CHAPTER II

# Greatest Common Divisors

## 1. Introducing greatest common divisors

We call the integer $a$ a **common divisor** of $b$ and $c$, naturally enough, if it is a divisor that $b$ and $c$ have in common—that is, if $a \mid b$ and $a \mid c$. Among all these common divisors, the largest one plays an important role in number theory, and so we give it a name. The largest number among all of the common divisors of $b$ and $c$ is called the **greatest common divisor** or **gcd** of $b$ and $c$, and we denote it by $\gcd(b, c)$

EXAMPLE. The divisors of 140 are 1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 70, and 140 (along with their negatives); the (positive) divisors of 168 are 1, 2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 28, 42, 56, 84, and 168. The common divisors of 140 and 168 are the integers that appear in both of these lists, namely $\pm 1$, $\pm 2$, $\pm 4$, $\pm 7$, $\pm 14$, and $\pm 28$. Therefore, their greatest common divisor $\gcd(140, 168)$ equals 28.

EXAMPLE. The divisors of $-15$ are $\pm 1$, $\pm 3$, $\pm 5$, and $\pm 15$. The divisors of 0 are—well, all the integers! (see Problem 1.2) Therefore, *all* of the divisors of $-15$ are common divisors of $-15$ and 0, and so $\gcd(-15, 0) = 15$.

Before you try it and get into trouble, we'll tell you that $\gcd(0, 0)$ is undefined—this is the only case where two integers can have infinitely many common divisors. If $b$ is a nonzero integer, then $b$ only has finitely many divisors (in fact, none of them are bigger than $|b|$, by Fact 1.8), and the same for $c$; so we see that if even one of $b$ and $c$ is nonzero, then it makes sense to talk about $\gcd(b, c)$. Certainly 1 is always a common divisor of $b$ and $c$ (as we showed in Problem 1.2), so at least we know that $\gcd(b, c) \geq 1$.

Many textbooks use the briefer notation $(b, c)$ for the greatest common divisor of $b$ and $c$. This saves space, although the possibility for confusion can arise, since points in the plane $(x, y)$ are denoted with the same notation, for example. So we'll stick to the notation $\gcd(b, c)$ in these notes.

We'll start this section right off with a theorem about greatest common divisors that we will use a lot in the future. Theorem 2.1 is probably the first fact about numbers you've come across in these notes that isn't simply *intuitively true* ... we're seeing the beginning of the good side of proof-based mathematics, the side that tells us things about numbers that we didn't already know.

**Theorem 2.1.** *Let $b$ and $c$ be integers, not both zero, and set $d = \gcd(b, c)$. Then we can find integers $u_0$ and $v_0$ such that $d = bu_0 + cv_0$.*

*Proof:* Consider the collection of all positive integers $a$ that can be written in the form $bu+cv$, for some integers $u$ and $v$. This collection has at least one element: taking $u=b$ and $v=c$, we see that $b^2+c^2$ is a positive integer that can be written that way. Therefore, by Fact 1.1, this collection has a smallest element $s$. Pick two integers $u_0$ and $v_0$ such that $s=bu_0+cv_0$.

Let's try to show that $s$ divides $b$. Using the Division Algorithm, we can write $b=qs+r$ with $0 \le r < s$. We're trying to show that $s \mid b$, and so by Fact 1.10 all we need to show is that $r=0$. Well, suppose not—suppose that $0<r<s$. We can write

$$r = b - qs = b - q(bu_0+cv_0) = b(1-qu_0) + c(-qv_0).$$

But this can't be, because then $r$ would be a positive number *smaller than* $s$ that can be written in the form $bu+cv$! Since it's impossible that $0<r<s$, we conclude that really $r=0$, and so $s$ divides $b$.

The exact same argument shows that $s$ divides $c$ as well, and so $s$ is a common divisor of $b$ and $c$. Since $d$ is the greatest common divisor of $b$ and $c$, it's definitely true that $s \le d$.

On the other hand, we can show that $d$ divides $s$! This is because $d \mid b$ and $d \mid c$, and so $d$ divides every integer of the form $bu+cv$ (Fact 1.7)—including $s$. Well, if $d$ divides $s$ then $d \le |s| = s$ (Fact 1.8); and since $s \le d$ and $d \le s$, we conclude that $d=s$. In particular, $d=bu_0+cv_0$, which is what we wanted to show. □

We know that every common divisor of $b$ and $c$ is no bigger than $\gcd(b,c)$ ... but in fact even more is true:

FACT 2.2. *Every common divisor of $b$ and $c$ divides* $\gcd(b,c)$.

For instance, in the example on page 5, all of the common divisors $\pm 1$, $\pm 2$, $\pm 4$, $\pm 7$, $\pm 14$, and $\pm 28$ of 140 and 168 are not only less than or equal to $\gcd(140,168)=28$, but they all divide 28. And we can prove that this always happens.

