

## Re: GCD(0,0)

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2005-12/msg05275.html>

---

- *From:* [rob@xxxxxxxxxxxxxxxx](mailto:rob@xxxxxxxxxxxxxxxx) (Rob Johnson)
  - *Date:* Fri, 30 Dec 2005 16:43:05 GMT
- 

In article <1135956595.949957.116940@xx>, "JoeS" <jhs@xxxxxxxxxxxxxxxx> wrote:  
>Rob Johnson wrote:  
>> In article <ub8ar15vpkruhjlh52689tadvl5g5n15g@xxxxxxx>,  
>> David C. Ullrich <ullrich@xxxxxxxxxxxxxxxx> wrote:  
>> >On Thu, 29 Dec 2005 20:58:08 -0500, quasi <quasi@xxxxxxx> wrote:  
>> >  
>> >>On 29 Dec 2005 19:59:26 -0500, hrubin@xxxxxxxxxxxxxxxxxxxxxxxx (Herman  
>> >>Rubin) wrote:  
>> >>  
>> >>>In article <1135888209.029280.145500@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>,  
>> >>>Leroy Quet <qququet@xxxxxxxxxxxxxxxx> wrote:  
>> >>>>I notice that these math-controversy threads often get massive  
>> >>>>numbers of replies.  
>> >>>>(While more serious math posts and my games, for example,  
>> >>>>hardly ever get any replies.)  
>> >>>>So I will post this troll-bait flame-bait message to sci.math  
>> >>>>because I always wanted to start one of those huge threads.  
>> >>>>:)  
>> >>>  
>> >>>>For n = any positive integer, it is known that  
>> >>>>  
>> >>>>GCD(n,n) = n  
>> >>>>  
>> >>>>and  
>> >>>>  
>> >>>>GCD(0,n) = n.  
>> >>>>  
>> >>>>(GCD is Greatest Common Divisor, of course.)  
>> >>>>  
>> >>>>But what is, if there is any defined value,  
>> >>>>  
>> >>>>GCD(0,0)?  
>> >>>>  
>> >>>>It certainly isn't 0 (which would fit the pattern above if  
>> >>>>n=0), is it?  
>> >>>>I would think that infinity would work as well as anything.  
>> >>>>  
>> >>>>Or is GCD(0,0) simply undefined, like 0/0?

Re: GCD(0,0)

>> >>>>  
>> >>>>  
>> >>>>>thanks, (half seriously, oh well, 3/4 seriously)  
>> >>>>>Leroy Quet  
>> >>>>  
>> >>>>When it comes to common divisors, since everything  
>> >>>>divides 0, and otherwise an integer never divides  
>> >>>>a smaller integer, for this purpose, 0 is the  
>> >>>>greatest common divisor of 0 and 0.  
>> >>>  
>> >>>You're justifying an exception to the name GCD by pointing out that 0  
>> >>>has other special properties. Sure, we could define  $\text{gcd}(0,0)=0$  or we  
>> >>>could leave it undefined. You can make the case for either one. From  
>> >>>my point of view the G in GCD says it all. No need to confuse things  
>> >>>unless there's a strong reason.  
>> >>  
>> >>A strong reason to want a definition of  $\text{GCD}(0,0)$  is so we  
>> >>don't have to worry about whether  $x$  and  $y$  are both 0 when  
>> >>we mention  $\text{GCD}(0,0)$ . Since that standard definition is in  
>> >>all other cases precisely equivalent to the one given above  
>> >>it seems like a very natural definition.  
>> >>  
>> >>To put the same point another way: Read the rest of the  
>> >>thread, in particular the post by JoeS. The notion of  
>> >> $\text{GCD}$  generalizes in a perfectly natural way to an  
>> >>arbitrary PID. But the definition that works in a PID  
>> >>is equivalent to the definition above, and gives  
>> >> $\text{GCD}(0,0) = 0$ .  
>> >>  
>> >>Another justification that I don't see mentioned yet:  
>> >>The euclidean algorithm gives  $\text{GCD}(0,0) = 0$ .  
>> >>  
>> >>I had originally written for my last post a paragraph about Bezout's  
>> >>identity. However, in Bezout's identity,  $\text{GCD}(x,y)$  is the non-negative  
>> >>generator of the ideal  $\{ ax + by : a \text{ and } b \text{ integers} \}$ , so this added  
>> >>very little to the post by Joe Silverman.  
>> >>  
>> >>The usual Euclidean Algorithm applied to 0 and 0 would require dividing  
>> >>0 by 0, and this would cause a problem. However, if we describe the  
>> >>algorithm for non-negative  $x$  and  $y$  as  
>> >>  
>> >> $x = yq + r$  where  $r = 0$  or  $r$  is the smallest positive integer possible  
>> >>if  $r = 0$ , then  $y$  is the GCD  
>> >>otherwise,  $x \leftarrow y$ ,  $y \leftarrow r$ , repeat  
>> >>  
>> >>This version is made so that  $\text{GCD}(0,x) = \text{GCD}(x,0) = x$  and  $\text{GCD}(0,0) = 0$ .  
>> >>  
>> >>As David Ulrich says, it's quite reasonable to define something as the  
>> >>output of an algorithm. (One has to prove that the algorithm  
>> >>terminates, of course.) In general a ring  $R$  is "Euclidean" if it has a  
>> >>Euclidean algorithm, which means that it has a size function

Re: GCD(0,0)

>  
> s :  $\mathbb{R} \rightarrow$  (nonnegative real numbers)  
>  
> satisfying certain properties. It's easy to show that a Euclidean ring  
> is a PID and that the output from the Euclidean algorithm is a  
> generator for the ideal generated by a and b. But there are rings that  
> are PIDs, but are not Euclidean. So in terms of generalizing the notion  
> of GCD, using the Euclidean algorithm seems like a halfway step. OTOH,  
> I certainly agree that it provides an instructive way to think about  
> what it means to generalize a concept.

The arguments using PIDs require less manipulation to work. I had to rewrite the instructions for the Euclidean algorithm above so that each of GCD(0,1), GCD(1,0), and GCD(0,0) would give the desired result. Besides, I've always liked using Bezout's identity rather than the Euclidean Algorithm in proofs.

However, the Euclidean Algorithm does add one more data point in favor of defining  $\text{GCD}(0,0) = 0$ .

Rob Johnson <rob@xxxxxxxxxxxxxxxx>  
take out the trash before replying

---

• **References:**

- ◆ **GCD(0,0)**  
    ◇ From: Leroy Quet
- ◆ **Re: GCD(0,0)**  
    ◇ From: Herman Rubin
- ◆ **Re: GCD(0,0)**  
    ◇ From: quasi
- ◆ **Re: GCD(0,0)**  
    ◇ From: David C . Ullrich
- ◆ **Re: GCD(0,0)**  
    ◇ From: Rob Johnson
- ◆ **Re: GCD(0,0)**  
    ◇ From: JoeS

- Prev by Date: **Re: Egyptian arithmetic and its remainders**
- Next by Date: **Re: Absolute continuity, another question,**
- Previous by thread: **Re: GCD(0,0)**
- Next by thread: **Re: GCD(0,0)**
- Index(es):
  - ◆ **Date**
  - ◆ **Thread**