Prime Numbers

- A **prime number** is an integer $n > 1$ whose only positive divisors are 1 and n. An integer greater than 1 which is not prime is **composite**.
- Euclid showed that there are infinitely many primes.
- The **Prime Number Theorem** says that the number of primes less than or equal to a real number x is approximately $\dfrac{x}{\ln x}$.
- The **Sieve of Eratosthenes** finds prime numbers by trial division.

Definition. An integer greater than 1 is **prime** if its only positive factors are 1 and itself. An integer greater than 1 which is not prime is **composite**.

The prime numbers are the "building blocks" of the integers. I'll make this more precise later when I discuss the **Fundamental Theorem of Arithmetic**.

Lemma. Every integer greater than 1 is divisible by at least one prime.

Proof. I'll prove the result by induction. To begin with, the result is true for $n = 2$, since 2 is prime.

Take $n > 2$, and assume the result is true for all integers greater than 1 but less than n. I want to show that the result holds for n. If n is prime, it's divisible by a prime — namely itself! So suppose n is composite. Then n has a positive factor a other than 1 and n. Suppose $n = ab$.

If $a > n$, then since $b \geq 1$, I get $n = ab > n \cdot 1 = n$ ↯. Thus, $a \leq n$, and since $a \neq n$, I have in fact $a < n$. Since $a \neq 1$, I get $1 < a < n$.

By the induction hypothesis, a has a prime factor p. But $p \mid a$ and $a \mid n$ implies $p \mid n$, so n has a prime factor as well. This shows that the result is true for all $n > 1$ by induction. □

Theorem. (Euclid) There are infinitely many prime numbers.

Proof. Suppose on the contrary that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Look at

$$p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1.$$

This number is not divisible by any of the primes $p_1, p_2, \ldots, p_n$, because it leaves a remainder of 1 when divided by any of them. But the previous lemma says that every number greater than 1 is divisible by a prime ↯. This contradiction implies that there can't be finitely many primes — that is, there are infinitely many. □

If you are trying to factor a number n, you do not need to try dividing by all the numbers from 1 to n: It's enough to go up to $\sqrt{n}$. This is the idea of the next lemma.

Lemma. Every composite number has a proper factor less than or equal to its square root.

Proof. Suppose n is composite. I can write $n = ab$, where $1 < a, b < n$. If both $a, b > \sqrt{n}$, then

$$n = \sqrt{n} \cdot \sqrt{n} < a \cdot b = n. \text{↯}$$

So at least one of a, b must be less than or equal to $\sqrt{n}$. □

In fact, you can adapt the preceding proof to show that a composite number must have a *prime* factor less than or equal to its square root.

For an arbitrary number that is several hundred digits in length, it may be impossible with current technology to determine whether the number is prime. In fact, many **cryptographic systems** depend on the difficulty of factoring large numbers.

Example. To see whether 127 is prime, I only need to see if it has a prime factor $\leq \sqrt{127} \approx 11.27$. You can do the arithmetic to verify that 127 isn't divisible by 2, 3, 5, 7, or 11. Hence, it must be prime. □

Example. (**The Sieve of Eratosthenes**) The sieve is a method for generating a list of primes by hand. Write down the integer beginning with 2. Go through the list, crossing out every integer divisible by 2. Then go through the list, crossing out every integer divisible by 3. Keep going. I've illustrated the first two passes below.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

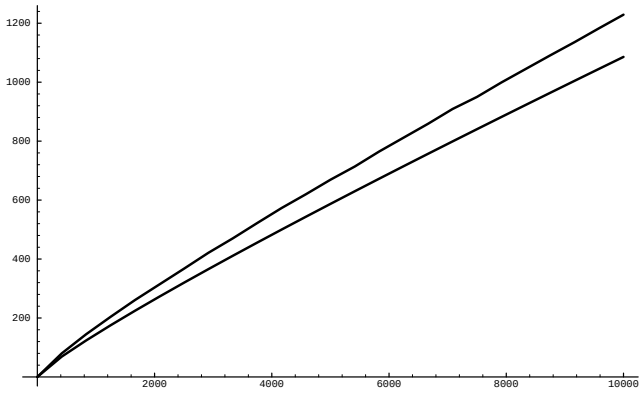
By the square root criterion above, I've already found all the primes less than 10, namely 2, 3, 5, and 7. After crossing out all the numbers divisible by 5, I'll have all the primes up to 25. And so on. Of course, more sophisticated sieve methods are used in practice. □

I showed above that there are infinitely many primes. How are they distributed? That is, are they evenly distributed, or do they get "sparser" as you look at bigger and bigger integers? The **Prime Number Theorem** gives an aymptotic estimate for $\pi(x)$, the number of primes less than or equal to x. It says:

$$\lim_{x \to +\infty} \frac{\pi(x)}{\dfrac{x}{\ln x}} = 1.$$

The picture below was generated by *Mathematica*, the symbolic mathematics program. It shows the

graphs of $\pi(x)$ and $\dfrac{x}{\ln x}$.