*Proof:* If we let $d=\gcd(b,c)$, then from Theorem 2.1, there are integers $u_0$ and $v_0$ such that $d=bu_0+cv_0$. Now let $a$ be any common divisor of $b$ and $c$. Since $a \mid b$, we can write $b=as$ for some integer $s$; and since $a \mid c$, we can similarly write $c=at$ for some integer $t$. Hence

$$d = (as)u_0 + (at)v_0 = a(su_0+tv_0),$$

which shows that $a$ is a divisor of $d$. □

By now, we have seen three different ways of describing the same number $\gcd(b,c)$:

- $\gcd(b,c)$ equals the largest of all the common divisors of $b$ and $c$ (this was the definition);
- $\gcd(b,c)$ equals the smallest number that can be written in the form $bu+cv$ for integers $u$ and $v$ (this was Theorem 2.1);
- $\gcd(b,c)$ equals the positive common divisor of $b$ and $c$, such that *every* common divisor of $b$ and $c$ divides it (this was Fact 2.2).

(Actually, to be technically correct there is one detail about the last statement that we haven't proved yet. Can you see what it is?)

EXAMPLE. From the equation $15 \times (-5) + 38 \times 2 = 1$, we see that 1 can be written in the form $15u + 38v$. Since 1 is the smallest number of all, 1 is certainly the smallest number that can be written in that form, and so we know that $\gcd(15, 38) = 1$. We can verify this by writing down all of the positive divisors of 15 (they are 1, 3, 5, and 15) and 38 (they are 1, 2, 19, and 38), and seeing that 1 is the only one in common.

We've remarked that 1 and $-1$ are always common divisors of any two integers $a$ and $b$. As it turns out, the situation where these are the *only* common divisors of $b$ and $c$ has great importance in the study of number theory—definitely important enough to warrant a name of its own: if $a$ and $b$ are two integers such that $\gcd(a, b) = 1$, then we say that $a$ and $b$ are **relatively prime**, or **coprime**. For instance, the previous example shows that 15 and 38 are relatively prime. We can also say that 15 is relatively prime to 38 (and vice versa).

If we just restate what we've already said in this section using this new terminology, we obtain a consequence of Theorem 2.1 that will be very useful to us:

CONSEQUENCE 2.3. *Two integers $a$ and $b$ are relatively prime if, and only if, there are integers $u$ and $v$ such that $au + bv = 1$.*

Here's an example of how we can use this Consequence to prove something interesting: if $n$ has no divisors (other than $\pm 1$) in common with $a$ nor with $b$, then in fact $n$ has no divisors (other than $\pm 1$) in common with the product $ab$. To say this another way:

FACT 2.4. *The product of two integers coprime to a third integer is again coprime to the third integer: If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.*

*Proof:* Because of Consequence 2.3, there are integers $x_0$ and $y_0$ such that $ax_0 + ny_0 = 1$, and there are integers $x_1$ and $y_1$ such that $bx_1 + ny_1 = 1$. This means

$$1 = 1 \times 1 = (ax_0 + ny_0)(bx_1 + ny_1) = (ab)(x_0x_1) + n(bx_1y_0 + ax_0y_1 + ny_0y_1).$$

(How often do you get any mileage out of the fact that $1 \times 1 = 1$?) Letting $u = x_0x_1$ and $v = bx_1y_0 + ax_0y_1 + ny_0y_1$, we see that 1 can be written in the form $(ab)u + nv$. Therefore, using Consequence 2.3 again, $\gcd(ab, n) = 1$. $\square$

FACT 2.5. *If $a$ is relatively prime to $b$, and $a \mid bc$, then actually $a \mid c$.*

*Proof:* Because of Consequence 2.3, there are integers $u$ and $v$ such that $au+bv = 1$. Multiplying this equation by $c$, we get $c = c(au + bv) = a(cu) + (bc)v$. Now $a$ certainly divides $a$, and we're also assuming that $a$ divides $bc$. This means, using Consequence 1.7, that $a$ divides any number of the form $am + (bc)n$. In particular, $a$ divides $a(cu) + (bc)v$, and since this last expression equals $c$ we are done with the proof. $\square$

Perhaps you're getting a sense of this already, but the facts about greatest common divisors in this section are sort of a set of tools for doing "algebra" within the theory of divisibility. By having a list of little facts like these, we will be able to manipulate formulas involving gcds more mechanically, just as we use algebraic manipulations to simplify equations. Here are a few more facts in this vein.

FACT 2.6. *If $n$ is any integer, then $\gcd(na, nb) = n \gcd(a, b)$.*

The proof is left as an exercise for you. ◇

FACT 2.7. *If $c$ is any common divisor of $a$ and $b$, then* $\gcd(\frac{a}{c}, \frac{b}{c}) = \frac{1}{|c|}\gcd(a, b)$.

