greatest common divisor

The *greatest common divisor* of $a, b \in \mathbb{N}^+$ is denoted $\gcd(a, b)$. (Some texts use the notation (a, b) but that just seems too confusing.)

Euclid devoted part of his great work on geometry, the *Elements*, to what would today be called number theory. He described, in particular, an algorithm for finding the greatest common divisor of two positive integers. For about 2,000 years, this remained the most important, most studied, and as a matter of fact, *only* algorithm in mathematics. (Gaussian elimination came next!)

The fascinating aspect of the Euclidean algorithm is that it is fast and does not involve prime numbers or prime factorizations.
In fact, it is used to *prove* properties of prime factorizations.

the Euclidean algorithm for the greatest common divisor

Note that for all $a, b, k \in \mathbb{Z}$,

$$\gcd(a, b) = \gcd(a + kb, b)$$

since anything that divides *both* a and b divides both $a + kb$ and b, and vice versa.

Euclidean algorithm Given: $a, b \in \mathbb{N}^+$.

Say $a \geqslant b$. Divide a by b with remainder:

$$a = q_0 b + r_0$$

where $0 \leqslant r_0 < b$.

If $r_0 = 0$ then $\gcd(a, b) = b$. Otherwise, note that $\gcd(a, b) = \gcd(b, r_0)$. Repeat.

The smaller of the two numbers whose gcd is being sought, decreases strictly at each step. It will hit 0 eventually and then the algorithm stops. The gcd is the number *just before* the 0.

the Euclidean algorithm with balanced remainders

When dividing by d, one can choose remainders from other complete sets of representatives (just as long as the absolute value of the remainder is less than that of the modulus).

Computationally, the best choice are *balanced remainders*:

$$\left\{\lfloor\frac{d}{2}\rfloor - d + 1, \ldots, -2, -1, 0, 1, 2, \ldots, \lfloor\frac{d}{2}\rfloor\right\}$$

$$\text{that is,} \quad a = qd + r \quad \text{with } |r| \leqslant \frac{d}{2}$$

This choice guarantees that $\gcd(a, b)$ is found within $\log_2(\min\{a, b\})$ steps.

the "extended" Euclidean algorithm

Start with $a \geqslant b$. If

$$r_0 := a$$

$$r_1 := b$$

$$r_2 := r_0 \pmod{r_1}$$

$$\dots$$

$$r_i := r_{i-2} \pmod{r_{i-1}}$$

$$\dots$$

is a run of the Euclidean algorithm then each of the remainders r_i is expressible in turn as an integer linear combination of a and b. Since $\gcd(a, b)$ is one of those remainders (the last non-zero one!) this can be used to find integers x, y that satisfy

$$ax + by = \gcd(a, b)$$

summary of our work so far

- The Euclidean algorithm is a fast process to find $\gcd(a, b)$. (The Euclidean algorithm with balanced remainders is even faster.)
- For any integers a, b, there exist integers x, y such that $\gcd(a, b) = ax + by$. These integers x, y can be found by working through the Euclidean algorithm.
- It follows that if $k|a$ and $k|b$ then $k|\gcd(a, b)$.

  That is, the greatest common divisor of a and b is not only the *biggest* of all the common divisors of a and b. It is actually a *multiple* of all the common divisors of a and b.

relatively prime integers

If $\gcd(a, b) = 1$ then a and b are said to be *relatively prime* or *coprime*. This means they have no divisors in common (other than ± 1).

a and b are relatively prime if and only if $ax + by = 1$ for some integers x, y.

relatively prime integers

If $\gcd(a, b) = 1$ then a and b are said to be *relatively prime* or *coprime*. This means they have no divisors in common (other than ± 1).

a and b are relatively prime if and only if $ax + by = 1$ for some integers x, y.

Lemma (Euclid)

If $a|bc$ and a and b are relatively prime then $a|c$.

relatively prime integers

If $\gcd(a, b) = 1$ then a and b are said to be *relatively prime* or *coprime*. This means they have no divisors in common (other than ± 1).

a and b are relatively prime if and only if $ax + by = 1$ for some integers x, y.

Lemma (Euclid)

If $a|bc$ and a and b are relatively prime then $a|c$.

Indeed, $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Since a divides bc, it divides $byc = (1 - ax)c = c - axc$. Therefore it divides c.