The graph of $\pi(x)$ is on top and the graph of $\dfrac{x}{\ln x}$ is on the bottom.

The Prime Number Theorem was first conjectured by Legendre and Gauss. The first rigorous proofs were given by Hadamard and de la Vallee Poussin around 1896. Elementary proofs were given by Atle Selberg and Paul Erdös in the 1930's.

On the other hand, there are "lots" of composite numbers around. For example,

$$1001! + 2, 1001! + 3, 1001! + 4, \ldots, 1001! + 1001$$

is a run of 1000 consecutive composite numbers. You can use the same method to generate runs of composite numbers of any length.

Example. Use the Prime Number Theorem to estimate the number of primes less than 1000000.

By the Prime Number Theorem,

$$\pi(1000000) \approx \frac{1000000}{\ln 1000000} \approx 72382.$$

The actual number of primes less than 1000000 is $\pi(1000000) = 78498$. □

On the other hand, many problems concerning the distribution of primes are unsolved. For example, there are primes that come in pairs (two units apart), such as 11 and 13, or 71 and 73. These are called **twin primes**.

Question: (**Twin Prime Conjecture**) Are there infinitely many twin primes?

There are enormously large twin primes known. The largest known in 2001 were

$$318032361.2^{107001} \pm 1,$$

which were discovered by David Underbakke and Phil Carmody. They are numbers having 32220 digits! The Twin Prime Conjecture is still unresolved: A proof was announced in 2004, but a gap was found, and the question remains open.

Greatest Common Divisors

- The **greatest common divisor** (m, n) of integer m and n is the largest integer which divides both m and n.
- The greatest common divisor can be found using the **Euclidean algorithm**, which is a process of repeated division.
- The greatest common divisor (m, n) of m and n is a **linear combination** of m and n.
- m and n are **relatively prime** if $(m, n) = 1$.

Definition. The **greatest common divisor** of two integers (not both zero) is the largest integer which divides both of them.

If a and b are integers (not both 0), the greatest common divisor of a and b is denoted (a, b).

(In Britain, the greatest common divisor is often called the **highest common factor**.)

Examples. $(4, 6) = 2$, $(17, 17) = 17$, $(42, 0) = 42$, $(12, -15) = 3$. □

Once and for all, in discussions of the greatest common divisor all the variables will denote integers, and it's understood that in (a, b) at least one of a and b is nonzero.

Proposition. (a) $(a, b) \geq 1$.

(b) $(a, b) = (|a|, |b|)$.

(c) $(a, 0) = |a|$.

Proof. (a) Since $1 \mid a$ and $1 \mid b$, (a, b) must be at least as big as 1.

(b) $x \mid a$ if and only if $x \mid -a$; that is, a and $-a$ have the same factors. But $|a|$ is either a or $-a$, so a and $|a|$ have the same factors. Likewise, b and $|b|$ have the same factors. Therefore, x is a common factor of a and b if and only if it's a common factor of $|a|$ and $|b|$. Hence, $(a, b) = (|a|, |b|)$.

(c) (By the convention I stated earlier, when I write "$(a, 0)$" I'm implying that $a \neq 0$.)

By (b), I have $(a, 0) = (|a|, 0)$.

I have $|a| \mid 0$, since $|a| \cdot 0 = 0$. Obviously, $|a| \mid |a|$. Thus, $|a|$ is a common divisor of $|a|$ and 0. Therefore, it's less than or equal to the greatest common divisor, so $|a| \leq (|a|, 0)$.

However, $(|a|, 0) \mid |a|$, and since these are both positive numbers, I must have $(|a|, 0) \leq |a|$.

Putting the two inequalities together, I have $(|a|, 0) = |a|$. Together with my earlier equation I have $(a, 0) = (|a|, 0) = |a|$. □

Definition. a and b are **relatively prime** if $(a, b) = 1$.