The proof is left as an exercise for you. ◇

CONSEQUENCE 2.8. *If $d = \gcd(a, b)$, then the integers $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.*

*Proof:* Just by applying Fact 2.7 with $c = d$, we see that $\gcd(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}\gcd(a, b) = 1$. □

This last consequence states something very intuitive: if you go to the trouble of dividing two numbers through by their highest common factor, then the resulting numbers aren't going to have any more factors in common. We take this for granted all the time—for instance, when we're reducing fractions to lowest terms. Using the tools we have now, we can actually prove that every fraction can be reduced to lowest terms in this way, and in fact there is only one fraction in lowest terms (up to the signs of the numerator and denominator) that equals any given fraction:

CONSEQUENCE 2.9. *Every rational number has a unique representation in the form $\frac{a}{b}$, where $b$ is positive and $a$ and $b$ have no common factors (other than $\pm 1$).*

The proof is left as an exercise for you. ◇

## 2. Solving the linear equation $ax + by = c$

Let $a$, $b$, and $c$ be given integers. We wish to find all pairs of integers $x$ and $y$ for which the linear equation $ax + by = c$ is satisfied. Let's forget about the case where $a = b = 0$, because then it doesn't matter what $x$ and $y$ are, the left-hand side will equal zero; in this case every pair $(x, y)$ is a solution if $c = 0$, or else no pair $(x, y)$ is a solution if $c \neq 0$.

So let's look at the interesting case, where $a$ and $b$ are not both zero. This means we can take their greatest common divisor, so we define $d = \gcd(a, b)$. We notice right away that if $d$ does not divide $c$, then the equation has no solution: since $d \mid a$ and $d \mid b$, we know that $d$ divides $ax + by$ no matter what $x$ and $y$ are (Fact 1.7), and therefore it is impossible for $ax + by$ to equal $c$ if $c$ is not even a multiple of $d$.

EXAMPLE. There are no solutions in integers to the equation $15x + 24y = 112$, because no matter what integers $x$ and $y$ we choose, the left-hand side will be a multiple of 3, while 112 is not a multiple of 3. In other words, the problem is that $\gcd(15, 24) = 3$ does not divide 112.

On the other hand, what if $d \mid c$? If we define $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, and $c' = \frac{c}{d}$, then we can divide the entire equation $ax + by = c$ through by $d$ to get the equation $a'x + b'y = c'$, which has exactly the same solutions as the original equation. The reason this is helpful is because we have made the coefficients of the variables relatively prime: by Consequence 2.8, the integers $a'$ and $b'$ satisfy $\gcd(a', b') = 1$.

EXAMPLE. By dividing through by $\gcd(60, 152) = 4$, we see that the solutions to the equation $60x + 152y = -28$ are exactly the same as the solutions to the equation $15x + 38y = -7$.

Now remember that when two numbers $a'$ and $b'$ are relatively prime, then we can find numbers $u$ and $v$ such that $a'u + b'v = 1$ (Consequence 2.3). All we have to do now is multiply the equation through by $c'$ to obtain $a'(uc') + b'(vc') = c'$. And there we go! We have found a solution $(x_0, y_0)$ to the equation $a'x+b'y = c'$ (and thus to the original equation $ax + by = c'$ as well), namely $x_0 = uc'$ and $y_0 = vc'$.

EXAMPLE. We saw in an example on page 7 that $15 \times (-5) + 38 \times 2 = 1$. Multiplying through by $-7$, we see that $15 \times 35 + 38 \times (-14) = -7$. Thus $x = 35$, $y = -14$ is a solution in integers to the equation $15x + 38y = -7$, and thus (by the previous example) to the equation $60x + 152y = -28$ as well.

There are two things left to say about solving linear equations. First, we've seen that finding a solution to a linear equation, in the case where $a'$ and $b'$ are relatively prime, depends on finding two integers $x$ and $y$ such that $a'x+b'y = 1$. We know from Consequence 2.3 that such integers $x$ and $y$ *exist*, but how do we actually find them? This question will be answered in the next section, with the Euclidean Algorithm. Second, just because we've found one solution doesn't mean it's the only solution:

EXAMPLE. The pairs of integers

$$\begin{aligned} x &= -3, \quad & y &= 1 \\ x &= 73, \quad & y &= -19 \\ x &= -117, \quad & y &= 46 \\ x &= 15{,}235, \quad & y &= -6{,}014 \end{aligned}$$

are all solutions to the equation $60x + 152y = -28$, in addition to the solution found in the previous example.

Let's see how to start with the one solution $(x_0, y_0)$ that we know and find all the others.

