24

The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states the familiar fact that every positive integer greater than 1 can be written in exactly one way as a product of primes. For example, the prime factorization of 60 is $2^2 \cdot 3 \cdot 5$, and the prime factorization of 625 is 5^4. The factorization of 60 can be written is several different ways: $60 = 2 \cdot 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 \cdot 2$, and so on. The order in which the factors are written does not matter. The factorization of 60 into primes will always have two 2's, one 3, and one 5. One more example: The factorization if 17 consists of the single factor 17. In the *standard form* of the factorization of an integer greater than 1, the primes are written in order of size, and exponents are used for primes that are repeated in the factorization. So, for example, the standard factorization of 60 is $60 = 2^2 \cdot 3 \cdot 5$.

24.1 Prime divisors

Before proving the Fundamental Theorem of Arithmetic, we will need to assemble a few facts.

Theorem 24.1. *If $n|ab$ and n and a are relatively prime, then $n|b$.*

Proof. *Suppose $n|ab$ and that $gcd(n,a) = 1$. We can find integers s, t such that $ns + at = 1$. Multiply both sides of that equation by b to get $nsb + abt = b$. Since n divides both terms on the left side of that equation, it divides their sum, which is b.* ♣

One consequence of this theorem is that if a prime divides a product of some integers, then it must divide one of the factors. That is so since if a prime does not divide an integer, then it is relatively prime to that integer. That is useful enough to state as a theorem.

Theorem 24.2. *If p is a prime, and $p|a_1a_2\cdots a_n$, then $p|a_j$ for some $j = 1, 2, \cdots, n$.*

24.2 Proving the Fundamental Theorem

Theorem 24.3 (Fundamental Theorem of Arithmetic)**.** *If $n > 1$ is an integer, then there exist prime numbers $p_1 \leq p_2 \leq \ldots \leq p_r$ such that $n = p_1p_2\cdots p_r$ and there is only one such prime factorization of n.*

Proof. *There are two things to prove: (1) every $n > 1$ can be written in at least one way as a product of primes (in increasing order) and (2) there cannot be two different such expressions equal to n.*

We will prove these by induction. For the basis, we see that 2 can be written as a product of primes (namely $2 = 2$) and, since 2 is the smallest prime, this is the only way to write 2 as a product of primes.

For the inductive step, suppose every integer from 2 to k can be written uniquely as a product of primes. Now consider the number $k+1$. We consider two cases:

(1) *If $k+1$ is a prime then $k+1$ is already an expression for $k+1$ as a product of primes. There cannot be another expression for $k+1$ as a product of primes, for if $k+1 = pm$ with p a prime, then $p|k+1$ and p and $k+1$ both primes tells us $p = k+1$, and so $m = 1$.*

(2) *If $k+1$ is not a prime, then we can write $k+1 = ab$ with $2 \leq a, b \leq k$. By the inductive hypothesis, each of a and b can be written as products of primes, say $a = p_1p_2\cdots p_s$ and $b = q_1q_2\cdots q_t$. That means $k+1 = p_1p_2\cdots p_sq_1q_2\cdots q_t$, and we can rearrange the primes in increasing order. To complete the proof, we need to show $k+1$ cannot be written in more than one way as a product of an increasing list of primes. So suppose $k+1$ has two different such expressions: $k+1 = u_1u_2\cdots u_l = v_1v_2\cdots v_m$. Since $u_1|v_1v_2\cdots v_m$, u_1 must divide some one of the v_i's and since u_1 and that v_i are both primes,*

they must be equal. As the v's are listed in increasing order, we can conclude $u_1 \geq v_1$. The same reasoning shows $v_1 \geq u_1$. Thus $u_1 = v_1$. Now cancel u_1, v_1 from each side of $u_1 u_2 \cdots u_l = v_1 v_2 \cdots v_m$ to get $u_2 \cdots u_l = v_2 \cdots v_m$. Since $k+1$ was not a prime, both sides of this equation are greater than 1. Both sides are also less than $k+1$. Since we started with two different factorizations, and canceled the same thing from both sides, we now have two different factorizations of a number between 2 and k. That contradicts the inductive assumption. We conclude the the prime factorization of $k+1$ is unique.