For example, 49 and 54 are relatively prime, but 25 and 105 are not.

Proposition. If $d = (m, n)$, then $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

Proof. Suppose $m = da$ and $n = db$. Then

$$\left(\frac{m}{d}, \frac{n}{d}\right) = (a, b).$$

Suppose that $p > 0$ and $p \mid a$, $p \mid b$. Then I can find e and f such that

$$a = pe \quad \text{and} \quad b = pf.$$

Thus,

$$m = dpe \quad \text{and} \quad n = dpf.$$

This shows that dp is a common divisor of m and n. Since d is the *greatest* common divisor, $d \geq dp$. Therefore, $1 \geq p$, so $p = 1$ (since p was a positive integer).

I've proven that 1 is the *only* positive common divisor of a and b. Therefore, 1 is the greatest common divisor of a and b:

$$\left(\frac{m}{d}, \frac{n}{d}\right) = (a, b) = 1. \quad \square$$

Proposition. $(m, n) = (m + kn, n)$ for any integer k.

Proof. First, if x is a common factor of m and n, then $x \mid m$ and $x \mid n$. So $x \mid kn$, and hence $x \mid m + kn$. Thus, x is a common factor of $m + kn$ and n.

Conversely, if x is a common factor of $m + kn$ and n, then $x \mid (m + kn)$ and $x \mid n$. Therefore, $x \mid kn$, so $x \mid [(m + kn) - kn] = m$. That is, x is a common factor of m and n.

Since m, n and $m + kn$, n have the same set of common divisors, the two pairs must have the same greatest common divisor. $\square$

Example. $(42, 24) = 6$, and if I add a multiple of 24 to 42, the greatest common divisor will still be 6. For instance,

$$(42 + 5 \cdot 24, 24) = (162, 24) = 6. \quad \square$$

The last result says that I don't change the greatest common divisor if I add or subtract multiples of one member of the pair from the other. This yields the following **recursive procedure** for computing the greatest common divisor.

Euclidean Algorithm. Begin with a pair of nonnegative integers $\{m, n\}$, not both 0. (The absolute value property I stated earlier shows that there's no harm in assuming the integers are nonnegative.)

1. If one of the numbers is 0, the other is the greatest common divisor of the pair. (Stop.)
2. Otherwise, apply the Division Algorithm to write $m = qn + r$, where $0 \leq r < n$.
3. Replace the pair $\{m, n\}$ with the pair $\{n, r\}$.
4. Go to step 1.

At each step, both elements are ≥ 0, and each pass through step 3 decreases the second element. Since the second element always gets smaller, but can't be negative, Well-Ordering implies that algorithm must terminate in an $\{m, 0\}$ pair (in step 2) after a finite number of steps.

The preceding property shows that these steps produce new pairs of numbers *with the same greatest common divisor as the previous pairs.* Therefore, when the algorithm terminates, the greatest common divisor I've found is the greatest common divisor of the original pair.

Example. Use the Euclidean algorithm to compute $(124, 348)$.

Write the pair as $\{348, 124\}$.

Equation	Pair of numbers

$348 = 2 \cdot 124 + 100$ $\{124, 100\}$

$124 = 1 \cdot 100 + 24$ $\{100, 24\}$

$100 = 4 \cdot 24 + 4$ $\{24, 4\}$

$24 = 6 \cdot 4 + 0$ $\{4, 0\}$

At this point, one of the numbers is 0, so the greatest common divisor is the other number: $(348, 124) = 4$. □

Example. You can also form the greatest common divisor of more than two numbers, in the obvious way. For instance, $(42, 105, 91) = 7$. □

Definition. If x and y are numbers, a **linear combination** of x and y (with integer coefficients) is a number of the form

$$ax + by, \quad \text{where} \quad a, b \in \mathbb{Z}.$$

Example. $29 = 2 \cdot 10 + 1 \cdot 9$ shows that 29 is a linear combination of 10 and 9. $7 = (-2) \cdot 10 + 3 \cdot 9$ shows that 7 is a linear combination of 10 and 9 as well.

The next result is extremely important, and is often used in proving things about greatest common divisors.