First of all, we can point out a property that any other solution $(x_1, y_1)$ must have. If $(x_1, y_1)$ is to be a solution, that means $a'x_1 + b'y_1 = c'$; and subtracting our known equation $a'x_0 + b'y_0 = c'$ from this, we obtain $a'(x_1 - x_0) + b'(y_1 - y_0) = 0$, or

$$a'(x_1 - x_0) = b'(y_0 - y_1).$$

Now notice that $b'$ certainly divides the right-hand side, and so it must divide the left-hand side as well, so $b' \mid a'(x_1 - x_0)$. Remember, though, that $a'$ and $b'$ are relatively prime. This means that we can apply Fact 2.5 to deduce that $b' \mid (x_1 - x_0)$.

Therefore, there is some number $k$ satisfying $(x_1 - x_0) = b'k$, or equivalently $x_1 = x_0 + b'k$. In other words, if $(x_1, y_1)$ is going to be another solution to $a'x + b'y = c'$, then $x_1$ has to be a number you can obtain from $x_0$ by adding a multiple of $b'$.

On the other hand, any such number $x_1 = x_0 + b'k$ actually works! This is because we can simply solve for $y_1$:

$$\begin{aligned} a'x_1 + b'y_1 &= c' \\ a'(x_0 + b'k) + b'y_1 &= a'x_0 + b'y_0 \\ b'y_1 &= b'y_0 - a'b'k \\ y_1 &= y_0 - a'k. \end{aligned}$$

So for any number $x_1$ that differs from $x_0$ be a multiple of $b'$, there is a corresponding number $y_1$ that differs from $y_0$ by a multiple of $a'$ (makes sense) such that $(x_1, y_1)$ is another solution to the equation.

EXAMPLE. Every pair of integers of the form

$$x = 35 + 38k, \quad y = -14 - 15k$$

is a solution to the equation $15x + 38y = -7$ (or, equivalently, to the equation $60x + 152y = -28$), and these are all of the solutions in integers to this equation. (Notice that the original solution, found in an example on page 9, corresponds to $k = 0$, and the particular solutions listed in the previous example can be obtained from this formula by setting $k = -1$, $k = 1$, $k = -4$, and $k = 400$, respectively.)

We summarize all that we've discovered about solving the linear equation $ax + by = c$ in integers in the following theorem:

**Theorem 2.10.** *Let $a$, $b$, and $c$ be integers, with $a$ and $b$ not both equal to 0.*

a. *If $\gcd(a, b)$ does not divide $c$, then the equation $ax + by = c$ has no solutions in integers $x$, $y$.*
b. *If $\gcd(a, b) \mid c$, then the equation $ax + by = c$ has exactly the same solutions as the equation $a'x + b'y = c'$, where $a' = a/\gcd(a, b)$, $b' = b/\gcd(a, b)$, and $c' = c/\gcd(a, b)$. Furthermore, $a'$ and $b'$ are relatively prime, so to solve the new equation we just go on to the next case:*
c. *If $\gcd(a, b) = 1$, then $ax + by = c$ is satisfied for infinitely many pairs of integers $(x, y)$. Furthermore, if $(x_0, y_0)$ is a particular integer solution of $ax + by = c$, then every pair of integers of the form $(x_0 + bk, y_0 - ak)$ (where $k$ is an integer) is also a solution of $ax + by = 1$, and these are all the solutions in integers.*

## 3. The Euclidean Algorithm

The whole procedure of the previous section revolves around finding integers $x$ and $y$ such that $ax + by = 1$, where $a$ and $b$ are two given coprime integers. Even more generally, Theorem 2.1 tells us that integers $x$ and $y$ exist satisfying the equation $ax + by = \gcd(a, b)$, but it doesn't really tell us how to find them. For that matter, we haven't even seen a systematic way to simply *calculate* the greatest common divisor of two numbers! We certainly don't want to have to list all of the divisors of both numbers, and compare the lists by hand, every time we want to find a gcd.

As it turns out, there is a single algorithm that will do all of these things for us, called the **Euclidean Algorithm**. This process was known to Euclid, who phrased it in terms of starting with two line segments and finding a common "ruler segment" so that each of the original segments could be measured exactly with a whole number of these ruler segments. First we'll describe how the algorithm finds greatest common divisors, and then we'll show how to fancy it up to find a solution to the equation $ax + by = \gcd(a, b)$.

As you're used to from these notes by now, we can't just launch straight into the good stuff—we need to write down a few more simple "algebraic" properties of gcds.

