The Fundamental Theorem of Arithmetic

- The **Fundamental Theorem of Arithmetic** says that every integer greater than 1 can be factored uniquely into a product of primes.
- **Euclid's lemma** says that if a prime divides a product of two numbers, it must divide at least one of the numbers.
- The **least common multiple** $[a, b]$ of nonzero integers a and b is the smallest positive integer divisible by both a and b.

Theorem. (**Fundamental Theorem of Arithmetic**) Every integer greater than 1 can be written in the form

$$p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

where $n_i \geq 0$ and the p_i's are distinct primes. The factorization is unique, except possibly for the order of the factors.

The Fundamental Theorem of Arithmetic was probably first stated by Gauss in *Disquisitiones arithmeticae*, his famous treatise on number theory. It's possible that earlier mathematicians were aware that the result was true, but never bothered to write down the result explicitly.

Example.

$$4312 = 2 \cdot 2156 = 2 \cdot 2 \cdot 1078 = 2 \cdot 2 \cdot 2 \cdot 539 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 77 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 7 \cdot 11.$$

That is,

$$4312 = 2^3 \cdot 7^2 \cdot 11. \quad \square$$

I need a couple of lemmas in order to prove the uniqueness part of the Fundamental Theorem. In fact, these lemmas are useful in their own right.

Lemma. If $m \mid pq$ and $(m, p) = 1$, then $m \mid q$.

Proof. Write

$$1 = (m, p) = am + bp \quad \text{for some } a, b \in \mathbb{Z}.$$

Then

$$q = amq + bpq.$$

Now $m \mid amq$ and $m \mid bpq$ (since $m \mid pq$), so $m \mid (amq + bpq) = q$. $\square$

Lemma. If p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i.

For $n = 2$, the result says that if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. This is often called **Euclid's lemma**; it is Proposition 30 in Book VII of Euclid's *Elements*. Euclid expressed it this way: "If two numbers, multiplied by one another make some number, and any prime number measures the product, then it also measures one of the original numbers."

Proof. Obviously, if $p \mid a_1$ then $p \mid a_1$: The case $n = 1$ is trivial.

I need to do the case $n = 2$ separately because I'll use it in my induction step. Therefore, suppose $p \mid a_1 a_2$, and suppose $p \not\mid a_1$. I must show $p \mid a_2$.

Now p is prime and $p \not\mid a_1$, so $(p, a_1) = 1$. (The only factors of p are 1 and p, and p doesn't divide a_1, so 1 is the only common factor — hence the greatest common factor.) Now $p \mid a_2$ by the preceding lemma. This establishes the result for $n = 2$.

Assume $n > 2$, and assume the result is true for products of fewer than n a_i's. Suppose that $p \mid a_1 a_2 \cdots a_n$. I have to show that p divides on of the a's.

By grouping the terms, I have

$$p \mid (a_1 a_2 \cdots a_{n-1}) a_n.$$

By the case $n = 2$, either $p \mid a_1 a_2 \cdots a_{n-1}$ or $p \mid a_n$. If $p \mid a_n$, I'm done. Otherwise, if $p \mid a_1 a_2 \cdots a_{n-1}$, then p divides one of a_1, a_2, ..., a_{n-1}, by induction. In either case, I've shown that p divides one of the a_i's, which completes the induction step and the proof. □

Proof. (**Fundamental Theorem of Arithmetic**) First, I'll use induction to show that every integer greater than 1 can be expressed as a product of primes.

$n = 2$ is prime, so the result is true for $n = 2$.

Suppose $n > 2$, and assume every number less than n can be factored into a product of primes. If n is prime, I'm done. Otherwise, n is composite, so I can factor n as $n = ab$, where $1 < a, b < n$. By induction, a and b can be factored into primes. Then $n = ab$ show that n can, too.

Now I'll prove the uniqueness part of the Fundamental Theorem.