Thus, our induction proof is complete. ♣

24.3 Number of positive divisors of n

We can apply the Fundamental Theorem of Arithmetic to the problem of counting the number of positive divisors of an integer greater than 1. For example, consider the integer $12 = 2^2 3$. It follows from the Fundamental Theorem that the positive divisors of 12 must look like $2^a 3^b$ where $a = 0, 1, 2$, $b = 0, 1$. So there are six positive divisors of 12:

$$2^0 3^0 = 1 \quad 2^1 3^0 = 2 \quad 2^2 3^0 = 4 \quad 2^0 3^1 = 3 \quad 2^1 3^1 = 6 \quad 2^2 3^1 = 12$$

24.4 Exercises

Exercise 24.1. *Determine the prime factorization of* 345678*.*

Exercise 24.2. *Determine the prime factorization of* 1016*.*

Exercise 24.3. *List all the positive divisors of* 1016*.*

Exercise 24.4. *How many positive divisors does* 345678 *have?*

24.5 Problems

Problem 24.1. *Determine the prime factorization of* 13579*.*

Problem 24.2. *List all the positive divisors of* 13579*.*

Problem 24.3. *Prove that if n is an even integer bigger than* 2*, then* $2^n - 1$ *is not a prime. Examples:* $2^4 - 1 = 15 = (3)(5)$*,* $2^{10} - 1 = 1023 = (3)(11)(31)$*, and Hint: Recall the factorization from college algebra* $s^2 - t^2 = (s+t)(s-t)$*.*

Problem 24.4. *Prime factorizations can be used to find greatest common divisors. The method is very inefficient compared to the Euclidean Algorithm since there is no known fast method of finding prime factorizations. Suppose a and b are two positive integers. Factor them each as product of primes. Say*

$$a = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n} \quad \text{and} \quad b = p_1^{f_1} p_2^{f_2} p_3^{f_3} \cdots p_n^{f_n}.$$

Note that the same list of primes is used for both factorizations, so we will need to allow exponents to be 0 *or more. For example, for* $a = 12$ *and* $b = 15$ *we will write* $a = 12 = 2^2 \cdot 3^1 \cdot 5^0$ *and* $15 = 2^0 \cdot 3^1 \cdot 5^1$*.*

Prove: $\gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} p_3^{\min(e_3,f_3)} \cdots p_n^{\min(e_n,f_n)}$.

Example: $\gcd(12,15) = 2^{\min(2,0)} 3^{\min(1,1)} 5^{\min(0,1)} = 2^0 3^1 5^0 = 3$.

Problem 24.5. *Prime factorizations can be used to find least common multiples The method, which is likely the one you were taught in grade school for adding fractions, is, once again, very inefficient. Say*

$$a = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n} \quad \text{and} \quad b = p_1^{f_1} p_2^{f_2} p_3^{f_3} \cdots p_n^{f_n}.$$

Prove: $\operatorname{lcm}(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} p_3^{\max(e_3,f_3)} \cdots p_n^{\max(e_n,f_n)}$.

Example: $\gcd(12,15) = 2^{\max(2,0)}3^{\max(1,1)}5^{\max(0,1)} = 2^2 3^1 5^1 = 60.$

Problem 24.6. *Using the formulas for* gcd *and* lcm *in the previous two problems, prove the result you guessed in the last chapter for the product of* $\gcd(a,b)\,\mathrm{lcm}(a,b)$. *(Hint: The fact you need is* $\min(s,t) + \max(s,t) = s+t$*, which is not hard to prove.)*

25

Linear Diophantine Equations

Consider the following problem:

Al buys some books at \$25 each, and some magazines at \$3 each. If he spent a total of \$88, how many books and how many magazines did Al buy? At first glance, it does not seem we are given enough information to solve this problem. Letting x be the number of books Al bought, and y the number of magazines, then the equation we need to solve is $25x + 3y = 88$. Thinking back to college algebra days, we recognize $25x + 3y = 88$ as the equation of a straight line in the plane, and any point along the line will give a solution to the equation. For example, $x = 0$ and $y = \frac{88}{3}$ is one solution. But, in the context of this problem, that solution makes no sense because Al cannot buy a fraction of a magazine. We need a solution in which x and y are both integers. In fact, we need even a little more care than that. The solution $x = -2$ and $y = 46$ is also unacceptable since Al cannot buy a negative number of books. So we really need solutions in which x and y are both nonnegative integers. The problem can be solved by brute force: If $x = 0$, y is not an integer. If $x = 1$, then $y = 21$, so that is one possibility. If $x = 2$, y is not an integer. If $x = 3$, y is not an integer. And, if x is 4 or more, then y would have to be negative. So, it turns out there is only one possible solution: Al bought one book, and 21 magazines.