FACT 2.11. *We hvae* $\gcd(n, \pm 1) = 1$ *for any integer* $n$*, and* $\gcd(n, 0) = |n|$ *for any nonzero integer* $n$*.*

The proof is left as an exercise for you. ◇

FACT 2.12. *For any integers* $a$ *and* $b$*, we have the equalities* $\gcd(a, b) = \gcd(b, a)$ *and* $\gcd(a, b) = \gcd(\pm a, \pm b)$*.*

The proof is left as an exercise for you. ◇

FACT 2.13. *The greatest common divisor of two integers does not change if we add a multiple of one of them to the other: For any integers* $a$*,* $b$*, and* $n$*, we have the equality* $\gcd(a, b) = \gcd(a, b + na)$*.*

*Proof:* This one we'll actually prove, since it's the least intuitive fact of the three in this section, as well as the most important. We'll prove it by showing that all common divisors of $a$ and $b$ are also common divisors of $a$ and $b + na$, and vice versa; hence the greatest common divisor must be the same in each case.

So let $c$ be a common divisor of $a$ and $b$. Then by Fact 1.7, $c$ divides any expression of the form $b + na$. Therefore any common divisor of $a$ and $b$ is also a common divisor of $a$ and $b + na$. But this argument goes the other direction too, since any common divisor of $a$ and $b + na$ also divides any expression of the form

$$(b + na) + (-n)a = b,$$

(again by Fact 1.7) and so is a common divisor of $a$ and $b$ as well. □

Now, given two positive integers $a$ and $b$, how can we calculate their greatest common divisor $d = \gcd(a, b)$? First of all, Fact 2.12 tells us that we can switch the sign(s) of $a$ and/or $b$ without affecting their gcd, so we can assume that both $a$ and $b$ are positive. Fact 2.12 also tells us that we can switch $a$ and $b$ without affecting their gcd, so we can assume that $a \geq b$ (if not, we just interchange the two numbers and rename them).

The Euclidean Algorithm goes like this: at each step we have a pair of numbers $(a, b)$. We get a new pair of numbers as follows:

*a.* We use the Division Algorithm to write $a = qb + r$ with $0 \leq r < b$;
*b.* We replace the old pair of numbers $(a, b)$ with the new pair $(b, r)$;
*c.* We keep doing those two steps over and over, until the second number of newest pair equals 0.

We claim that when this happens, the first number of the newest pair is the greatest common divisor of the original pair $(a, b)$!

Sounds a little like magic ... we had better back up such a bold claim. In fact there are two things we'd better establish: first, that we eventually will get a pair whose second number equals 0; and second, that the first number of that pair really will be the gcd of the original two numbers.

Notice that every time we replace the old pair $(a, b)$ with the new pair $(b, r)$, the newer pair has a *smaller* second number than the old pair's second number. This is simply an outcome of the Division Algorithm—the remainder is always smaller than the number we're dividing by. So every time we perform steps 1 and 2 of the Euclidean Algorithm, the second number gets smaller. This is exactly the situation that Fact 1.2 talks about: if we start writing down a sequence of nonnegative numbers one by one (in this case, the second numbers in all these pairs), and each number is smaller than the previous one, then eventually we must hit 0. This shows that at some point, we will get a pair of the form $(d, 0)$.

Good so far, but why will that first number $d$ actually equal $\gcd(a, b)$? Notice that at each step, we replace the old pair of numbers $(a, b)$ by the new pair $(b, r) = (b, a - qb)$. But adding a multiple of one number to another number doesn't change their greatest common divisor—Fact 2.13 tells us that $\gcd(b, a - qb) = \gcd(b, a)$, which Fact 2.12 tells us is itself equal to $\gcd(a, b)$. In other words, every time we repeat the first two steps of the Euclidean Algorithm, the new pair of numbers has the same gcd as the old pair of numbers! And of course, if this is true for each individual step, then it doesn't matter how many steps we perform—every single pair has the same gcd as the original pair.

Now it's easy to see why $d$ actually equals $\gcd(a, b)$: the last pair is $(d, 0)$, and $\gcd(d, 0) = d$ (Fact 2.11); all the pairs have the same gcd, which we now know is $d$, and therefore $\gcd(a, b) = d$.

Example. Let's use the Euclidean Algorithm to compute the greatest common factor of $a = 1356$ and $b = 414$.

$$\begin{aligned}
1356 &= 414 \times 3 + 114, &&\text{so } \gcd(1356, 414) = \gcd(414, 114);\\
414 &= 114 \times 3 + 72, &&\text{so } \gcd(414, 114) = \gcd(114, 72);\\
114 &= 72 \times 1 + 42, &&\text{so } \gcd(114, 72) = \gcd(72, 42);\\
72 &= 42 \times 1 + 30, &&\text{so } \gcd(72, 42) = \gcd(42, 30);\\
42 &= 30 \times 1 + 12, &&\text{so } \gcd(42, 30) = \gcd(30, 12);\\
30 &= 12 \times 2 + 6, &&\text{so } \gcd(30, 12) = \gcd(12, 6);\\
12 &= 6 \times 2 + 0, &&\text{so } \gcd(12, 6) = \gcd(6, 0).
\end{aligned}$$

We stop now, since the second number in this last pair equals 0; the first number in that pair, 6, is the greatest common divisor we're looking for. Indeed, since $\gcd(6, 0) = 6$ (see Fact 2.11), we conclude that $\gcd(1356, 414) = 6$ as well.

