1 Euclid's algorithm

Euclid's algorithm allows you to quickly find the greatest common denominator of any two integers, A and B. This is written "gcd(A,B)". gcd(A,B) is the largest number that evenly divides A and B. So, while "2" divides 12 and 20, it isn't the biggest number that does. You'll find that gcd(12,20) = 4.

If A and B have a common divisor (the gcd is just the biggest of these), then you can write them as $A = jG$ and $B = kG$ where G is the common divisor. But notice that when you subtract one from the other that the difference also has the same divisor.

$A - B = jG - kG = (j - k)G$

Therefore, $gcd(A, B) = gcd(A - B, B)$. The reason for doing this is it gives you a smaller number to work with. So, if you can't look at A and B, immediately factor them, and compare their factors, then maybe you can look at A and $A - B$?

Example: gcd(65,70)=?

$gcd(65, 70) = gcd(65, 70 - 65) = gcd(65, 5)$

So, the only possible common divisors are 1 and 5. 5 divides 65, so gcd(65,70)=5. You can double check this: $65 = 5 \times 13$, $70 = 2 \times 5 \times 7$. 5 is the only shared factor, and the gcd.

Q 1.0.1: $gcd(9, 15) =?$

Q 1.0.2: $gcd(931, 946) =?$

Q 1.0.3: $gcd(836, 957) =?$

Q 1.0.4: Show that 7645389 and 7635389 are relatively prime. That is, show that $gcd(7645389, 7635389) = 1$.

Notice that when you say "$gcd(A, B) = gcd(A - B, B)$", you're basically asking a new, easier question.

Q 1.0.5: $gcd(205, 101) =?$

Q 1.0.6: $gcd(135, 271) =?$

Q 1.0.7: $gcd(289, 165) =?$

Q 1.0.8: $gcd(21, 24, 27) =?$

Q 1.0.9: $gcd(30, 24, 22) =?$

Q 1.0.10: Some of these may have more than one answer depending on N:
-$gcd(N, N) =?$
-$gcd(N, N + 1) =?$
-$gcd(N, N + 2) =?$
-$gcd(N, N + 3) =?$
-$gcd(N, N + 4) =?$

Q 1.0.11: $gcd(3N + 1, 3N + 4) =?$

Q 1.0.12: What can you say about $gcd(N, N + P)$ if N is:
-Greater than P?
-Equal to P?
-Less than P?

Q 1.0.13: $gcd(2N, N + P) =?$, where P is a prime number such that $2 < P < N$.

Q 1.0.14: For different N, $3N + 1$ generates the sequence $\{1, 4, 7, 10, \cdots\}$. Find two numbers in the sequence with a gcd of: 4, 13

Q 1.0.15: Without multiplying out, find $gcd(2^1 3^2 5^3, 2^3 3^2 5^1)$. Consider the definition of gcd.

Q 1.0.16: $gcd(7^2 11^{47}, 3^1 7^{567} 11^3) =?$

Q 1.0.17: $gcd(2^3 5^1 7^8, 5^2 7^1 13^3) =?$

Q 1.0.18: $gcd(2^1 3^2 5^1 11^6, 2^1 3^0 5^2 7^1 11^{73}) =?$

Q 1.0.19: Any positive integer can be written as powers of primes, $(2^{e_2})(3^{e_3})(5^{e_5}) \cdots$. For example, $84 = 2^2 3^1 7^1$ and $e_2 = 2$, $e_3 = 1$, $e_5 = 0$, $e_7 = 1$, $e_{11} = 0$, and so on.

Define $N = (2^{e_2})(3^{e_3})(5^{e_5}) \cdots$ and $M = (2^{f_2})(3^{f_3})(5^{f_5}) \cdots$.

-In terms of e's and f's, what is $gcd(N, M)$? If you don't know how to describe this algebraically, describe it in words.

The "least common multiple" of A and B, written "$lcm(A, B)$", is the smallest number that is a multiple of both A and B. For example, $lcm(6, 9) = 18$.

You're probably used to this from finding the least common denominator when adding or subtracting fractions. For example; $\frac{5}{6} + \frac{2}{9} = \frac{15}{18} + \frac{4}{18} = \frac{19}{18}$.

One of the important properties of the $lcm(A, B)$ is that any factor that *either* A or B have is found in $lcm(A, B)$.

Q 1.0.20: Without multiplying out, find $lcm(2^3 5^1 7^8, 5^2 7^1 13^3)$. Consider the definition of lcm.

