Math Circles: Euclid and Fibonacci

M. Victor Wickerhauser

Sunday, February 24th, 2019

Euclid wrote the book on geometry 2300 years ago ("Elements," still available from Dover Books) but he was also interested in arithmetic. Even if he himself did not invent the math, he gets the credit for writing it down.

Fibonacci, or Leonardo of Pisa, wrote the book on arithmetic 900 years ago ("Liber Abaci," still available from Springer Verlag) that convinced everyone in medieval Europe to use Hindu/Arabic numbers. He did not invent the system but we should give him credit for sparing us from having to learn how to multiply and divide Roman numerals.

These two men are perhaps best known for "Euclid's algorithm" and "Fibonacci numbers," respectively. These monuments to their intellects are related in a curious way which we will now explore.

1. When working with fractions, it is easiest to put them in lowest terms and use common denominators.
   - Put 3/9 and 15/25 into lowest terms.
   - What is a common denominator in the sum $\frac{1}{6} + \frac{1}{4}$? What is the answer in lowest terms?
2. To get lowest terms requires finding common divisors in the numerator and denominator.
   - What are the common divisors of 3 and 9? 4 and 6? 15 and 25?
   - What are the common divisors of 12 and 30?
   - This works for more than two numbers. What is a common divisor of 12, 16, and 30?
3. The *greatest common divisor* of two numbers is the largest number that divides both of them. If the numbers are the numerator and denominator of a fraction, the greatest common divisor must be factored out of both to get lowest terms.
   - What is the greatest common divisor of 12 and 30? What is 12/30 in lowest terms?
   - What is the greatest common divisor of 768 and 512? What is 512/768 in lowest terms?

4. What is the greatest common divisor of 299792458 and 0? The principle here is that every number d is a divisor of 0 since we may write $0 = d \times 0$.

5. What is the greatest common divisor of 6022140923 and 6022140923? What is the principle here?

6. When the numbers are large, positive, and unequal, it may take many trial divisions to find common divisors. In Euclid's "Elements" it is noted that any common divisor of numbers a and b is also a common divisor of b and $a - b$. Prove this by supposing that d is a common divisor, $a = a_0 d$ and $b = b_0 d$ for numbers a_0, b_0, then writing $a - b$ as a multiple of d.

7. Now suppose that $a > b > 0$ are (large) numbers. Try to prove, using properties of ">," that $a > a - b > 0$. Then note that any common divisor of a and b is also a common divisor of the smaller numbers b and $a - b$.

8. Euclid's idea may be applied *recursively* (more than once, on each new result). Given $a > b > 0$, let $a_1 = \max(b, a - b)$ and let $b_1 = \min(b, a - b)$. Try to prove that $a_1 \geq b_1 > 0$. Then note that if $a_1 > b_1$, the process may be repeated with a_1 and b_1 replacing a and b.

   Otherwise, if $a_1 = b_1$, then their greatest common divisor is a_1, which is therefore the greatest common divisor of a and b.

   (This recursive proceedure is the original *Euclidean algorithm* of 2300 years ago.)

9. Using the Euclidean algorithm, find the greatest common divisor of 768 and 512. Hint: no trial division is needed.

10. A more modern version of Euclid's algorithm uses the *division principle:*

    For any numbers a and b with $b > 0$, there are unique numbers q and r (the "quotient" and "remainder," respectively) such that $a = qb + r$ and $0 \leq r < b$.

    - Find q and r for $a = 30$ and $b = 12$.
    - Prove that if d is a divisor of a and b, and $a = qb + r$, then d is a divisor of r.

11. The modern Euclidean algorithm is to replace a, b with $a_1 = b$ and $b_1 = r$, where $a = qb + r$ from the division principle. The greater efficiency comes from the greater reduction in number size per step. $a > b > 0$ results in $a > b = a_1 > r = b_1 \geq 0$.

    If $b_1 = 0$, then the greatest common divisor is a_1.

    Otherwise, division is repeated on a_1, b_1.