What a great algorithm—we calculate the greatest common divisor of two numbers, without ever writing down any of the factor of either number! Score one for building big truths upon little truths.

It's not too hard to convert this algorithm for calculating greatest common divisors into a procedure for finding integer solutions to the equation $ax + by = \gcd(a, b)$. All we have to do is write out all the steps in the Euclidean algorithm, and then start doing "backwards substition" and a little bit of bookkeeping. The best way to understand how to work backwards in this way is through another example.

EXAMPLE. Since $\gcd(1356, 414) = 6$, the Euclidean Algorithm will allow us to find integers integers $u$ and $v$ such that $6 = 1356u + 414v$. We start with the second-to-last step of the Euclidean Algorithm from the previous example, which tells us that $6 = 30 - 12 \times 2$. Then, working backwards one line at a time:

$$\begin{aligned}
12 &= 42 - 30 \times 1, &\quad \text{so } 6 &= 30 - (42 - 30 \times 1) \times 2 \\
&& &= 42 \times (-2) + 30 \times 3; \\
30 &= 72 - 42 \times 1, &\quad \text{so } 6 &= 42 \times (-2) + (72 - 42 \times 1) \times 3 \\
&& &= 72 \times 3 + 42 \times (-5); \\
42 &= 114 - 72 \times 1, &\quad \text{so } 6 &= 72 \times 3 + (114 - 72 \times 1) \times (-5) \\
&& &= 114 \times (-5) + 72 \times 8; \\
72 &= 414 - 114 \times 3, &\quad \text{so } 6 &= 114 \times (-5) + (414 - 114 \times 3) \times 8 \\
&& &= 414 \times 8 + 114 \times (-29); \\
114 &= 1356 - 414 \times 3, &\quad \text{so } 6 &= 414 \times 8 + (1356 - 414 \times 3) \times (-29) \\
&& &= 1356 \times (-29) + 414 \times 95.
\end{aligned}$$

Thus we have found a solution to $6 = 1356u + 414v$, namely $u = -29$ and $v = 95$.

Of course, if the original numbers $a$ and $b$ are actually relatively prime, then this procedure will find numbers $x$ and $y$ such that $ax + by = 1$, just as Consequence 2.3 says is possible.

## 4. Pythagoras and the irrationality of $\sqrt{2}$

When we learned about irrational numbers, we were probably given $\sqrt{2}$ as an example. But how do we know that this number is really irrational?

EXAMPLE. We can certainly get very close to $\sqrt{2}$ with rational numbers:

$$\begin{aligned}
\sqrt{2} &= 1.4142135623730950\ldots \\
\tfrac{41}{29} &= 1.4137\ldots \\
\tfrac{1393}{985} &= 1.41421319\ldots \\
\tfrac{47321}{33461} &= 1.41421356205\ldots \\
\tfrac{54608393}{38613965} &= 1.4142135623730948\ldots
\end{aligned}$$

So who's to say that if we tried a little harder, we couldn't get $\sqrt{2}$ exactly as a fraction? Or equivalently, if we looked far enough in the decimal expansion of $\sqrt{2}$, who's to say that it wouldn't start repeating?

In fact, the ancient Greeks felt this way—in fact, they thought that every number was rational (in our modern terminology). But Pythagoras discovered a proof that $\sqrt{2}$ was in fact irrational! Reportedly, he was so shaken by this discovery that he swore his school/cult of mathematicians to secrecy; and when one of them leaked the news to outsiders, his betrayed brethren drowned him. ... At the risk of suffering the same fate, we'll show you a proof that no rational number (fraction) can possibly equal $\sqrt{2}$.

Suppose that $\sqrt{2}$ were a rational number, say

$$\sqrt{2} = \frac{p}{q}.$$

As with any fraction, we can assume that $p$ and $q$ are relatively prime (see Consequence 2.9). Squaring both sides of this equation, we see that

$$2 = \frac{p^2}{q^2},$$

or, rearranging terms,

$$2q^2 = p^2.$$

Now the left-hand side is an even number, so the right-hand side is also an even number. This tells us that $p$ is itself an even number, since the square of an even number is even and the square of an odd number is odd. Since $p$ is even, we can write $p = 2r$ for some number $r$. Then we have

$$2q^2 = (2r)^2,$$

which becomes, after cancelling a factor of 2 from both sides,

$$q^2 = 2r^2.$$

Now the right-hand side is clearly even, so by the same reasoning as before, we deduce that $q$ itself must be even.