Q 1.0.21: Same idea: $lcm(2^1 3^2 5^1 11^6, 2^1 3^0 5^2 7^1 11^{73}) =?$.

Q 1.0.22:
Again, define $N = (2^{e_2})(3^{e_3})(5^{e_5}) \cdots$ and $M = (2^{f_2})(3^{f_3})(5^{f_5}) \cdots$.
-In terms of e's and f's, what is $lcm(N, M)$, the "least common multiple of N and M"?
-$[gcd(N, M)]\,[lcm(N, M)] =?$
-Write a quick algorithm for finding $lcm(A, B)$. "Find the gcd" is a valid step.

1.1 The algorithm

You may have already noticed that it's quicker to divide than subtract. For example, say you want to find $gcd(126, 30)$.

You can subtract several times:
$gcd(126, 30) = gcd(96, 30) = gcd(66, 30) = gcd(36, 30) = gcd(6, 30)$
Or you can say "I'll just remove all the 30's":
$gcd(126, 30) = gcd(4 \cdot 30 + 6, 30) = gcd(6, 30)$
Notice that the quick way to find that 4 (the number of times that 30 goes into 126) is to divide. That 6 is the remainder. The following example solves the same problem the same way, just one way is faster.

Using subtraction	Using the remainder	
$gcd(126, 30)$	$gcd(126, 30)$	
$= gcd(96, 30)$	$= gcd(6, 30)$	$126 = 4 \cdot 30 + 6$
$= gcd(66, 30)$	$= gcd(6, 0)$	$30 = 5 \cdot 6 + 0$
$= gcd(36, 30)$	$= 6$	
$= gcd(6, 30)$		
$= gcd(6, 24)$		
$= gcd(6, 18)$		
$= gcd(6, 12)$		
$= gcd(6, 6)$		
$= gcd(6, 0)$		
$= 6$		

As a matter of mathematical convenience, $gcd(0, x) = x$ by definition. This is so that we can say, in general, that $gcd(A, B) = gcd(A - B, B)$. So, $gcd(x, x) = gcd(0, x) = x$.

Using subtraction	Using the remainder	
$gcd(53, 116)$	$gcd(53, 116)$	
$= gcd(53, 63)$	$= gcd(53, 10)$	$116 = 2 \cdot 53 + 10$
$= gcd(53, 10)$	$= gcd(3, 10)$	$53 = 5 \cdot 10 + 3$
$= gcd(43, 10)$	$= gcd(3, 1)$	$10 = 3 \cdot 3 + 1$
$= gcd(33, 10)$	$= gcd(0, 1)$	$3 = 3 \cdot 1 + 0$
$= gcd(23, 10)$	$= 1$	
$= gcd(13, 10)$		
$= gcd(3, 10)$		
$= gcd(3, 7)$		
$= gcd(3, 4)$		
$= gcd(3, 1)$		
$= gcd(2, 1)$		
$= gcd(1, 1)$		
$= gcd(0, 1)$		
$= 1$		

The Algorithm

You want to find $gcd(A, B)$. Without loss of generalization, assume that $A > B$.

1) Start a list with A then B. Define $A = r_1$ and $B = r_2$.

2) To get r_{n+1}, subtract r_n from r_{n-1} over and over until you get a number smaller than r_n. This new number is r_{n+1}. That is, $r_{n+1} = r_{n-1} - jr_n$ for some j. A simpler way to say this is: r_{n+1} is the remainder of $r_{n-1} \div r_n$.

3) If r_{n+1} isn't zero, then go to step two. If it is zero, then the last non-zero number is the gcd.

Example: $gcd(20, 12) =?$

$r_1 = 20$

$r_2 = 12$

$r_3 = 8 \quad 20 = 1 \cdot 12 + 8$

$r_4 = 4 \quad 12 = 1 \cdot 8 + 4$

$r_5 = 0 \quad 8 = 2 \cdot 4 + 0$

So, gcd(12,20) = 4.

Example: $gcd(531, 702) =?$

$r_1 = 702$

$r_2 = 531$

$r_3 = 171$

$r_4 = 18 \quad 531 = 3 \cdot 171 + 18$

$r_5 = 9 \quad 171 = 9 \cdot 18 + 9$

$r_6 = 0$

Q 1.1.1: $gcd(52584, 87452) =?$

Q 1.1.2: $gcd(15646, 5124) =?$

Q 1.1.3: $gcd(0.4, 3) =?$

Q 1.1.4: $gcd(\sqrt{18}, \sqrt{8}) =?$
Hint: Simplify the radicals first.