Theorem. (m, n) is the smallest positive linear combination of m and n. In particular, there are integers a and b (not necessarily unique) such that

$$(m, n) = am + bn.$$

Example. I showed above that $(348, 124) = 4$. The theorem says that there are integers a and b such that

$$4 = a \cdot 348 + b \cdot 124.$$

In fact,

$$4 = 5 \cdot 348 + (-14) \cdot 124.$$

This combination is not unique. For example,

$$4 = 129 \cdot 348 + (-362) \cdot 124. \quad \square$$

I'll give a few easy corollaries before proving the theorem.

Corollary. If $d \mid m$ and $d \mid n$, then $d \mid (m, n)$.

Proof.

$$(m, n) = am + bn \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

Therefore, $d \mid m$ and $d \mid n$, then $d \mid (am + bn = (m, n)$. □

This says that the greatest common divisor is not only "greatest" in terms of *size*; it's also "greatest" in the sense that any other common factor must *divide* it.

Corollary. m and n are relatively prime if and only if

$$am + bn = 1 \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

Proof. ($\Rightarrow$) Suppose m and n are relatively prime. Then $(m, n) = 1$. By the theorem,

$$(m, n) = am + bn \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

Therefore,

$$am + bn = 1 \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

($\Leftarrow$) Suppose

$$am + bn = 1 \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

This says that 1 is a positive linear combination of m and n, so (since 1 is the smallest positive integer) it's the *smallest* positive linear combination of m and n. By the theorem, this implies that 1 is the greatest common divisor, and m and n are relatively prime. □

Proof of the theorem. I'll use the Euclidean algorithm.

The initial pair $\{m, n\}$ consists of two numbers m and n. Each of these numbers is a linear combination of m and n.

The only changes the algorithm makes are to switch the elements or to subtract a multiple of one element from the other. I have to show that neither changes the fact that the two elements are linear combinations of m and n.

If two elements are each linear combinations of m and n, this obviously remains true if I the swap the elements.

For subtracting a multiple, suppose I have the pair $\{x, y\} = \{am + bn, cm + dn\}$. I divide x by y:

$$x = qy + r, \quad \text{where} \quad 0 \leq r < y.$$

The new pair is

$$\{y, r\} = \{y, x - qy\} = \{cm + dn, (am + bn) - q(cm + dn)\} = \{cm + dn, (a - qc)m + (b - qd)n\}.$$

Each element of this new pair is a linear combination of m and n.

I know the algorithm terminates in $\{(m, n), 0\}$. It follows that (m, n) must be a linear combination of m and n.

Now suppose p is a positive linear combination of m and n:

$$p = am + bn \quad \text{for some} \quad a, b \in \mathbb{Z}.$$

$(m, n) \mid m$ and $(m, n) \mid n$, so $(m, n) \mid p$. Both of these numbers are positive, so $(m, n) \leq p$. Since (m, n) is smaller than any positive linear combination of m and n, (m, n) must be the *smallest* positive linear combination of m and n. □

Example. $(42, 105) = 21$, so the theorem asserts that the set of all linear combinations of 42 and 105 — that is, the set of all numbers of the form $42a + 105b$ — is

$$\ldots, -42, -21, 0, 21, 42, 63, \ldots.$$

Notice that the greatest common divisor is the smallest positive element of this set.

If you know a little group theory, you may recognize this as the result that *subgroups of cyclic groups are cyclic.* □

The Extended Euclidean Algorithm

- The **Extended Euclidean Algorithm** finds integers a and b such that $(m, n) = am + bn$.
- The **backward recurrence** is an implementation of the Extended Euclidean Algorithm. This implementation is well suited for hand computation.

The **Euclidean algorithm** is an efficient way of computing the greatest common divisor of two numbers. It also provides a way of finding numbers a, b, such that

$$(x, y) = ax + by.$$

The Euclidean Algorithm. Take $m, n > 0$. Define

$$r_0 = m, \quad r_1 = n.$$

Then recursively define r_k using the Division Algorithm:

$$r_{k-2} = qr_{k-1} + r_k, \quad \text{where} \quad 0 \leq r_k < r_{k-1}.$$

The inequality $0 \leq r_k < r_{k-1}$ shows that the r_k's form a decreasing sequence of nonnegative integers. It follows that the algorithm must terminate.

Example. Compute $(1914, 899)$.

$$\begin{aligned} 1914 &= 2 \cdot 899 + 116 \\ 899 &= 7 \cdot 116 + 87 \\ 116 &= 1 \cdot 87 + 29 \\ 87 &= 3 \cdot 29 + 0 \end{aligned}$$

The greatest common divisor is the last nonzero remainder: $(1914, 899) = 29$.

