Pólya's Paragon

Greatest Common Divisors

Ian VanderBurgh

Most of us learned about greatest common divisors ($\gcd$'s) in elementary school when we first learned about prime numbers and prime factorizations. (Remember those prime factorization trees?) We used greatest common divisors again when we learned to add fractions. Since then, however, we have probably forgotten most of what we learned! Here is a refresher on $\gcd$'s along with some related calculations and manipulations.

Definition. If a and b are integers that are not both 0, the *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the largest positive integer that divides exactly into both a and b.

In other words, $\gcd(a, b)$ is the greatest of all the common divisors of a and b. (Don't you wish that all mathematical definitions made this much sense?) To emphasize, d is a *divisor* of a if d divides exactly into a (that is, if $a = qd$ for some integer q). To tidy up a loose end, we say that $\gcd(0, 0) = 0$. (Notice here that there is not, in fact, a largest positive integer that divides into both 0 and 0, since every positive integer divides into 0. This means that we either need to ignore this case entirely, or we need to say something special here, as we have done.)

Calculations. Finding the $\gcd$ of a pair of integers is not terribly difficult when the integers are small: $\gcd(2, -4) = 2$, $\gcd(3, 5) = 1$, and $\gcd(-13, 1) = 1$. It is worth noting that $\gcd(a, 0) = a$ if a is positive and $\gcd(a, 0) = -a$ if a is negative. (Those of you comfortable with absolute values can condense this to $\gcd(a, 0) = |a|$.) Also, $\gcd(b, 1) = 1$ for every integer b. Can you see why these formulas are true from the definition?

What happens if the integers are large? For example, suppose we want to calculate $\gcd(1977, 2007)$. Your first instinct might be to try to factor 1977 and 2007 to find their positive divisors, then compare lists to find the largest of all common divisors. Let's try this.

First, $1977 = 3 \times 659$. After a bit of painful trial and error, we find that 659 appears to be a prime number. (How do we know that 659 is prime? That's a subject for another Paragon!) This tells us that the positive divisors of 1977 are 1, 3, 659, and 1977.

Next, $2007 = 3 \times 669 = 3 \times 3 \times 223$. Again, after a bit of flailing around, we discover that 223 is prime; hence, the positive divisors of 2007 are 1, 3, 9, 223, 669, and 2007.

Therefore, the positive common divisors of 1977 and 2007 are 1 and 3, which implies that $\gcd(1977, 2007) = 3$.

This method works reasonably well, but it would be pretty gruesome if 1977 and 2007 were each eight digits long instead of only four, or if there were no readily apparent small prime factors. We can cut down our work a bit by looking directly at the prime factorizations instead of listing divisors, but this still requires calculating the prime factorizations, which, as it turns out, is a very demanding problem computationally.

There is a better way, which takes advantage of the following fact:

> *Important Fact #1:* If a, b, q, and r are integers with $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

This fact is not all that intuitive (lots of number theory books contain a proof, if you're interested), but we can use this fact to do what mathematicians love to do: take a problem and turn it into a smaller (or simpler) one. Here's how:

$$\begin{array}{rcl@{\quad\Longrightarrow\quad}rcl} 2007 &=& 1(1977) + 30 & \gcd(2007, 1977) &=& \gcd(1977, 30) \\ 1977 &=& 65(30) + 27 & \gcd(1977, 30) &=& \gcd(30, 27) \\ 30 &=& 1(27) + 3 & \gcd(30, 27) &=& \gcd(27, 3) \\ 27 &=& 9(3) + 0 & \gcd(27, 3) &=& \gcd(3, 0) \end{array}$$

Following through this chain, $\gcd(2007, 1977) = \gcd(3, 0)$, which equals 3. (We could have stopped earlier when we saw a gcd that was easy to calculate, but it doesn't hurt to keep going until we get a 0.) Can you tell what we did at each step? At each step, we took out as many copies of the smaller number as we could from the larger number, and determined what was left over. (In technical terms, we performed the Division Algorithm several times, calculating the remainder at each stage.) Overall, this method of calculating the gcd is called the Euclidean Algorithm. Try this algorithm on 6540 and 1236. (Did you get 12 as your answer?)

After you get comfortable with this method, you may notice two time-saving features. The first is that you don't have to write all of the equalities of gcd's down the right side—these will always be true, so we can relate the gcd of the original numbers to the gcd of the final numbers directly. The second builds on the first—the gcd will actually always be the final non-zero remainder in the Algorithm. (Can you see why?)

Manipulations. These methods seem to work really well for numbers, you may say, but can I use them in a more abstract setting, like what might appear in a contest problem?

Funny you should ask . . . . Here is the very first problem from the very first International Mathematical Olympiad in 1959:

> *Problem #1.* Prove that the fraction $\dfrac{21n + 4}{14n + 3}$ is irreducible for every natural number n.

Step one here, as in any problem, is to figure out what it is really asking. This problem can be restated as "Prove that $\gcd(21n + 4, 14n + 3) = 1$ for

every natural number n" (since a fraction is irreducible if its numerator and denominator have no common factors).

We try to model our method from above:

$$\begin{aligned} 21n+4 &= 1(14n+3)+(7n+1)\,, \\ 14n+3 &= 2(7n+1)+1\,, \\ 7n+1 &= (7n+1)(1)+0\,. \end{aligned}$$

Thus, $\gcd(21n+4, 14n+3) = \gcd(14n+3, 7n+1) = \gcd(7n+1, 1) = 1$, as we wanted. So, we can adapt this method!

Another fact that can be quite handy:

Important Fact #2: If $\gcd(c, b) = 1$, then $\gcd(ac, b) = \gcd(a, b)$.

This fact is actually useful in both directions—it allows us to convert $\gcd(a, b)$ to $\gcd(ac, b)$ (although it is not immediately obvious why we would ever want to do this), and it allows us to convert $\gcd(ac, b)$ to $\gcd(a, b)$. This fact is more intuitive—can you explain it to yourself?

We now try a second problem:

Problem #2. Prove that $\gcd(n^2, 2n+1) = 1$ for any natural number n.

Our initial instinct is to try to use the abstract version of the Euclidean Algorithm, but it is very difficult to make $2n+1$ go into n^2 without introducing fractions. This is where Important Fact #2 can be used: since $2n+1$ is odd, then $\gcd(2n+1, 2) = 1$. Thus,

$$\begin{aligned} \gcd(n^2, 2n+1) &= \gcd(2n^2, 2n+1) && (\text{since } \gcd(2n+1, 2) = 1) \\ &= \gcd(-n, 2n+1) && (\text{since } 2n^2 = n(2n+1)+(-n)) \\ &= \gcd(n, 2n+1) && (\text{since } \gcd(-1, 2n+1) = 1) \\ &= \gcd(n, 1) && (\text{since } 2n+1 = 2(n)+1) \\ &= 1\,, \end{aligned}$$

as required.

I hope you have remembered a bit and learned a bit about gcd's here. By no means is what we have done comprehensive, but it should give you some ideas to think about and some strategies to use. Try applying them to one of this month's Mayhem problems!

Ian VanderBurgh
Centre for Education in Mathematics and Computing
University of Waterloo
200 University Avenue West
Waterloo, ON, Canada N2L 3G1
iwtvande@uwaterloo.ca