    - Use this division version of Euclid's algorithm to find the greatest common divisor of $a = 36$ and $b = 8$. How many steps are required?

    - Use the original Euclidean algorithm (just subtraction) to find the greatest common divisor of $a = 36$ and $b = 8$. How many steps are required?

12. Suppose we use the modern version and keep track of the quotients and remainders. Start with $a > b > 0$ and define a sequence of remainders $\{r_0, r_1, \ldots\}$ and a sequence of quotients $\{q_1, q_2, \ldots\}$ as follows:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_{n+1} &= r_{n-1} - q_n r_n, \qquad \text{for } n = 1, 2, \ldots, \end{aligned}$$

where q_n is defined to be the unique whole-number quotient r_{n-1}/r_n, and r_{n+1} is the remainder, in the division formula

$$r_{n-1} = q_n r_n + r_{n+1}.$$

For example, starting with $r_0 = a = 36$ and $r_1 = b = 8$ gives this table:

n	r_n	q_n
0	36	
1	8	4
2	4	2
3	0	

Since $r_3 = 0$ it is impossible to find q_3. The greatest common divisor of 36 and 8 is then found at $r_2 = 4$.

Fill out this similar table to find the greatest common divisor of 60 and 45:

n	r_n	q_n
0	60	
1	45	
2		
3		

13. Notice that any common divisor d of both a and b is also a divisor of $sa + tb$, where s, t are any whole numbers. That becomes clear if we write $a = a_0 d$ and $b = b_0 d$ and expand (using the associative and distributive axioms of arithmetic):

$$sa + tb = s(a_0 d) + t(b_0 d) = (sa_0)d + (tb_0)d = (sa_0 + tb_0)d,$$

which is evidently a multiple of d. This is true for the greatest common divisor d, so every number in this set is a multiple of the greatest common divisor of a and b:

$$I(a, b) = \{sa + tb : \ s, t \text{ any integers, positive, negative, or zero.}\}$$

The smallest positive number in $I(a, b)$ is in fact the greatest common divisor of a and b.

Fill out the empty places of this table to get a sampling of the elements of $I(9, 6)$, namely $I(a, b)$ with $a = 9$ and $b = 6$:

s	t	$sa + tb$	s	t	$sa + tb$	s	t	$sa + tb$
0	0	0	2	0		-1	0	
0	1	6	2	1		-1	1	
1	0	9	2	-1		-1	2	
1	-1	3	2	-2		-1	3	

14. The preceding result is called *Bézout's lemma:* The greatest common divisor of two positive numbers a and b can be written as $sa + tb$ for some integers s, t, and it is the smallest positive number that can be written this way.

A classical puzzle is to measure exactly 1 gallon of water into a tank if you only have a 3 gallon measure and a 5 gallon measure. This is possible because the greatest common divisor of 3 and 5 is 1, so by Bézout's lemma we write $1 = 2 \times 5 - 3 \times 3$ and apply this by filling the tank with 2 5-gallon measures then draining out (subtracting!) 3 3-gallon measures of water.

If we have only a 2 gallon measure and a 4 gallon measure, then by the same lemma it is impossible to end up with exactly one gallon of water since the greatest common divisor of 2 and 4 is 2, and no smaller positive amount can be obtained by filling and draining.

Find the procedure for measuring out exactly 1 gallon of water if you only have a 9 gallon measure and an 11 gallon measure.

15. To prove Bézout's lemma, suppose $a > b > 0$ are given and let d be the smallest positive number that can be written as $d = sa + tb$ for some integers s, t. We already know that any common divisor of a and b also divides d. It remains to show that d itself is a common divisor of a and b.

    So divide a by d and consider the remainder: $a = qd + r$, so

    $$r = a - qd = a - q(sa + tb) = a - (qs)a - (qt)b = (1 - qs)a + (-qt)b,$$

    so the remainder can also be written as $s'a + t'b$ for integers $s' = 1 - qs$ and $t' = -qt$, so $r \in I(a, b)$. But by the division principle, the remainder r satisfies $0 \leq r < d$, and d is the smallest positive integer in $I(a, b)$, so we must conclude that $r = 0$. Thus $a = qd$, so d is a divisor of a.