Suppose

$$p_1^{m_1} \cdots p_j^{m_j} = q_1^{n_1} \cdots q_k^{n_k},$$

where the p's are distinct primes, the q's are distinct primes, and all the exponents are greater than or equal to 1. I want to show that $j = k$, and that each $p_a^{m_a}$ is $q_b^{n_b}$ for some b — that is, $p_a = q_b$ and $m_a = n_b$.

Look at p_1. It divides the left side, so it divides the right side. By the last lemma, $p_1 \mid q_i^{n_i}$ for some i. But $q_i^{n_i}$ is $q_i \cdots q_i$ (n_i times), so again by the last lemma, $p_1 \mid q_i$. Since p_1 and q_i are prime, $p_1 = q_i$.

To avoid a mess, renumber the q's so q_i becomes q_1 and vice versa. Thus, $p_1 = q_1$, and the equation reads

$$p_1^{m_1} \cdots p_j^{m_j} = p_1^{n_1} \cdots q_k^{n_k}.$$

If $m_1 > n_1$, cancel $p_1^{n_1}$ from both sides, leaving

$$p_1^{m_1 - n_1} \cdots p_j^{m_j} = q_2^{n_2} \cdots q_k^{n_k}.$$

This is impossible, since now p_1 divides the left side, but not the right.

For the same reason $m_1 < n_1$ is impossible.

It follows that $m_1 = n_1$. So I can kill the p_1's off both sides, leaving

$$p_2^{m_2} \cdots p_j^{m_j} = q_2^{n_2} \cdots q_k^{n_k}.$$

Keep going. At each stage, I pair up a power of a p with a power of a q, and the preceding argument shows the powers are equal. I can't wind up with any primes left over at the end, or else I'd have a product of primes equal to 1. So everything paired up, and the original factorizations were the same (except possibly for the order of the factors). □

Example. The **least common multiple** of nonzero integers a and b is the smallest positive integer divisible by both a and b. The least common multiple of a and b is denoted $[a, b]$.

For example,

$$[6, 4] = 12, \quad [33, 15] = 165.$$

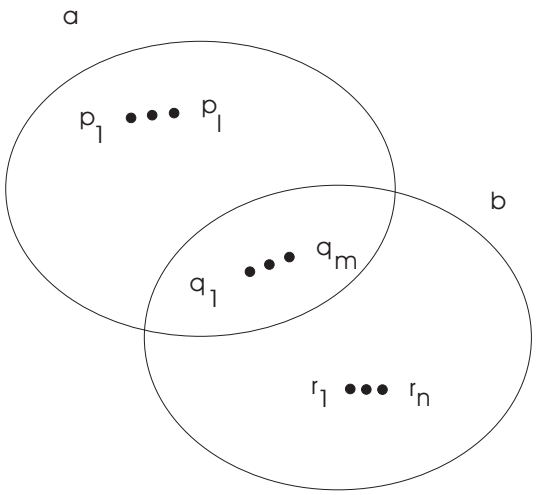
Here's an interesting fact that is easy to derive from the Fundamental Theorem:

$$[a, b](a, b) = ab.$$

Factor a and b in products of primes, but write out all the powers (e.g. write 2^3 as $2 \cdot 2 \cdot 2$):

$$a = p_1 \cdots p_l q_1 \cdots q_m, \quad b = q_1 \cdots q_m r_1 \cdots r_n.$$

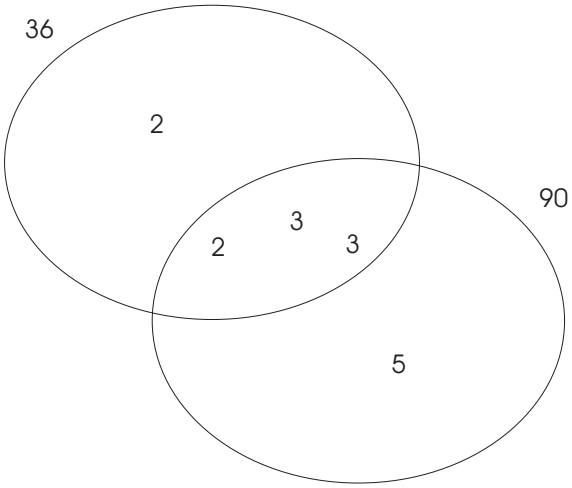
Here the q's are the primes a and b have in common, and the p's and r don't overlap. Picture:



From the picture,

$$(a, b) = q_1 \cdots q_m, \quad [a, b] = p_1 \cdots p_l q_1 \cdots q_m r_1 \cdots r_n, \quad ab = p_1 \cdots p_l q_1^2 \cdots q_m^2 r_1 \cdots r_n.$$

Thus, $[a, b](a, b) = ab$.
Here's how this result looks for 36 and 90:



$(36, 90) = 18$, $[36, 90] = 180$, and $36 \cdot 90 = 32400 = 18 \cdot 180$. □

Divisibility Tests and Factoring

- There are simple tests for divisibility by small numbers such as 2, 3, 5, 7, and 9. These tests involve performing operations on the decimal representation of the number to be tested for divisibility.
- **Fermat factorization** attempts to factor a number by representing it as the difference of two squares.
- The **Fermat numbers** are numbers of the form $F_n = 2^{2^n} + 1$.

First, I'll discuss quick ways for deciding whether a number is divisible by various small integers. In what follows, I'll assume that numbers are represented as strings of decimal digits (i.e. in base 10) as usual.

1. An integer is divisible by 2 if and only if its last digit is divisible by 2.
2. An integer is divisible by 5 if and only if its last digit is 0 or 5.

   The proofs for these two tests are nearly identical; I'll do the one for divisibility by 2 as an example. Suppose the decimal representation of x is

   $$x_n x_{n-1} \ldots x_2 x_1 x_0.$$

   That is, x_0 is the units digit, x_1 is the tens digit, and so on. For 1728,

   $$x_3 = 1, x_2 = 7, x_1 = 2, x_0 = 8.$$

   Then

   $$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_1 \cdot 10 + x_0.$$

   Since $2 \mid 10$, it follows that $2 \mid 10^n$ for $n \geq 1$. Thus, $2 \mid x$ if and only if $2 \mid x_0$ — that is, x is even if and only if the units digit x_0 is even.

Definition. The **digital sum** of an integer is the result of applying the function

$$\text{SUM}(n) = (\text{the sum of the digits in } n)$$

iteratively until the result is less than 10.

Example. The digital sum of 1728 is 9:

$$1 + 7 + 2 + 8 = 18, \quad 1 + 8 = 9.$$

The digital sum of 278349 is 6:

$$2 + 7 + 8 + 3 + 4 + 9 = 33, \quad 3 + 3 = 6. \quad \square$$

---

3. An integer is divisible by 3 if and only if its digital sum is divisible by 3.
4. An integer is divisible by 9 if and only if its digital sum is divisible by 9.

   I'll prove the test for divisibility by 9 as an example. Suppose the decimal representation of x is

   $$x_n x_{n-1} \ldots x_2 x_1 x_0.$$

Then

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_1 \cdot 10 + x_0.$$

The sum of the digits of x is

$$s = x_n + x_{n-1} + \cdots + x_1 + x_0.$$

Observe that

$$x - s = \left(x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_1 \cdot 10 + x_0\right) - (x_n + x_{n-1} + \cdots + x_1 + x_0) =$$

$$x_n(10^n - 1) + x_{n-1}(10^{n-1} - 1) + \cdots + x_1(10 - 1).$$

The right side is divisible by 9, because

$$10 - 1 = 9, 10^2 - 1 = 99, 10^3 - 1 = 999, \text{ and so on.}$$

That is,

$$x - s = \text{something divisible by 9.}$$

Hence, if $9 \mid x$, then $9 \mid s$, and if $9 \mid s$, then $9 \mid x$.