By an earlier result, the greatest common divisor 29 must be a linear combination $a \cdot 1914 + b \cdot 899$. Here's how to find integers a and b which work. Simply work backwards through the equations above, *treating the r_k's as if they were variables.*

$$29 = 116 + (-1) \cdot 87 \quad \text{and} \quad 87 = 899 + (-7) \cdot 116.$$

Substituting for 87 in the first equation,

$$29 = 116 + (-1) \cdot [899 + (-7) \cdot 116] = (-1) \cdot 899 + 8 \cdot 116.$$

But

$$116 = 1914 + (-2) \cdot 899.$$

Substituting for 116, I find that

$$29 = (-1) \cdot 899 + 8 \cdot [1914 + (-2) \cdot 899] = 8 \cdot 1914 + (-17) \cdot 899.$$

I've written the greatest common divisor 29 as a linear combination of the original numbers 1914 and 899. □

While you can use this back-substitution approach to write the greatest common divisor as a linear combination of the original numbers, it's rather tedious. Here's a better way. I'll write it more formally, since the steps are a little complicated.

Terminology. If a and b are things, a **linear combination** of a and b is something of the form $sa + tb$, where s and t are numbers. (The kind of "number" depends on the context.)

I proved the next result earlier, but this proof will actually give an algorithm which constructs a linear combination. It is called a *backward recurrence*, and appeared in a paper by S. P. Glasby [1]. It will look a little complicated, but you'll see that it's really easy to use in practice.

Theorem. (a, b) is a linear combination of a and b: $(a, b) = sa + tb$ for some integers s and t.

Warning: s and t are not unique.

Proof. (a, b) is only defined if at least one of a, b is nonzero. If $a \neq 0$, $(a, 0) = a$ and $a = 1 \cdot a + 0 \cdot 0$. This proves the result if one of the numbers is 0, so I may as well assume both are nonzero. Moreover, since $(a, b) = (|a|, |b|)$, I can assume both numbers are positive.

Suppose $a \geq b$. Apply the Euclidean Algorithm to $a_0 = a$ and $a_1 = b$, and suppose that a_n is the last *nonzero* remainder:

$$\begin{aligned}
a_0 &= a_1 q_1 + a_2, \quad \text{where} \quad 0 \leq a_2 < a_1 \\
a_1 &= a_2 q_2 + a_3, \quad \text{where} \quad 0 \leq a_3 < a_2 \\
&\vdots \\
a_k &= a_{k+1} q_{k+1} + a_{k+2}, \quad \text{where} \quad 0 \leq a_{k+2} < a_{k+1} \\
&\vdots \\
a_{n-1} &= a_n q_n + 0.
\end{aligned}$$

I'm going to define a sequence of numbers y_n, y_{n-1}, $\ldots y_1$, y_0. They will be constructed recursively, *starting with y_n, y_{n-1} and working downward to y_0*. (This is why this is called a *backward recurrence*.)

Define $y_n = 0$ and $y_{n-1} = 1$. Then define

$$y_{k-1} = q_k y_k + y_{k+1} \quad \text{for} \quad k = n-2, \ldots, 2, 1.$$

Now I claim that

$$(-1)^{n+k+1} a_{k-1} y_k + (-1)^{n+k} a_k y_{k-1} = a_n \quad \text{for} \quad 1 \leq k \leq n.$$

I will prove this by *downward* induction, starting with $k = n$ and working downward to $k = 1$.

For $k = n$, I have

$$(-1)^{2n+1} a_{n-1} y_n + (-1)^{2n} a_n y_{n-1} = -a_{n-1} y_n + a_n y_{n-1} = -a_{n-1} \cdot 0 + a_n \cdot 1 = a_n.$$

The result holds for $k = n$.