    Repeat this argument with any needed changes to show that d is a divisor of b as well. Conclude that d is a common divisor of a and b.

16. The *extended Euclidean algorithm* is one way to find the numbers s, t such that $sa + tb = \gcd(a, b)$. (Here $\gcd(a, b)$ denotes the greatest common divisor of a and b.) In this algorithm, not only do we

keep track of the remainders r_n and quotients q_n, we keep track of two more sequences s_n and t_n that ultimately equal s and t. Namely, start with $r_0 = a$ and $r_1 = b$ as before, but now also put $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, and $t_1 = 1$, and then for $n = 1, 2, \ldots$, compute

$$\begin{aligned} r_{n+1} &= r_{n-1} - q_n r_n, \qquad \text{where } q_n \text{ is the whole-number quotient } r_{n-1}/r_n, \\ s_{n+1} &= s_{n-1} - q_n s_n, \\ t_{n+1} &= t_{n-1} - q_n t_n. \end{aligned}$$

For example, starting with $a = 36$ and $b = 8$ gives this table:

n	r_n	q_n	s_n	t_n
0	36		1	0
1	8	4	0	1
2	4	2	1	-4
3	0			

We stop at $r_3 = 0$ since it is then impossible to find q_3. The greatest common divisor of 36 and 8 is then found at $r_2 = 4$, and it may be written as $r_2 = 4 = 1 \times 36 + (-4) \times 8 = s_2 a + t_2 b$.

Fill out this similar table to find the greatest common divisor of 60 and 45 as a combination of the two numbers:

n	r_n	q_n	s_n	t_n
0	60		1	0
1	45		0	1
2				
3				

17. To prove that the extended Euclidean algorithm works, it suffices to prove that

$$r_n = s_n a + t_n b, \qquad \text{for } n = 0, 1, 2, \ldots, N,$$

since then the last nonzero remainder r_N, which is $\gcd(a, b)$, will equal $sa + tb$ with $s = s_N$ and $t = t_N$.

So we first check $n = 0$:

$$s_0 a + t_0 b = 1 \times a + 0 \times b = a = r_0.$$

And we then check $n = 1$:

$$s_1 a + t_1 b = 0 \times a + 1 \times b = b = r_1.$$

And we finally check the cases $n > 1$ "by induction" using the recursive formulas:

$$\begin{aligned} s_{n+1}a + t_{n+1}b &= (s_{n-1} - q_n s_n)a + (t_{n-1} - q_n t_n)b \\ &= s_{n-1}a - q_n s_n a + t_{n-1}b - q_n t_n b \\ &= s_{n-1}a + t_{n-1}b - q_n s_n a - q_n t_n b \\ &= [s_{n-1}a + t_{n-1}b] - q_n[s_n a + t_n b] \\ &= [r_{n-1}] - q_n[r_n] \\ &= r_{n+1}. \end{aligned}$$

The formula thus works for all n until $r_{N+1} = 0$, after which q_n is undefined.

18. Now let us consider how many steps the modern Euclidean algorithm will need to find $\gcd(a, b)$. Starting with $r_0 = a$ and smaller $r_1 = b$, it produces new, smaller remainder r_{n+1} after step n, and terminates when $r_{n+1} = 0$. We have

$$r_0 = a > b = r_1 > r_2 > \cdots \geq 0,$$

and each reduction is by at least 1, so it will take at most b steps to hit zero.

But b steps is a lot of work if b is large. A better estimate comes from *Lamé's theorem:* If Euclid's algorithm takes N steps to get $r_{N+1} = 0$, then $r_0 \geq F_{N+1}$ and $r_1 \geq F_N$, where F_n is the nth Fibonacci number.