I'm not quite done, because s isn't the digital sum — it's simply the sum of the digits in x, and if *this sum* has more than one digit, I have to sum its digits, and so on. But the argument above applied to s shows that $9 \mid s$ if and only if 9 divides the sum of the digits of s. And 9 divides the sum of the digits of s if and only if 9 divides the sum of the digits of the sum of the digits of s. And so on, till I reach the digital sum.

Thus, $9 \mid x$ if and only if 9 divides the digital sum of x.

5. To test divisibility by 7, remove the last (units) digit, double it, and subtract it from the remainder of the number. The original number is divisible by 7 if and only if the result is divisible by 7.

Example. ~~9423242~~ is divisible by 2 and by 9. Here's how the divisibility by 7 test looks for this number:

$$942324 - 2 \cdot 2 = 942320,$$

$$94232 - 2 \cdot 0 = 94232,$$

$$9423 - 2 \cdot 2 = 9419,$$

$$941 - 2 \cdot 9 = 923,$$

$$92 - 2 \cdot 3 = 86.$$

86 is not divisible by 7, so 942324 is not divisible by 7. □

It is difficult to factor a large, arbitrary integer in a reasonable amount of time. You can use simple divisibility tests like those above to deal with "obvious" cases, but the general problem is the object of current research. Here's a useful idea which is called **Fermat factorization**.

Proposition. Let n be an odd integer. There is a one-to-one correspondence

$$\left\{\begin{array}{c}\text{factorizations}\\ \text{of } n\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{expressions of } n \text{ as the}\\ \text{difference of two squares}\end{array}\right\}$$

Proof. If $n = ab$, n is odd so a and b are odd. Then $a+b$ and $a-b$ are even, so $\dfrac{a+b}{2}$ and $\dfrac{a-b}{2}$ are integers. Now

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

expresses n as a difference of two squares.

Conversely, suppose n is written as as difference of squares: $n = s^2 - t^2$. Then

$$n = (s-t)(s+t)$$

is a factorization of n.

You can check that these two procedures — factors to difference and difference to factors — "undo" one another. □

Example. Use Fermat factorization to factor 4819.

The idea is to try to write 4819 as $s^2 - t^2$. I will form $s^2 - 4819$ and increase s till I get a perfect square. What s's do I need to use?

First, $\sqrt{4819} \approx 69.4$. Since $4819 = s^2 - t^2$, s must be at least as big as $69.4 \approx 70$.

On the other hand, the factorization with the biggest factor is $4819 = 1 \cdot 4819$. By the proof of the last result, this would produce an s of the form $\dfrac{4819+1}{2} = 2410$. So I need to try s for $70 \le s \le 2410$.

On the very first try,

$$70^2 - 4819 = 4900 - 4819 = 81 = 9^2.$$

Thus, $s = 70$ and $t = 9$. $s + t = 79$, $s - t = 61$, and $79 \cdot 61 = 4819$. □

Example. Use Fermat factorization to factor 779.

$\sqrt{779} \approx 27.91057$, so I need $s \ge 28$. $\dfrac{779+1}{2} = 390$, so $s \le 390$.

$$28^2 - 779 = 5,$$

$$29^2 - 779 = 62,$$

$$30^2 - 779 = 121 = 11^2.$$

The factors are $30 + 11 = 41$ and $30 - 11 = 19$: $779 = 41 \cdot 19$. □

The **Fermat numbers** are numbers of the form

$$F_n = 2^{2^n} + 1.$$

Fermat thought that all the F_n were prime. However, it turns out that $641 \mid F_5 = 2^{32} + 1$. Note that

$$641 = 2^4 + 5^4 \quad \text{and} \quad 641 = 2^7 \cdot 5 + 1.$$

Therefore,

$$2^7 \cdot 5 = 641 - 1, \text{ and so } 2^{28} \cdot 5^4 = (641-1)^4 = 641 \cdot \text{junk} + 1.$$

On the other hand, $5^4 = 641 - 2^4$, so

$$2^{28} \cdot (641 - 2^4) = 641 \cdot \text{junk} + 1,$$

$$641 \cdot 2^{28} - 2^{32} = 641 \cdot \text{junk} + 1,$$

$$2^{32} + 1 = 641 \left(2^{28} - \text{junk}\right).$$

This proves that $641 \mid 2^{32} + 1$.

