2, we pick e = 1, which is half that distance. (A smaller number would work well also.)

Now what we show is that for every N, there is an n > N, with $|(-1)^n - A| \geq 1$.

For any N, we pick any even number n > N. Then $Y_n = 1$. If $|1 - A| \geq 1$ we have already satisfied the condition.

But if $|1 - A| < 1$, for another number > N, we choose n + 1. Then $Y_{n+1} = -1$.

The condition $|1 - A| < 1$ implies that A > 0. (This is kind of obvious by looking at the number line, but more formally: $|1 - A| < 1 \Rightarrow -1 < A - 1 < 1 \Rightarrow 0 < A < 2$.)

And for this positive A, the distance to the number -1 must be great that 1. Algebraically, $|A - (-1)| = |A + 1| = A + 1$ since A is positive. And also $1 < A + 1 = |A - (-1)| = |A - Y_{n+1}|$. So this is the condition that $|A - Y_{n+1}| > 1 = \varepsilon$.