The Fibonacci numbers are defined by this recursion:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+1} &= F_n + F_{n-1}, \qquad \text{for } n = 1, 2, 3, \ldots, \end{aligned}$$

The first few values are thus the well-known sequence

F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
0	1	1	2	3	5	8	13	21	34

See if you can compute F_{17}.

19. To prove Lamé's theorem suppose that $a > b > 0$ and that it takes N divisions in Euclid's algorithm to find $\gcd(a, b)$, namely that $r_N > 0$ but $r_{N+1} = 0$ for $r_0 = a$ and $r_1 = b$. Since $r_{n+1} = r_{n-1} - q_n r_n$, $r_n \geq 0$, and $q_n \geq 1$ for $0 < n \leq N$, we have

$$r_{n-1} = q_n r_n + r_{n+1} \geq r_n + r_{n+1}.$$

Now imagine starting at $n = N$, so $r_{N+1} = 0$ and $r_N \geq 1$. Thus r_{N-1} is at least as big as the Fibonacci number F_2 since it is the sum of two numbers at least as big as F_0 and F_1. Working backwards $N - 1$ more steps, we see that $r_1 \geq F_N$ and $r_0 \geq F_{N+1}$.

To see this in action, use Euclid's algorithm to find $\gcd(F_9, F_8) = \gcd(34, 21)$. Does it take 8 divisions? How would you describe the sequence $r_2, r_3, \ldots$?

20. The worst case for the modern Euclidean algorithm, namely the case requiring the most division steps, has all quotients equal to 1, so the remainders are found by subtraction just like in the original Euclidean algorithm.

21. Adjacent Fibonacci numbers have no common divisor greater than 1. In other words, we claim that $\gcd(F_n, F_{n+1}) = 1$ for all $n = 0, 1, \ldots$

    To prove this claim, note that $\gcd(F_0, F_1) = \gcd(0, 1) = 1$. Now suppose that $n > 0$ and let d be a common divisor of F_n and F_{n+1}. Then d also divides $F_{n-1} = F_{n+1} - F_n$ (by Euclid's original observation!), so d is a common divisor of F_{n-1} and F_n. Repeating this argument (how many times?) shows that d is a common divisor of F_0 and F_1, so d must be 1.

    Try to prove that $\gcd(F_n, F_{n+2}) = 1$ for all $n = 0, 1, 2, \ldots$. Hint: apply Euclid's observation to $F_{n+2} = F_{n+1} + F_n$ and F_n to reduce to the case of computing $\gcd(F_{n+1}, F_n)$, which is known to be 1.

22. Another application of Bźout's lemma and the extended Euclidean algorithm is to answer questions like: "Is there an integer x such that $34x - 1$ is divisible by 21?" The answer is "yes" if and only if there is an integer y such that

$$34x - 1 = 21y, \qquad \iff 34x + (-y)21 = 1,$$

    which by Bézout's lemma exists if and only if $\gcd(34, 21) = 1$. But we recognize that 34 and 21 are adjacent Fibonacci numbers, so their greatest common divisor is 1, so there is indeed a solution.

    See if you can find x using the extended Euclidean algorithm.

23. In general, the answer to the question "Is there an integer x such that $Mx - D$ is divisible by N?" is yes if and only $\gcd(M, N)$ divides D.

    If $\gcd(M, N) = 1$, then the answer is yes for every D. Given $D > 1$ simply find x, y such that $Mx + Ny = 1$, and then use Dx since

    $$D = D \times 1 = D(Mx + Ny) = M(Dx) + (Dy)N,$$

    so $M \times (Dx) - D = (Dy) \times N$, a multiple of N.

    - What is the answer if $D = 0$? (Notice that M and N can be anything and the answer will be the same!)

    - What is the answer if $M = 2019$, $N = 9999$, and $D = 9$?

    - The answer will be yes if $M = N = D$. Can you find an x that works in all such cases? Will any x work?