25.1 Diophantine equations

The above question is an example of a Diophantine problem. Pronounce Diophantine as *dee-uh-FAWN-teen* or *dee-uh-FAWN-tine*, or, the more common variations, *die-eh-FAN-teen* or *die-eh-FAN-tine*. http://www.merriam-webster.com/audio.php?file=diopha01&word=Diophantineequation) . In general, problems in which we are interested in finding solutions in which the variables are to be integers are called **Diophantine** problems.

For a modern pronunciation of Diophantus's name ($\Delta\iota o\phi\alpha\nu\tau o\zeta$) see http://www.pronouncenames.com/Diophantus

In this chapter we will learn how to easily find the solutions to all linear Diophantine equations: $ax + by = c$ where a, b, c are given integers. To show some of the subtleties of such problems, here are two more examples:

(1) Al buys some books at \$24 each, and some magazines at \$3 each. If he spent a total of \$875, how many books and how many magazines did Al buy? For this question we need to solve the Diophantine equation $24x + 3y = 875$. In this case there are no possible solutions. For any integers x and y, the left-hand side will be a multiple of 3 and so cannot be equal to 875 which is not a multiple of 3.

(2) Al buys some books at \$26 each, and some magazines at \$3 each. If he spent a total of \$157, how many books and how many magazines did Al buy? Setting up the equation as before, we need to solve the Diophantine equation $26x + 3y = 157$. A little trial and error, testing $x = 0, 1, 2, 3$, and so on shows there are two possible answers this time: $(x, y) \in \{(2, 35), (5, 9)\}$.

25.2 Solutions and $\gcd(a, b)$

Determining all the solutions to $ax + by = c$ is closely connected with the idea of gcd's. One connection is theorem 23.1. Here is how solutions of $ax + by = c$ are related.

Theorem 25.1. *$ax + by = c$ has a solution in the integers if and only if $\gcd(a, b)$ divides c.*

So, for example, $9x + 6y = 211$ has no solutions (in the integers) while $9x + 6y = 213$ does have solutions. To find a solution to the last equation, apply the Extended Euclidean Algorithm method to write the $\gcd(9, 6)$ as a linear combination of 9 and 6 (actually, this one is easy to do by sight): $9 \cdot 1 + 6 \cdot (-1) = 3$, then multiply both sides by $213/\gcd(9, 6) = 213/3 = 71$ to get $(71)9 + (-71)6 = 213$. That shows $x = 71$, $y = -71$ is a solution to $9x + 6y = 213$.

But that is only one possible solution. When a linear Diophantine equation has one solution it will have infinitely many. In the example above, another solution will be $x = 49$ and $y = -38$. Checking shows that $(49)9 + (-38)6 = 213$.

25.3 Finding all solutions

There is a simple recipe for all solutions, once one particular solution has been found.

Theorem 25.2. *Let $d = \gcd(a, b)$. Suppose $x = s$ and $y = t$ is one solution to $ax + by = c$. Then all solutions are given by*

$$x = s + k\frac{b}{d} \quad \textit{and} \quad y = t - k\frac{a}{d} \quad \textit{where, } k = \textit{ any integer.}$$

Proof. *It is easy to check that all the displayed x, y pairs are solutions simply by plugging in:*

$$a\left(s + k\frac{b}{d}\right) + b\left(t - k\frac{a}{d}\right) = as + \frac{abk}{d} + bt - \frac{abk}{d} = as + bt = c.$$

Checking that the displayed formulas for x and y give all possible solutions is trickier. Let's assume $a \neq 0$. Now suppose $x = u$ and $y = v$ is a solution. That means $au + bv = c = as + bt$. It follows that $a(u - s) = b(t - v)$. Divide both sides of that equation by d to get

$$\frac{a}{d}(u - s) = \frac{b}{d}(t - v).$$

That equation shows $\frac{a}{d} \,\Big|\, \frac{b}{d}(t - v)$. Since $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime, we conclude that $\frac{a}{d} \,\Big|\, (t - v)$. Let's say $k\frac{a}{d} = t - v$. Rearrange that equation to *get*

$$v = t - k\frac{a}{d}.$$

Next, replacing $t - v$ *in the equation* $\frac{a}{d}(u - s) = \frac{b}{d}(t - v)$ *with* $k\frac{a}{d}$ *gives*

$$\frac{a}{d}(u - s) = \frac{b}{d}(t - v) = \frac{b}{d}\left(k\frac{a}{d}\right).$$