Next, suppose $1 < k < n$. Suppose the result holds for $k + 1$, i.e.

$$(-1)^{n+k+2} a_k y_{k+1} + (-1)^{n+k+1} a_{k+1} y_k = a_n.$$

I want to prove the result for k. Substitute $y_{k+1} = y_{k-1} - q_k y_k$ in the preceding equation and simplify:

$$a_n = (-1)^{n+k+2} a_k y_{k+1} + (-1)^{n+k+1} a_{k+1} y_k = (-1)^{n+k+2} a_k (y_{k-1} - q_k y_k) + (-1)^{n+k+1} a_{k+1} y_k =$$

$$(-1)^{n+k} a_k (y_{k-1} - q_k y_k) + (-1)^{n+k+1} a_{k+1} y_k = (-1)^{n+k} a_k y_{k-1} + (-1)^{n+k+1} a_k q_k y_k + (-1)^{n+k+1} a_{k+1} y_k =$$

$$(-1)^{n+k} a_k y_{k-1} + (a_k q_k + a_{k+1})(-1)^{n+k+1} y_k = (-1)^{n+k} a_k y_{k-1} + (-1)^{n+k+1} a_{k-1} y_k.$$

This proves the result for k, so the result holds for $1 \le k \le n$, by downward induction.
In particular, for $k = 1$, the result says

$$a_n = (-1)^{n+1} a_1 y_0 + (-1)^{n+2} a_0 y_1 = (-1)^{n+1} a_1 y_0 + (-1)^n a_0 y_1 = \left[(-1)^n y_1\right] a_0 + \left[(-1)^{n+1} y_0\right] a_1.$$

Since $a_n = (a_0, a_1)$, I've expressed (a_0, a_1) as a linear combination of a_0 and a_1. □

There are many algorithms (like the one in the proof) which produce a linear combination. I'll call this algorithm the **Extended Euclidean Algorithm**.

Example. In this example, I'll show how you can use the algorithm in the proof to obtain a linear combination. I'll arrange the computations in the form of a table; the table is simply an extension of the table I used for the Euclidean algorithm.

Here's how you start:

a	q	y
187	-	
102		

(You can save a step by putting the larger number first.)

The a and q columns are filled in using the Euclidean algorith, i.e. by successive division: Divide the next-to-the-last a by the last a. The quotient goes into the q-column, and the remainder goes into the a-column.

a	q	y
187	-	
102	1	
85		

Divide 187 by 102;
Quotient 1, remainder 85.

a	q	y
187	-	
102	1	
85	1	
17		

Divide 102 by 85;
Quotient 1, remainder 17.

When the division comes out evenly, you stop. In this case, 85 divided by 17 is 5, with remainder 0.

a	q	y
187	-	
102	1	
85	1	
17	5	

The last entry in the a-column is the greatest common divisor. Thus, $(187, 102) = 17$.

The y-column is filled in from bottom to top. Always start with 0 for the last y and 1 for the next-to-the-last y.

a	q	y
187	-	
102	1	
85	1	1
17	5	0

Then, working from bottom to top, fill in the y's using the rule

$$(\text{next } y) = (\text{last } q) \cdot (\text{last } y) + (\text{next-to-last } y).$$

It's probably easier to show than it is to explain:

a	q	y
187	-	
102	1	1
85	1	1
17	5	0

$1 \cdot 1 + 0 = 1$

a	q	y
187	-	2
102	1	1
85	1	1
17	5	0

$1 \cdot 1 + 1 = 2$

To get the linear combination, form the products diagonally and subtract one from the other:

a	q	y
187	-	2
102	1	1
85	1	1
17	5	0

Thus,

$$17 = (187, 102) = (2)(102) - (1)(187).$$

How do you know the order for the subtraction? The proof gives a formula, but the easiest thing is to pick one of the two ways, then fix it if it isn't right. If you subtract "the wrong way", you'll get a negative number. For example,

$$(1)(187) - (2)(102) = -17.$$

Since I know the greatest common divisor should be 17 — it's the last number in the a-column — I just multiply this equation by -1:

$$(-1)(187) + (2)(102) = 17.$$

This way, you don't need to memorize the exact formula. □

Example. Compute $(246, 194)$ and express it as a linear combination of 246 and 194.

a	q	y
246	-	52
194	1	41
52	3	11
38	1	8
14	2	3
10	1	2
4	2	1
2	2	0

Thus,

$$2 = (246, 194) = 52 \cdot 194 - 41 \cdot 246. \quad \square$$

I think this algorithm is the best for *hand* computation. For implementation on a computer, it has a drawback: You need to store all the Euclidean algorithm quotients and remainders, because you need to work your way backward up the table. There is another version of this algorithm which only requires that you save a couple of table lines at a time; it is not as good for hand computation, since you need two helper variables x and y at each step.

---

[1] S. P. Glasby, Extended Euclid's algorithm via backward recurrence relations, *Mathematics Magazine*, 72(3)(1999), 228–230.