But wait a minute! If $p$ is even and $q$ is even, then 2 divides both $p$ and $q$, and hence 2 divides their greatest common divisor $\gcd(p, q)$ ... the problem is, we started by assuming that $\gcd(p, q) = 1$, which is not a multiple of 2. This is a contradiction, which is unavoidable as soon as we assume that $\sqrt{2}$ is a rational number; our only recourse is to grudgingly (like Pythagoras) admit that $\sqrt{2}$ is in fact an irrational number.

You can use this method to show that, whenever $\sqrt{n}$ is not an integer (that is, whenever $n$ is not a square), then $\sqrt{n}$ is in fact irrational. With a little more cleverness, you can even show that whenever $n$ is not a square, any expression of the form $\frac{a}{b}\sqrt{n} + \frac{c}{d}$ is irrational if $a$, $b$, $c$, and $d$ are integers (with $b$ and $d$ nonzero, of course).

## 5. A geometric detour

We're used to the fact that properties of pairs of real numbers can be viewed by graphing them as points in the plane; for instance, we know that the pairs of real numbers that are solutions of certain equations like $y = mx + b$ make up a single straight line when we plot them in the plane, while others such as $(x - a)^2 + (y - b)^2 = r^2$ make circles, and so on.

Similarly, there are some properties of integers that have graphical interpretations in terms of the corresponding points in the plane.

A pair $(x, y)$ of two integers is called a **lattice point** of the plane. Lots of lattice points are pictured in Figure 2.1. Let's say that two lattice points P and Q are **mutually visible** (and that Q is visible from P and vice versa) if the line segment joining P and Q contains no lattice points other than the endpoints P and Q. In other words, if two friends were standing at the two lattice points P and Q and every other lattice point had a tree, being mutually visible means that the friends would be able to see each other because there were no trees blocking their line of sight.

EXAMPLE. The lattice points $P = (1, 1)$ and $Q = (3, 2)$ of Figure 2.1 are mutually visible. However, the lattice points $(0, 0)$ and $S = (-2, -4)$ are not mutually visible, since the line segment joining them contains the point $R = (-1, -2)$.

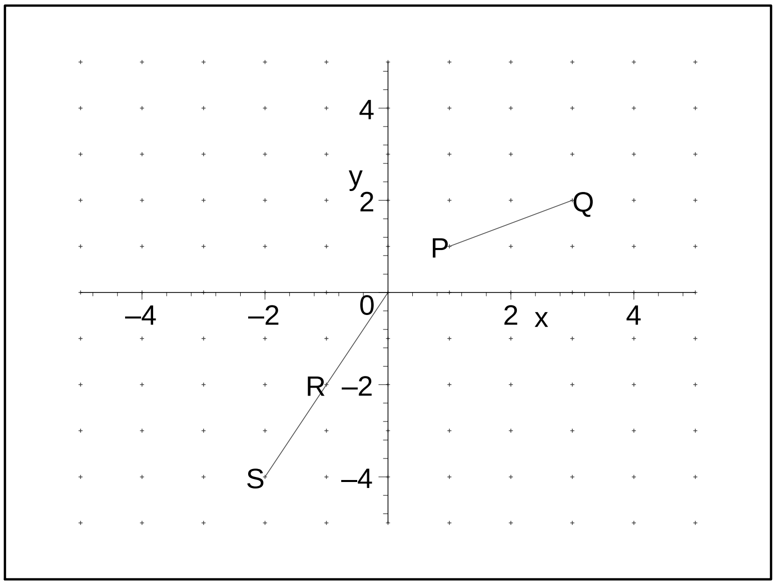


FIGURE 2.1. Mutual visibility of lattice points

It might be somewhat surprising to hear that this property of mutual visibility is directly related to greatest common divisors!

**Theorem 2.14.** *The lattice point $(a, b)$ is visible from the origin $(0, 0)$ if and only if $a$ and $b$ are relatively prime.*

*Proof:* First let's assume that $a$ and $b$ are relatively prime, and show that the point $(a, b)$ is visible from the origin. If we let $(c, d) \neq (0, 0)$ be any nonzero lattice point on the line going through the points $(0, 0)$ and $(a, b)$, this means that we have to show that $(c, d)$ cannot be between them.

We know that we can find integers $x$ and $y$ such that $ax+by = 1$ (Consequence 2.3). Multiplying this equation through by $c$, we obtain

$$acx + bcy = c. \tag{2.1}$$

Now if $(c, d)$ is on the line going through the points $(0, 0)$ and $(a, b)$, we know that

$$\frac{d-0}{c-0} = \frac{b-0}{a-0},$$

or in other words $ad = bc$. Using this fact in equation (2.1), we see that

$$acx + ady = c.$$

Since $a$ clearly divides the left-hand side of this equation, we see that $a$ divides $c$. But Fact 1.8 tells us that a nonzero multiple of $a$ is at least as big as $a$ itself—in other words, $|c| \geq |a|$, and there's no way for the point $(c, d)$ to be between the origin and $(a, b)$. Therefore the lattice point $(a, b)$ is indeed visible from the origin.