Here are some properties of the Fermat numbers.

Proposition. If p is prime and $p \mid F_n$, then $p = k \cdot 2^{n+2} + 1$ for some k. □

I won't prove this result, since the proof requires some stuff about quadratic residues which I won't discuss for a while. Here's how it can be used.

Example. $F_4 = 2^{2^4} + 1 = 65537$. Here $n = 4$, so all prime divisors must have the form $k \cdot 2^6 + 1 = 64k + 1$. There are around 1024 numbers less than 65537 of this form, but I only need to check numbers up to the square root: $\sqrt{65537} \approx 256$.

There are only 4 numbers of the form $64k + 1$ less than 256: 1, 65, 129, and 193. 1 is a trivial factor, while 65 and 129 aren't prime. 193 *is* prime, but it doesn't divide 65537. Conclusion: 65537 must be prime! □

Proposition. $F_0F_1 \cdots F_{n-1} = F_n - 2$ for $n > 0$.

Proof. I'll prove the result by induction. $F_0 = 3$ and $F_1 = 5$, so $F_0 = F_1 - 2$. The result is true for $n = 1$.

Take $n > 0$, and assume the result is true for n; I'll try to prove it for $n + 1$. By assumption,

$$F_0F_1 \cdots F_{n-1} = F_n - 2, \quad \text{so} \quad F_0F_1 \cdots F_{n-1}F_n = (F_n - 2)F_n.$$

Now

$$(F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2 \cdot 2^n} - 1 = 2^{2^{n+1}} - 1 = 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2.$$

That is,

$$F_0F_1 \cdots F_{n-1}F_n = F_{n+1} - 2.$$

This is the statement for $n + 1$, so the proof is complete, by induction. □

Proposition. If $m \neq n$, $(F_m, F_n) = 1$.

Proof. Assume $m < n$ (if not, switch m and n). Suppose p is prime and $p \mid F_m$ and $p \mid F_n$. I have

$$F_n - 2 = F_0F_1 \cdots F_{n-1}, \quad \text{so} \quad F_n - F_0F_1 \cdots F_{n-1} = 2.$$

Note that $p \mid F_0F_1 \cdots F_{n-1}$, since $p \mid F_m$ and $m < n$ implies that F_m is one of the F's in this product. Since $p \mid F_n$, the equation above shows that $p \mid 2$. Since p is prime, this means that $p = 2$. But this is impossible, since all the F_n's are odd.

Therefore, there is no prime dividing both F_m and F_n, and hence $(F_m, F_n) = 1$. □

Linear Diophantine Equations

- A **Diophantine equation** is an equation which is to be solved over the integers.
- A linear Diophantine equation of the form

$$ax + by = c$$

has solutions if and only if $(a, b) \mid c$. There is a similar result for linear Diophantine equations in more than 2 variables.

A **Diophantine problem** is one in which the solutions are required to be integers. Abusing terminology, I'll refer to **Diophantine equations**, meaning equations which are to be solved over the integers.

Diophantine equations have occupied mathematicians for centuries. L. E. Dickson's three-volume *History of the Theory of Numbers* [1] and L. J. Mordell's *Diophantine Equations* [2] contain extensive lists of equations with their solutions.

Example. The equation $x^2 + y^2 = z^2$ has many integer solutions — for example $x = 3$, $y = 4$, and $z = 5$. A solution to this equation is called a **Pythagorean triple**, since (in case x, y and z are positive) the numbers represent the sides of a right triangle.