Q 1.1.5: $gcd(3, \sqrt{2}) =?$
Hint: Use a calculator. This is a kinda a trick question.

Q 1.1.6: $gcd(F_n, F_{n+1}) =?$, where F_n and F_{n+1} are consecutive Fibonacci numbers.

Q 1.1.7: $gcd(F_n, F_{n+2}) =?$

Q 1.1.8: $gcd(F_n, F_{n+3}) =?$

Q 1.1.9: Qualitatively, why is $gcd(93, 15)$ quick to find and $gcd(93, 57)$ slow to find, using the algorithm?

Q 1.1.10: Clearly, on average, Euclid's algorithm should take longer the larger A and B are. After all, if A and B are both small it can't take *too* many steps.

-Does Euclid's algorithm work slowest if A and B are nearly equal, one is much smaller than the other, or somewhere in between?

-Can you construct a worst-case scenario? That is, how would you find a pair of fairly small numbers with the maximum possible number of steps?

Q 1.1.11: Using your answer to the last question, for a given N, what is the maximum number of steps you need to take if $A, B < N$?

1.2 proof!

In a nutshell; every step in the algorithm produces a new number that is smaller and retains all of the divisors common to both A and B. So, the last number it can produce is the gcd, since the gcd(A,B) is by definition the smallest number with all the common divisors of A and B. The more rigorous proof isn't necessary to use Euclid's algorithm, but it is a good exercise.

For any pair of numbers, x and q, you can find unique numbers j and r, such that $x = jq + r$ where $r < q$. For example, with $x = 14$ and $q = 5$, you'll find $14 = 2 \cdot 5 + 4$.

Assume $B < A$, and set $A = r_1$ and $B = r_2$. Then $A = j_3B + r_3$ for some j_3 and r_3. In the algorithm, r_3 is the first new number generated. In turn, $B = j_4r_3 + r_4$. Continuing the algorithm creates a string of numbers, $r_1, r_2, \cdots, r_{n-1}, r_n$ where $r_n = 0$ and $r_{n-1} = gcd(A, B)$. This needs an example: $gcd(702, 531)$.

string of numbers	as equations	original
$r_1 = 702$		
$r_2 = 531$		
$r_3 = 171$	$r_1 = 1 \cdot r_2 + r_3$	$702 = 1 \cdot 531 + 171$
$r_4 = 18$	$r_2 = 3 \cdot r_3 + r_4$	$531 = 3 \cdot 171 + 18$
$r_5 = 9$	$r_3 = 9 \cdot r_4 + r_5$	$171 = 9 \cdot 18 + 9$
$r_6 = 0$	$r_4 = 2 \cdot r_5 + r_6$	$18 = 2 \cdot 9 + 0$

So, $r_4 = 0$ and $r_3 = 9$, which is the gcd of 702 and 531. The fact that n=6 is completely unimportant. Also, in general the values of the j's can also be ignored.

Step1: Say $d|A$, $d|B$ (this says "d divides A" and "d divides B"). We know that $A = j_3B + r_3$, so $A - j_3B = r_3$. But since d divides all of the left side it must divide all of the right side. So $d|r_3$. In the next step of the algorithm, $B = j_4r_3 + r_4$. Doing the same thing, $B - j_4r_3 = r_4$, and we find that $d|r_4$. Doing the same thing over and over we find that d divides all the r's, including r_{n-1}. Now since d can be any divisor of both A and B, including $gcd(A, B)$. Therefore, since d divides r_{n-1}, it can't be larger than r_{n-1}, so we know that $gcd(A, B) \leq r_{n-1}$.