Now let's prove the other half of this theorem: assuming that $a$ and $b$ are *not* relatively prime, let's show that the point $(a, b)$ is *not* visible from the origin. If we let $d = \gcd(a, b)$, then $d > 1$ since $a$ and $b$ are not relatively prime. Then it is easy to check that the point $(\frac{a}{d}, \frac{b}{d})$ is a lattice point that lies on the line segment between the origin and $(a, b)$ (the details are left for you as an exercise). Therefore the lattice point $(a, b)$ is not visible from the origin in this case. □

In Figure 2.2, we have plotted the lattice points in the first quadrant (i.e., those with positive coordinates) that are visible from the origin. This plot is very æsthetically pleasing (so much so that it has graced the cover of at least one number theory textbook).

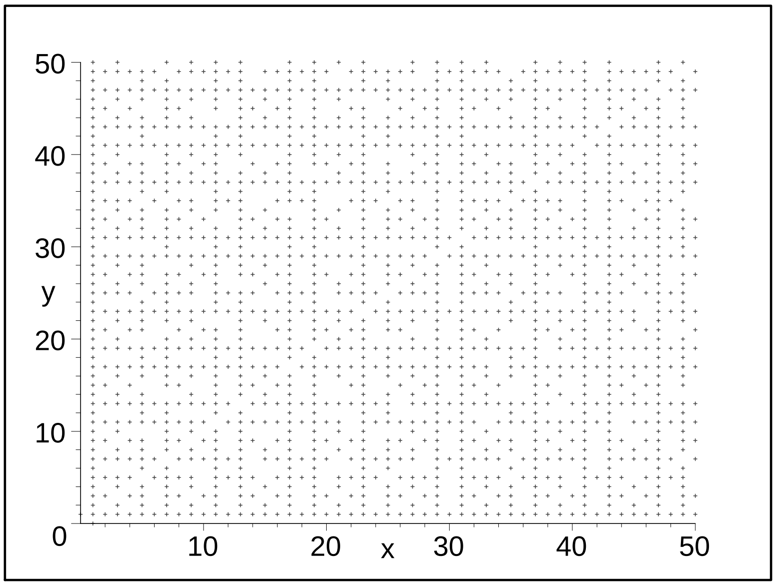


FIGURE 2.2. The lattice points in the first quadrant that are visible from the origin

## Problems for Chapter II

**2.1.** Knowing that $31 \times 999 - 632 \times 49 = 1$, find all solutions of $999x - 49y = 5000$.

**2.2.** Prove the converse of Fact 2.4. In other words, show that if $\gcd(ab, n) = 1$, then both $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$.

**2.3.** Here's a hint for the following pair of problems: between them, there are five possible solutions.

*a.* You have some pennies, dimes, and quarters—100 coins in all—totalling \$5.00. How many of each type of coin do you have?
*b.* You have some pennies, dimes, and quarters—100 coins in all—totalling \$4.99. How many of each type of coin do you have?

**2.4.** Provide a proof of Fact 2.6.

**2.5.** Provide a proof of Fact 2.7.

**2.6.** Provide a proof of Consequence 2.9.

**2.7.** Suppose $a$ and $b$ are integers that are relatively prime. Let $c$ be any integer. Show that if $a \mid c$ and $b \mid c$ then $ab \mid c$. Does this always work if $a$ and $b$ are not relatively prime?

**2.8.** Let $x$ and $y$ be relatively prime numbers. Show that there are unique numbers $a$ and $b$ satisfying $0 \le a < y$, $0 \le b < x$, and $ax - by = 1$.

**2.9.** We saw in an example on page 5 that $\gcd(140, 168) = 28$. Use the Euclidean Algorithm to verify this, and find integers $x$ and $y$ such that $140x + 168y = 28$.

**2.10.** Find the greatest common divisor of 246 and 951. Also, find integers $u$ and $v$ such that $246u + 951v = \gcd(246, 951)$.

**2.11.** Find the greatest common divisor of 42823 and 6409. Also, find integers $u$ and $v$ such that $42823u + 6409v = \gcd(42823, 6409)$.

**2.12.** Provide a proof of Fact 2.11.

**2.13.** Provide a proof of Fact 2.12.

**2.14.** Show that $\frac{1}{2} + \frac{\sqrt{3}}{4}$ is irrational.

**2.15.** Find all of the lattice points that lie on the line given by the equation $y = \frac{5}{3}x - \frac{7}{3}$. Do the same thing for the line $y = \frac{5}{3}x - \frac{7}{6}$.

**2.16.** Justify the claim made near the end of the proof of Theorem 2.14: if $d = \gcd(a, b) > 1$, then $(\frac{a}{d}, \frac{b}{d})$ is a lattice point that lies on the line segment between the origin and $(a, b)$.