$x^3 + y^3 = z^3$ has many solutions over the reals; for example,

$$x = 1, \quad , y = 1, \quad z = \sqrt[3]{2}.$$

However, this equation has no nonzero integer solutions. This is a special case of **Fermat's Last Theorem**. It says that the equation $x^n + y^n = z^n$ has no nonzero integer solutions if $n \geq 3$. After remaining unproven for over 300 years, it was finally settled in 1993 by Andrew Wiles. □

Example. Since $(9, 100) = 1$, the Extended Euclidean Algorithm can be used to find integers x and y such that $9x + 100y = 1$.

For example, $9 \cdot (-11) + 100 \cdot 1 = 1$, and $9 \cdot 89 + 100 \cdot (-8) = 1$. That is, the Diophantine equation $9x + 100y = 1$ has solutions — in fact, infinitely many solutions. □

Linear equations are the simplest kind of equations. This result tells when a 2-variables linear Diophantine equation is solvable.

Theorem. Let $a, b, c \in \mathbb{Z}$. Consider the Diophantine equation

$$ax + by = c.$$

(a) If $(a, b) \nmid c$, there are no solutions.

(b) If $(a, b) = d \mid c$, there are infinitely many solutions of the form

$$x = \frac{b}{d}k + x_0, \quad y = -\frac{a}{d}k + y_0.$$

Here (x_0, y_0) is a particular solution, and $k \in \mathbb{Z}$.

Proof. Consider the linear Diophantine equation

$$ax + by = c.$$

Case 1. Suppose $(a, b) \nmid c$. If x and y solve the equation, then

$$(a, b) \mid ax + by = c. \quad \lightning$$

Hence, there cannot be a solution.

Case 2. Suppose $(a, b) \mid c$. Write $c = k(a, b)$ for $k \in \mathbb{Z}$. There are integers m and n such that

$$am + bn = (a, b).$$

Then

$$amk + bnk = (a, b)k = c.$$

Hence, $x = km$, $y = kn$, is a solution.
Suppose $x = x_0$, $y = y_0$, is a particular solution. Then

$$a\left(\frac{b}{d}k + x_0\right) + b\left(-\frac{a}{d}k + y_0\right) = \frac{ab}{d}k - \frac{ab}{d}k + (ax_0 + by_0) = 0 + c = c.$$

This proves that $x = \dfrac{b}{d}k + x_0$, $y = -\dfrac{a}{d}k + y_0$ is a solution for every $k \in \mathbb{Z}$.
Finally, I want to show that every solution has this form. Suppose then that (x, y) is a solution. Then $ax + by = c$ and $ax_0 + by_0 = c$ imply

$$a(x - x_0) + b(y - y_0) = c - c = 0.$$

Therefore,

$$\frac{a}{(a, b)}(x - x_0) + \frac{b}{(a, b)}(y - y_0) = 0,$$

$$\frac{a}{(a, b)}(x - x_0) = -\frac{b}{(a, b)}(y - y_0).$$

Now $\dfrac{a}{(a, b)}$ divides the left side, so it divides the right side. However, $\left(\dfrac{a}{(a, b)}, \dfrac{b}{(a, b)}\right) = 1$. Therefore,

$$\frac{a}{(a, b)} \mid y - y_0, \quad \text{or} \quad y - y_0 = k \cdot \frac{a}{(a, b)} \text{ for some } k.$$

Thus,

$$y = y_0 + k \cdot \frac{a}{(a, b)}.$$

Substitute this back into the last x-y equation:

$$\frac{a}{(a, b)}(x - x_0) = -\frac{b}{(a, b)}(y - y_0) = -\frac{b}{(a, b)}k \cdot \frac{a}{(a, b)},$$

$$x - x_0 = -k \cdot \frac{b}{(a, b)},$$

$$x = x_0 - k \cdot \frac{b}{(a, b)}.$$

This is the result stated in the theorem (with an unimportant switch of k and $-k$.) $\square$

Example. Solve $6x + 9y = 5$.