Step2: This is where the fact that $r_n = 0$ becomes important. The last step of the algorithm looks like $r_{n-2} = j_nr_{n-1} + r_n$. But $r_n = 0$, so $r_{n-2} = j_nr_{n-1}$. But this is just another way of saying that $r_{n-1}|r_{n-2}$. That is, since r_{n-2} is equal to r_{n-1} times some number, then by definition r_{n-1} is a divisor of r_{n-2}. In turn, $r_{n-3} = j_{n-1}r_{n-2} + r_{n-1} = j_{n-1}(j_nr_{n-1}) + r_{n-1} = (j_{n-1}j_n + 1)r_{n-1}$. We don't know what $(j_{n-1}j_n + 1)$ is, but it doesn't matter. What does matter is that $r_{n-1}|r_{n-3}$. Repeating the same trick you can continue along *inductively* and find that $r_{n-1}|r_{n-4}$ and $r_{n-1}|r_{n-5}$ and $r_{n-1}|r_{n-6}$ and $\cdots$ and $r_{n-1}|r_3$ and $r_{n-1}|B$ and $r_{n-1}|A$. Now, since r_{n-1} divides both A and B, then by definition it divides $gcd(A, B)$. But that means that $r_{n-1} \leq gcd(A, B)$.

Step3: In step 1 we found that $r_{n-1} \geq gcd(A, B)$, and in step 2 we found that $r_{n-1} \leq gcd(A, B)$. Therefore, $r_{n-1} = gcd(A, B)$. That is, when using Euclid's algorithm, the last non-zero term you get must be the gcd. $\square$

1.3 Linear Diophantine Equations

A linear diophantine equation is an equation of the form $xA + yB = d$ where A, B, and d are constant integers. For example, $2x + 5y = 3$.

Solving a Diophantine equation means finding integer values for x and y that satisfy the equation.

Example: Find a solution to $4x + 6y = 2$
$x = -1$ and $y = 1$

Q 1.3.1: Find a solution to $5x + 3y = 9$.

Q 1.3.2: Find a solution to $6x + 8y = 10$.

Q 1.3.3: Find a solution to $6x + 8y = 9$.

Q 1.3.4: Find a solution to $15x + 6y = 24$.

Q 1.3.5: Find a solution to $12x + 15y = 10$.

Q 1.3.6: Find a solution to $30x + 45y = 60$.

Q 1.3.7: Find a solution to $30x + 45y = 70$.

Note that in order for there to be solutions, d must be a multiple of $gcd(A, B)$.

Q 1.3.8: For a given Diophantine equation of the form $xA + yB = d$, where x and y are integer solutions:
-Show that if $s \mid A$ and $s \mid B$, then $s \mid d$.
-Show that $gcd(A, B) \mid d$

The expression "$xA + yB$" is called a "linear combination of A and B". So, since $d = xA + yB$, the last question was really a proof that if $s \mid A$ and $s \mid B$, then s divides any linear combination of A and B (with integer coefficients, x and y).

Every step in Euclid's algorithm produces a new number, r_k, that's just a linear combination of r_{k-1} and r_{k-2}. But both of those numbers are linear combinations of earlier numbers, which are linear combinations of earlier numbers, and so on. As a result, every r_k is some linear combination of A and B (r_1 and r_2). So the $gcd(A, B)$ itself is some linear combination of A and B. By using Euclid's algorithm, and carefully keeping track of how many A's and B's there are, you can quickly find solutions to Diophantine equations of the form $xA + yB = gcd(A, B)$.

Q 1.3.9: Show that a linear combination of a linear combination of A and B is a linear combination of A and B.

Example: Find a solution to $18x + 39y = 3$.
$A = 39$, $B = 18$

$r_1 = 39$		$r_1 = 1A + 0B$
$r_2 = 18$		$r_2 = 0A + 1B$
$r_3 = 3$	$r_3 = r_1 - 2 \cdot r_2$	$r_3 = 1A - 2B$
$r_4 = 0$	$r_4 = r_2 - 6 \cdot r_3$	

So, $18 \cdot (-2) + 39 \cdot 1 = 3$, and therefore $x = -2$, and $y = 1$.

Example: Find a solution to $703x + 540y = 1$.
$A = 703$, $B = 540$

$r_1 = 703$		$r_1 = 1A + 0B$
$r_2 = 540$		$r_2 = 0A + 1B$
$r_3 = 163$	$r_3 = r_1 - 1 \cdot r_2$	$r_3 = 1A - 1B$
$r_4 = 51$	$r_4 = r_2 - 3 \cdot r_3$	$r_4 = -3A + 4B$
$r_5 = 10$	$r_5 = r_3 - 3 \cdot r_4$	$r_5 = 10A - 13B$
$r_6 = 1$	$r_6 = r_4 - 5 \cdot r_5$	$r_6 = -53A + 69B$
$r_7 = 0$	$r_7 = r_5 - 10 \cdot r_6$	

So, $703 \cdot (-53) + 540 \cdot 69 = 1$, and therefore $x = -53$, and $y = 69$.