24. There is an exponential formula for Fibonacci numbers:

    $$F_n = \frac{\Phi^n - (-\Phi)^{-n}}{\sqrt{5}},$$

    where $\Phi = (1 + \sqrt{5})/2 \approx 1.618\ldots$ and $\sqrt{5} \approx 2.236\ldots$. Since $\Phi^{-n} = 1/\Phi^n < 1$ for all $n > 0$, and $\sqrt{5} > 2$, the following simpler formula gives the same answer:

    $$F_n = \texttt{round}\left(\frac{\Phi^n}{\sqrt{5}}\right),$$

    where $\texttt{round}(X)$ denotes the integer nearest to the number X. We can use this to estimate the number of decimal digits D in the nth Fibonacci number F_n:

    $$10^D = F_n \approx \frac{\Phi^n}{\sqrt{5}},$$

where we may ignore the small difference caused by rounding since the numbers are very large for large n. Such equations are solved by logarithms:

$$\log(10^D) = D\log(10) = \log(F_n) \approx \log\left(\frac{\Phi^n}{\sqrt{5}}\right) = n\log(\Phi) - \log(\sqrt{5}),$$

so

$$D \approx \left[\frac{\log(\Phi)}{\log(10)}\right] n - \left[\frac{\log(\sqrt{5})}{\log(10)}\right] \approx 0.2090n - 0.3495.$$

The accuracy improves as n increases. Roughly speaking, F_n has about $0.2n$, or about $n/5$, digits, so F_{100} has more than 20 digits (in fact it is more than 300 billion billion).

By Lamé's theorem, this means that the smallest numbers that require 100 divisions in Euclid's algorithms are bigger than 300 billion billion.

- About how many digits will there be in the smallest numbers that require one million divisions in Euclid's algorithm?

- Suppose that a is a one-million-digit number. How many divisions will it require, at most, to find $\gcd(a, 34)$?

25. To derive the exponential formula for Fibonacci numbers, use a fact about their generalization: a *Lucas sequence* is determined by initial values $L_0 = A$ and $L_1 = B$ and the recursion

$$L_{n+1} = PL_n + QL_{n-1}, \qquad n = 1, 2, 3, \ldots$$

(The Fibonacci sequence is the special case with $A = 0$, $B = 1$, and $P = Q = 1$.)

We first suppose that the nth term is of the form

$$L_n = r^n,$$

where r is a numbers to be determined. For this to satisfy the recursion we must have

$$r^{n+1} = Pr^n + Qr^{n-1}, \qquad n = 1, 2, 3, \ldots$$

so either $r = 0$ (in which case $L_n = 0$ for all n) or else $r \neq 0$ and we may divide both sides by r^{n-1} to get the quadratic relation

$$r^2 = Pr + Q.$$

This imposes a condition on r: it is a root of the quadratic equation $r^2 - Pr - Q = 0$. We may use the quadratic formula to find the two roots:

$$r_\pm = \frac{P \pm \sqrt{P^2 + 4Q}}{2},$$

which in the Fibonacci case gives $r_+ = (1 + \sqrt{5})/2 = \Phi$ and $r_- = (1 - \sqrt{5})/2$.

Then we observe that the sum of two solutions to the recurrence is also a solution, and likewise any constant multiple of a solution is also a solution. We may thus try the exponential formula

$$F_n = ar_+^n + br_-^n,$$

which solves Fibonacci's recursion for any a, b, and then find values for a, b that give $F_0 = 0$ and $F_1 = 1$.

- Show that $r_- = 1/r_+ = -1/\Phi = (-\Phi)^{-1}$. Hint: rationalize

$$\frac{1}{r_-} = \frac{2}{1 - \sqrt{5}} = \frac{2(1 + \sqrt{5})}{(1 - \sqrt{5})(1 + \sqrt{5})}.$$

- Find a, b such that $0 = F_0 = ar_+^0 + br_-^0 = a + b$ and $1 = F_1 = ar_+^1 + br_-^1 = ar_+ + br_- = a\Phi + b(-\Phi)^{-1}$. Hint: solve the 2×2 system of linear equations for the unknowns a and b in terms of r_+ and r_-, then simplify.