This 'simple' lemma is the driving force behind the theory of primes and divisibility. The trick is that one can prove Euclid's lemma *without* appealing to the notion of prime factorization.

primes

$n \in \mathbb{N}^+$ is called *composite* if $n = n_1 \cdot n_2$ where $1 < n_1 < n$ and $1 < n_2 < n$. (That is, n has a "proper factorization".)

$p \in \mathbb{N}^+$ is a prime number if $p > 1$ and p is not composite. That is, whenever $p = ab$ (with $a, b \in \mathbb{N}^+$) then $a = 1$ or $b = 1$.

Note: under this classification, 0 is neither prime nor composite, and 1 is neither prime nor composite. These conventions actually make life nicer. Among the integers, 1 and -1 are called *units* or *invertible elements*, since their inverse is an integer too.

primes

$n \in \mathbb{N}^+$ is called *composite* if $n = n_1 \cdot n_2$ where $1 < n_1 < n$ and $1 < n_2 < n$. (That is, n has a "proper factorization".)

$p \in \mathbb{N}^+$ is a prime number if $p > 1$ and p is not composite. That is, whenever $p = ab$ (with $a, b \in \mathbb{N}^+$) then $a = 1$ or $b = 1$.

Note: under this classification, 0 is neither prime nor composite, and 1 is neither prime nor composite. These conventions actually make life nicer. Among the integers, 1 and -1 are called *units* or *invertible elements*, since their inverse is an integer too.

If p is prime then

$$\gcd(p, a) = \begin{cases} 1 & \text{if } p \nmid a \\ p & \text{if } p \mid a \end{cases}$$

If p is prime and $p|ab$ then $p|a$ or $p|b$.

Indeed, if $p \nmid a$ then $\gcd(p, a) = 1$ so $p|b$ by Euclid's lemma.

prime factorization

Any $n \in \mathbb{N}^+$ can be written as a product

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$$

where the factors p_i are primes.

Indeed, if n is not already a prime then $n = ab$ for $a, b \in \mathbb{N}^+$, $a < n$, $b < n$.

Continue. Cannot continue *forever*.

uniqueness of prime factorization

Suppose p_i, $i = 1, 2, \ldots, n$ and q_j, $j = 1, 2, \ldots, m$ are primes such that

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$$

Then $n = m$ and, after a possible rearrangement, the sequence of p_i is the same as the sequence of q_j.

Indeed, p_1 divides the left-hand product so divides $q_1 \cdot q_2 \cdot \ldots \cdot q_m$. That is only possible if $p_1 = q_{j_1}$ for some $1 \leqslant j_1 \leqslant m$. Divide both sides by p_1 and iterate.

divisibility and prime factorization

Let

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$$

$$m = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$$

where the p_i are distinct primes and $a_i, b_j \in \mathbb{N}$.

Then $n|m$ if and only if $a_i \leqslant b_i$ for all $i = 1, 2, \dots, k$.

gcd and prime factorization

Let

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$$

$$m = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$$

where the p_i are distinct primes.

Then

$$\gcd(n, m) = p_1^{c_1} p_2^{c_2} p_3^{c_3} \dots p_k^{c_k}$$

where $c_i = \min\{a_i, b_i\}$ for $1 \leqslant i \leqslant k$.

lcm and prime factorization

Let

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$$

$$m = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$$

where the p_i are distinct primes.

Then

$$\operatorname{lcm}(n, m) = p_1^{c_1} p_2^{c_2} p_3^{c_3} \dots p_k^{c_k}$$

where $c_i = \max\{a_i, b_i\}$ for $1 \leqslant i \leqslant k$.

relation between gcd and lcm

For all $n, m \in \mathbb{N}^+$,

$$\gcd(n, m) \cdot \operatorname{lcm}(n, m) = n \cdot m$$

From the prime decompositions given on the previous two slides, this follows from

$$\min\{a, b\} + \max\{a, b\} = a + b$$

valid whether $a < b$ or $a = b$ or $a > b$.

Homework Problem 7

Let a and b be positive integers such that $a \mid n$ and $b \mid n$.

Show that $\text{lcm}(a, b) \mid n$.

Justify your answer.

Due Thu, Sept 19, in class.

Homework Problem 8

Let a and b be positive integers such that a^3 divides b^2.

Does it follow that a divides b?

Justify your answer.