To find answers to more general Diophantine equations of the form $xA+yB = d$, where d is a multiple of $gcd(A, B)$, you just multiply by the appropriate amount. In the case in which d is not a multiple of $gcd(A, B)$ there are no solutions at all.

Example: Find a solution to $39x + 22y = 5$.
$A = 39$, $B = 22$

$r_1 = 39$		$r_1 = 1A + 0B$
$r_2 = 22$		$r_2 = 0A + 1B$
$r_3 = 17$	$r_3 = r_1 - 1 \cdot r_2$	$r_3 = 1A - 1B$
$r_4 = 5$	$r_4 = r_2 - 1 \cdot r_3$	$r_4 = -1A + 2B$
$r_5 = 2$	$r_5 = r_3 - 3 \cdot r_4$	$r_5 = 4A - 7B$
$r_6 = 1$	$r_6 = r_4 - 2 \cdot r_5$	$r_6 = -9A + 16B$
$r_7 = 0$	$r_7 = r_5 - 2 \cdot r_6$	

So, $39 \cdot (-9) + 22 \cdot 16 = 1$. Multiplying both sides by 5 we get, $39 \cdot (-45) + 22 \cdot 80 = 5$, and therefore $x = -45$, and $y = 80$.

Q 1.3.10: $374x + 231y = 11$, ind a solution for x and y.

Q 1.3.11: $6x + 45y = 3$, find a solution for x and y.

Q 1.3.12: $213x + 744y = 3$, solve for x and y.

Q 1.3.13: $32x + 39y = 6$, solve for x and y.

Q 1.3.14: In general, what is the solution to $Ax + By = d$, when $d = 0$, for a given A and B?

Q 1.3.15: If (for a given A, B, and d) $Ax + By = d$ has a solution, is that solution unique? If not, how would you construct new solutions?

1.4 Hodgepodge of questions

Q 1.4.1: $A > B$, $gcd(A, B) = 1$, and $2 \mid A$ or $2 \mid B$, both not both.
Show that $gcd(A + B, A - B) = 1$

Q 1.4.2: Show that any fraction of the form $\frac{21N+4}{14N+3}$ is already in lowest terms.

Q 1.4.3: $gcd(7! + 4!, 5!) =?$

Q 1.4.4: $gcd((N + 3)! + N!, (N + 1)!) =?$

Q 1.4.5: $gcd(N! + M!, K!) =?$

Q 1.4.6: -Find a solution for $6x + 5y = 7$.
-Setting S as your solution for x, and T as your solution for y, what do Q and R have to be in order for $x = kQ + S$, $y = kR + T$ to be solutions for all values of k?

Q 1.4.7: Show that F_{m+n} is a linear combination of F_n and F_m, where the F's are Fibonacci numbers.

Q 1.4.8: Show that $F_n \mid F_{kn}$ for any integer k.

Q 1.4.9: Show that $gcd(F_n, F_m) = F_{gcd(n,m)}$. This means that, for example, $gcd(F_3, F_6) = gcd(2, 8) = 2 = F_3 = F_{gcd(3,6)}$

Q 1.4.10: -Describe how you would extend the Euclid's algorithm technique for solving Diophantine equations of the form "$d = xA + yB$", to solving Diophantine equations of the form "$d = xA + yB + zC$".
-When are there no solutions to this new kind of equation?
-How would you generate new solutions?
-Use your technique to find a solution for $3x - 14y + 2z = 5$, where $xyz \neq 0$.

Q 1.4.11: Show that if $gcd(A, B) = 1$, then:
-The smallest value of k for which $\frac{kA}{B}$ is an integer is $k = B$.
-The remainder of $\frac{kA}{B}$ is different for every value of k for $k = 1, 2, 3, \cdots, B$.

"$\lfloor x \rfloor$" means the "take the integer part of x", so $\lfloor \pi \rfloor = \lfloor 3.5 \rfloor = \lfloor 3 \rfloor = \lfloor 3.9999999 \rfloor = 3$.

Q 1.4.12: Prove that if $gcd(A, B) = 1$, then
$\lfloor \frac{A}{B} \rfloor + \lfloor \frac{2A}{B} \rfloor + \lfloor \frac{3A}{B} \rfloor + \cdots + \lfloor \frac{(B-1)A}{B} \rfloor = \frac{1}{2}(A - 1)(B - 1)$