Since $(6, 9) = 3 \not| 5$, the equation has no solutions. □

Example. Solve $6x + 9y = 21$.

Since $(6, 9) = 3 \mid 21$, there are infinitely many solutions. By trial and error, $x_0 = -7$, $y_0 = 7$, is a particular solution. Hence, the general solution is

$$x = 3k - 7, \quad y = -2k + 7.$$

For example, setting $k = 5$ produces the solution $x = 8$, $y = -3$. □

Example. Solve $71x + 45y = 32$.

Since $(71, 45) = 1 \mid 32$, there are infinitely many solutions. But how can I find a particular solution? Use the Extended Euclidean Algorithm to write $1 = (71, 45)$ as a linear combination of 71 and 45:

a	q	y
71	-	30
45	1	19
26	1	11
19	1	8
7	2	3
5	1	2
2	2	1
1	2	0

I have

$$\begin{aligned} 71 \cdot (-19) + 45 \cdot 30 &= 1 \\ 32(71 \cdot (-19) + 45 \cdot 30) &= 32 \cdot 1 \\ 71 \cdot [32 \cdot (-19)] + 45 \cdot (32 \cdot 30) &= 32 \\ 71 \cdot (-608) + 45 \cdot 960 &= 32 \end{aligned}$$

(Notice how I multiplied the 32 into the numbers -19 and 30, **not** the coefficients 71 and 45 of the original equation.)

If you compare the last equation to $71x + 45 = 32$, you can see that $x_0 = -608$ and $y_0 = 960$ comprise a particular solution. Therefore, the general solution is

$$x = 45k - 608, \quad y = -71k + 960. \quad \square$$

I won't give a proof of the result for more than 2 variables, but I'll illustrate how to reduce the 3-variable case to the 2-variable case by example.

Example. Solve the Diophantine equation

$$3x + 3y + 5z = 10.$$

First, I'll factor $(3, 3)$ out of the first two coefficients:

$$(3, 3)\left(\frac{3}{(3, 3)}x + \frac{3}{(3, 3)}y\right) + 5z = 10.$$

Notice that $(3, 3) = 3$, so those two fractions are actually integers. I'm not simplifying $\dfrac{3}{(3, 3)}$ so that you can see what's going on.

Let

$$w = \frac{3}{(3, 3)}x + \frac{3}{(3, 3)}y.$$

The equation becomes

$$(3, 3)w + 5z = 10, \quad \text{or} \quad 3w + 5z = 10.$$

$(3, 5) = 1 \mid 10$, so this two variable equation is solvable. $\hat{x} = 5$, $\hat{y} = -1$, is a particular solution, so the general solution is

$$w = 5s + 5, \quad z = -3s - 1.$$

Now I have to find x and y:

$$w = \frac{3}{(3, 3)}x + \frac{3}{(3, 3)}y, \quad \text{so} \quad w = x + y.$$

Thus,

$$x + y = 5s + 5.$$

This is a two variable equation. Since $(1, 1) = 1 \mid 5s + 5$, it's solvable. $x = 5$, $y = 5s$, is a particular solution. Therefore, the general solution is

$$x = t + 5, \quad y = 5s - t.$$

All together, the general solution to the original three variable equation is

$$x = t + 5, \quad y = 5s - t, \quad z = -3s - 1. \quad \square$$

In general, if there is a solution to the linear Diophantine equation

$$a_1x_1 + \cdots a_nx_n = c,$$

the solution will depend on $n - 1$ parameters — exactly as you'd expect from linear algebra.

---

[1] Leonard Eugene Dickson, *History of the Theory of Numbers* (volumes I, II, and III). Bronx, NY: Chelsea Publishing, 1992.

[2] L. J. Mordell, *Diophantine Equations*. New York: Academic Press, 1969.