Due Thu, Sept 19, in class.

solving $ax + by = c$

Let $a, b, c \in \mathbb{Z}$ be given. Goal: find all $x, y \in \mathbb{Z}$ so that

$$ax + by = c$$

solving $ax + by = c$

Let $a, b, c \in \mathbb{Z}$ be given. Goal: find all $x, y \in \mathbb{Z}$ so that

$$ax + by = c$$

Suppose $\gcd(a, b) \nmid c$. Then there is *no* solution.

solving $ax + by = c$

Let $a, b, c \in \mathbb{Z}$ be given. Goal: find all $x, y \in \mathbb{Z}$ so that

$$ax + by = c$$

Suppose $\gcd(a, b) \nmid c$. Then there is *no* solution.

If $\gcd(a, b) \mid c$, one can divide throughout by $\gcd(a, b)$:

$$Ax + By = C$$

where $A = \frac{a}{\gcd(a,b)}$, $B = \frac{b}{\gcd(a,b)}$, $C = \frac{c}{\gcd(a,b)}$.

Note that $\gcd(A, B) = 1$. So there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$Ax_0 + By_0 = 1$$

solving $ax + by = c$

So there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$Ax_0 + By_0 = 1$$

$$A(Cx_0) + B(Cy_0) = C$$

so $x_1 = Cx_0$, $y_1 = Cy_0$ give *one* set of solutions to the equation.

What are *all* the solutions to $Ax + By = C$?

solving $ax + by = c$

What are *all* the solutions to $Ax + By = C$?

Subtracting $Ax_1 + By_1 = C$,

$$A(x - x_1) + B(y - y_1) = 0$$

So $A \mid B(y - y_1)$. Since $\gcd(A, B) = 1$, $A \mid (y - y_1)$.

So $y = y_1 + kA$ for some $k \in \mathbb{Z}$. So $x = x_1 - kB$.

$$x = x_1 - kB$$

$$y = y_1 + kA$$

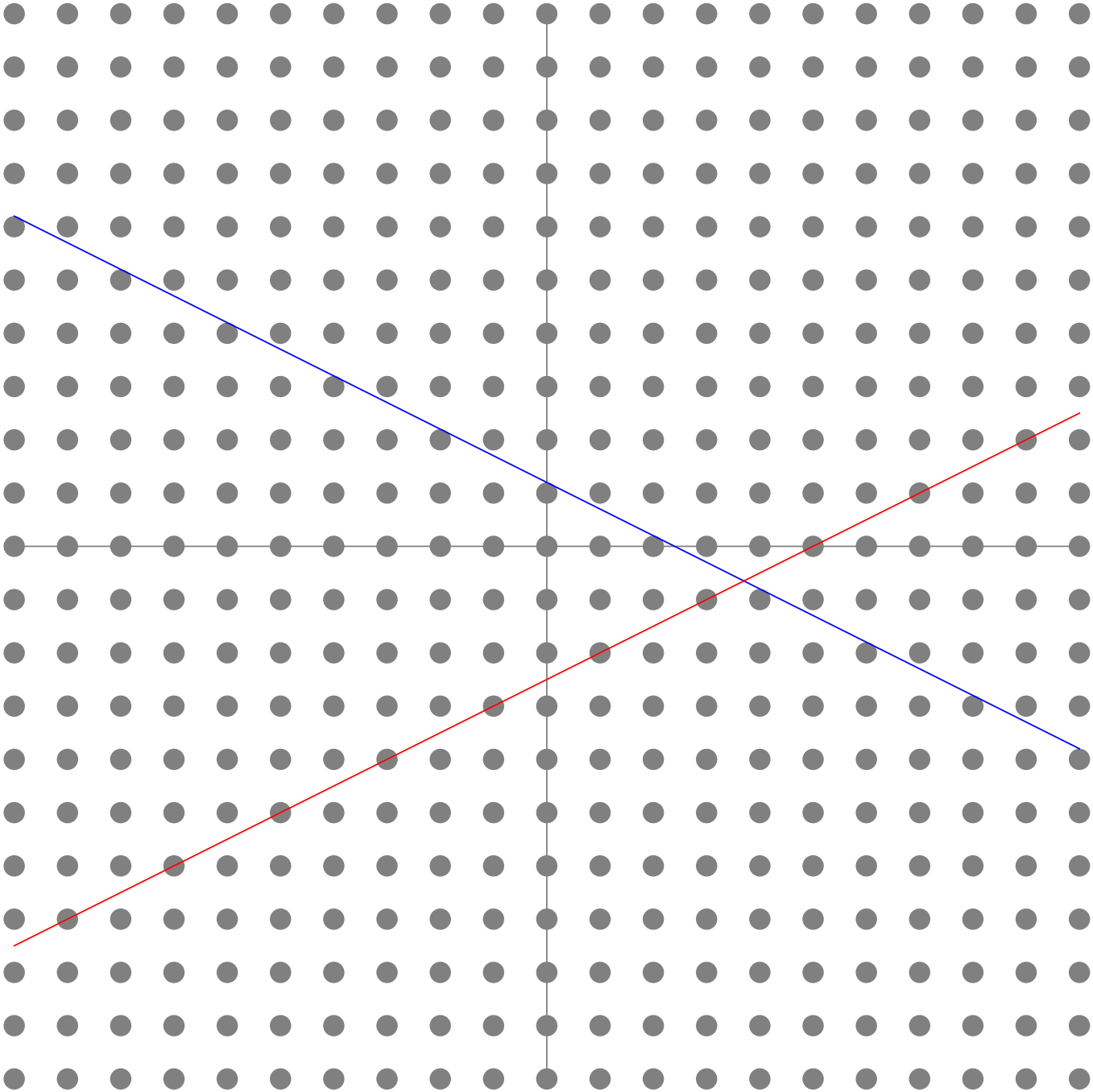
give *all* the solutions, where x_1, y_1 is one particular set of solutions (these need to be found separately!) and $k \in \mathbb{Z}$ is arbitrary.