Since $\frac{a}{d} \neq 0$*, we can cancel that factor. So, we have*

$$u - s = k\frac{b}{d} \quad \text{so that} \quad u = s + k\frac{b}{d}.$$

That proves the solution $x = u$*,* $y = v$ *is given by the displayed formulas.*

♣

25.4 Examples

Example 25.3. *Determine all the solutions to* $221x + 91y = 39$*.*

Using the Extended Euclidean Algorithm method, we learn that $\gcd(221, 91) = 13$ *and since* $13|39$*, the equation will have infinitely many solutions. The Extended Euclidean Algorithm table provides a linear combination of* 221 *and* 91 *equal to* 13*:* $221(-2) + 91(5) = 13$*. Multiply both sides by* 3 *and we get* $221(-6) + 91(15) = 39$*. So one particular solution to* $221x + 91y = 39$ *is* $x = -6$*,* $y = 15$*. According the the theorem above, all solutions are given by*

$$x = -6 + k\frac{91}{13} = -6 + 7k \quad \text{and} \quad y = 15 - k\frac{221}{13} = 15 - 17k,$$

where k is any integer.

Example 25.4. *Armand buys some books for \$25 each and some cd's for \$12 each. If he spent a total of \$331, how many books and how many cd's did he buy?*

Let x *= the number of books, and* y *= the number of cd's. We need to solve* $25x + 12y = 331$*. The* $\gcd$ *of* 25 *and* 12 *is* 1*, and there is an obvious linear combination of* 25 *and* 12 *which equals* 1*:* $25(1) + 12(-2) = 1$*. Multiplying both sides by* 331 *gives* $25(331) + 12(-662) = 331$*. So one particular solution to* $25x + 12y = 331$ *is* $x = 331$ *and* $y = -662$*. Of course, that won't do for an answer to the given problem since we want*

$x, y \geq 0$. To find the suitable choices for x and y, let's look at all the possible solutions to $25x + 12y = 331$. We have that

$$x = 331 + 12k \quad \textit{and} \quad y = -662 - 25k.$$

We want x and y to be at least 0, and so we need

$$331 + 12k \geq 0 \quad \textit{and} \quad -662 - 25k \geq 0.$$

Which means that

$$k \geq -\frac{331}{12} \quad \textit{and} \quad k \leq -\frac{662}{25},$$

or

$$-\frac{331}{12} \leq k \leq -\frac{662}{25}.$$

The only option for k is $k = -27$, and so we see Armand bought $x = 331 + 12(-27) = 7$ books and $y = -662 - 25(-27) = 13$ cd's.

25.5 Exercises

Exercise 25.1. *Find all integer solutions to* $21x + 48y = 8$.

Exercise 25.2. *Find all integer solutions to* $21x + 48y = 9$.

Exercise 25.3. *Find all integer solutions to* $33x + 12y = 7$.

Exercise 25.4. *Find all integer solutions to* $33x + 12y = 6$.

Exercise 25.5. *Sal sold some ceramic vases for \$59 each, and a number of ash trays for \$37 each. If he took in a total of \$4270, how many of each item did he sell?*

25.6 Problems

Problem 25.1. *Find all integer solutions to* $14x + 77y = 69$.

Problem 25.2. *Find all integer solutions to* $14x + 77y = 70$.

Problem 25.3. *Beth stocked her video store with a number of video game machines at \$79 each, and a number of video games at \$41 each. If she spent a total of \$6358, how many of each item did she purchase?*

Problem 25.4. *If you all you have are dimes and quarters, in how many ways can you pay a \$7 bill?*

(For example, one way would be 10 *dimes and* 24 *quarters.)*

Problem 25.5. *How many integer solutions are there to the equation* $11x + 7y = 137$ *if the value of* x *has to be at least* -15 *and not more than* 20.

Problem 25.6. *Determine all integer solutions to* $5x - 7y = 99$. *(Watch that minus sign!)*