Instructions: We'll use the same whiteboard process until, as a whole class, we decide to use some other process.

For the fill-in-the-blank questions, you can take a screen shot of the question in PDF, and then write on the picture using Paint (in Windows).

If you'd prefer to use LaTeX, I can include the source file. Just let me know.

Announcements: 1) Homework 1 solution is posted in the Week 1 folder.

2) You already noticed this but files are now split into folders based on week (and topic is listed in the folder name to help find files).

3) Change in dates just a bit. Pre-class due Wednesday to give myself (and you) a bit extra time to fill in any blank pages.

4) You will receive an email from me about the official documentation for the independent study. If you'd like to register for the course in the fall, you need to fill out a part of the form and send to me. More info in the email.

5) Is Google Chat working? Do you prefer emails? Email reminders?

gcd(a,0)=a since every integer a divides itself, and every integer a divides 0

gcd(a,1) =1 since 1 is the only divisor of 1.

-joe

2

2. Using your answers to the pre-class activity problems 2-5, think about how to complete the greatest common divisor properties below. No justification is needed (yet).

a. If $d|a$ and $d|b$, then $d \mid \gcd(a,b)$.

b. If $g = \gcd(a, b)$, then $\gcd(a/g, b/g) = 1$.

c. $\gcd(ac, bc) = \gcd(a,b) \cdot c$.

d. If $d = \gcd(a, b)$, then d divides $ax + by$ for any x and y.

e. If $d = \gcd(a, b)$, then $\gcd(a, a - b) = d$.

-Nick

Corollary

Corollary 1. $\gcd(a,b) = 1$ *if and only if there exists integers x and y such that $ax + by = 1$.*
Note that this result is labeled as corollary *because it is a direct consequence of the previous theorem.*

Using the property of greatest common divisor as a linear combination, we can also prove the first of the greatest common divisor properties you were asked to guess above:

Corollary 2. *If $d \mid a$ and $d \mid b$ then $d \mid \gcd(a,b)$.*

Proof. Let a,b and d be integers with d being nonzero, and assume that d divides a and d divides b. We will prove directly that for all integers x and y, d divides $(ax + by)$. Since d divides a, there exists an integer q_1 such that $a = q_1 d$ and since d dives b, there exists an integer q_2 such that $b = q_2 d$. Using substitution and algebra, we obtain

$$\begin{aligned} ax + by &= (q_1 d)x + (q_2 d)y \\ &= d(q_1 x + q_2 y). \end{aligned} \tag{1}$$

Since $(q_1 x + q_2 y)$ is an integer, equation 1 shows that d divides $ax + by$ and this consequently proves that for all integers x and y, d divides $ax + by$. Recall from Theorem 3 that if a and b are not both zero and $d = \gcd(a,b)$, then d is the smallest element in the set of all positive integers of the form $ax+by$. Furthermore from Corollary 1 that $\gcd(a,b) = (ax + by)$ □

Cy

Theorem 5

BASE: Say n=2 so then p|b1*b2. By Euclids Lemma p must divide b1 or b2 and we are done

Maybe we can do base n=1? I do this often, with some statements, I don't clearly indicate what n's I'm referring to and expect it to be deduced from the context.

In this case, I think n=1 and n=2 are both valid basis cases. n=1 really is the most general case, but since that's a truly trivial case with a tautology statement, it could be omitted.

We want to show the statement is true for n=k+1

If p divides b1*b2*b3*...*b(k+1) then p divides b(i) for some i

We assume p divides b1*b2*b3*...*b(k+1)

We strive to show p divides b(i) for some i

Using the corollary on p| [b1*b2*b3...*b(k)] * b(k+1) we know either p| [b1*b2*b3...*b(k)] or p|b(k+1)

If p| [b1*b2*b3...*b(k)] then we know from our inductive assumption that one of the b(i)'s is divisible by p

If p| b(k+1) then it divided one of the b(i)'s

Cian

Corollary

Corollary: If $d|a$ and $d|b$ then $d|\gcd(a, b)$

Let a and b be integers. Let $c = \gcd(a, b)$. Suppose $d|a$ and $d|b$, then we know $d|(ax + by)$ for any integers x and y. Additionally we know $c = ma + nb$ for some integers m and n, so from this we know $d|c$.

-Miah

Division Algorithm Proof sketch: (For in-class discussion)

Division = repeated subtraction

Well-ordering principle=every non-empty subset of natural numbers has a minimum element.

Existence proof

S = { a-b*k >= 0 : k is an integer }

For example: a=-7 b = 5. Then we can find a non-negative a-b*k by using a negative k: a-b*k = -7-5(-2) =-7+10=3>=0

Since S is not empty it has a minimum, call it r. This is >=0 by definition of the set S.

Say r=a-b*k_0. Suppose r>=b. Then a-(k_0+1)b is a smaller element in set S. This contradicts the fact that r was the smallest in S. Therefore, r must be < b.

Uniqueness proof: bq+r = bq'+r'

GCD as a linear combination:

Create a set for Well-ordering principle: S={ax+by>0: x, y integers}

e=smallest element of the set : Want e=d

Show e<=d

The way we will show this is e|a and e|b.

To show e|a, consider the remainder, r, of a divided by e. We will show that's 0. r = a-e*k (for some k). Since e=ax+by, we have r=a-(ax+by)*k = a(1-k*x)- b*y*k.

So r is a linear combination of a and b as well, and it's >=0. If it's >0, then it's an element in S and is smaller than e (because it's remainder after division by e). That's a contradiction.

So r must be 0, which means e|a. Similarly e|b. This means e is a common factor of a and b, meaning it also divides gcd(a,b)=d, and hence e<=d.

Show e>=d: e=ax+by for some x, y integers because e is the smallest in S. Since d divides both a, b, then d|e, so d<=e