Diophantine equations

$$ax + by = c$$

was our first example of a *Diophantine* equation (named after the Greek mathematician Diophantus, 3rd century CE). Diophantine equations are algebraic equations with integer coefficients, such that one seeks *integer* solutions only.

Our solution has a geometric interpretation. $ax + by = c$ is the equation of a straight line whose x- and y-intercepts are rational numbers. (Thus, it has a rational slope.) We've shown that such a line either misses all points with integer coordinates in $\mathbb{R}^2$, or goes through infinitely many lattice points, spaced periodically.



Homework Problem 9

From your textbook:

Klain: Essential Number Theory, Exercise 8.4 on page 41.

Due Thu, Sept 19, in class.

Homework Problem 10

In Smurfland, there are 5-dollar and 12-dollar bills in circulation. There are no other types of paper bills and no coins either.

Show that Smurfs can make cash payments of n dollars, for any integer amount n that is 44 or larger.

PS: Assume that Smurfs can print as many \$5 and \$12 bills as necessary, but *only* \$5 and \$12 bills.

Due Thu, Sept 19, in class.

how *slow* can the Euclidean algorithm be?

Let's count the number of steps of the algorithm as follows. Recall that 4983 and 1056 are the inputs, and 33 is the output.

4983	
1056	
759	$\leftarrow$ step 1
297	$\leftarrow$ step 2
165	
132	...
33	
0	$\leftarrow$ step 6

Homework Problem 11* (optional)

Find the *smallest* pair of integers on which the Euclidean algorithm takes exactly 10 steps.

PS: "smallest pair" means that if the inputs are n, m with $n \geqslant m$, then n should be as small as possible.

* Due (optionally) Thu, Sept 26, in class.

Fibonacci sequence

Set $F_0 = 0$, $F_1 = 1$ and thereafter

$$F_n = F_{n-1} + F_{n-2}$$

Homework Problem 12

(a) What is $\gcd(F_n, F_{n+1})$?

(b) What is $\gcd(F_n, F_{n+2})$?

Justify your answer.

Due Thu, Sept 19, in class.

Binet's formula

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

Homework Problem 13

Set $\phi = \frac{1+\sqrt{5}}{2}$.

(a) Show that

$$\lim_{n\to\infty} \left(F_n - \frac{1}{\sqrt{5}}\phi^n\right) = 0$$

(b) Show that for any $n \geqslant 0$, F_n is the integer closest to the value of $\frac{1}{\sqrt{5}}\phi^n$.

Due Thu, Sept 19, in class.

where we are in your textbooks

- gcd, Euclidean algorithm: Klain Ch. 6; Santos section 5.1
- relatively prime integers: Klain Ch. 7
- linear diophantine equations: Klain Ch. 8
- unique factorization: Klain Ch. 9; Santos Ch. 4
- Fibonacci numbers: Santos section 1.4