Number Theory and Cryptography
(V55.0106)

Notes by Professor Melvin Hausner
New York University

Fall, 2002

Introduction.

Since the theory of numbers concerns itself with the familiar numbers 1, 2, 3, . . . , it might seem at first glance to be little more than grade school arithmetic. We shall see that this is far from true. The first clue that we are dealing with something more than a simple subject is the three dots in the expression "1, 2, 3, . . . " The three dots, which translate into "and so on" is the clue that tells us that we are dealing with *infinitely many* numbers. As such, since we cannot examine all of the integers one by one, we may well expect to find many mysteries and unsolved problems regarding these numbers. In fact this is true, as we shall point out. However, we shall also be able to solve many problems that seem at first sight to be intractable.

Throughout the text, when we speak of numbers, we understand ordinary whole numbers, including zero and negative numbers. These are called integers. Much of what many students know about numbers has been handed down as fact, and these are by now taken for granted. In what follows, we shall investigate many of these "facts" a little more deeply. In many cases, we will explain why they are true by giving proofs. Along the way, however, many new ideas will be introduced. We should mention at the outset, that the topic of number theory was once considered to be a field of mathematics with no practical applications. Recently, however, it has proved extremely useful in the study and applications of cryptography. In a later chapter, we shall explore this further.

We shall take for granted that you are familiar with some simple facts about integers. These include the following.

Arithmetic operations. For example $43 + 58 = 101$, $21 \times 65 = 1,365$, $31^2 = 961$. These are easily found on a calculator, which we assume you have. However, a calculator has limitations, since it can usually accept at most nine or ten digits. So if you have to add or multiply two 40 digit numbers, you would have to revert to the old grade school way of computation without a calculator[1] or else have a powerful computer program to do this exactly. In all arithmetic calculations, the answer is always understood to be exact. So if you use a calculator to find that $2^{50} = 1.12589990684 \times 10^{15}$, you do not have the exact answer. All you have is the first 12 digits of a 16 digit number. When dealing with integers, we will usually want the exact answer. Calculators only give approximations for very large numbers. For example, if you are used to writing $1/3 = .333$, you are using an approximation. The calculator which gives $1/3 = 0.333333333$ is also giving an approximation.

Algebra. For example, you should know that $(x+y)^2 = x^2+2xy+y^2$. and $n(n+1) = n^2+n$,

[1] We won't do this in this class!

and you should be able to solve the equation $2x+4 = 7x-3$, and understand that the solution need not be an integer.

For the present, we take it for granted that the reader of these notes knows what it means for one number to *divide* another.[2] We also take it for granted that the reader knows that a *prime number* is a number larger than 1, which is divisible only by itself and by 1.[3] A few examples of numbers that are not primes (called *composite numbers*) are 51, 91, and 543,678,967,805. Do you see why? Here are a few questions about numbers. How many can you answer?

- What is the 20th prime number?
- Is 571,435,871,001 prime number? What about 34,571?
- How many numbers divide 120?
- Is the fraction $28,841/33,043$ in lowest terms?
- The numbers $1-1+41=41,\ 4-2+41=43,\ 9-3+41=47,\ 16-4+41=53$ are all primes. Is it true that n^2-n+41 is always a prime for all positive integers n?
- The numbers $4=2+2$, $6=3+3$, $8=5+3$, and $10=7+3$ are all sums of two primes. Is every even number greatere than 2 a sum of two primes?
- The pairs (3,5), (5,7), (11,13), (17,19), (29,31) all consist of twin prime numbers. (These are primes whose difference is 2.) Are there infinitely many twin primes?
- The odd perfect squares 1, 9, and 25 all leave a remainder of 1 when divided by 8. Is this true for the square of every odd number?
- The numbers $2=1+1,\ 9=9+0,\ 13=4+9$, and $34=9+25$ are all sums of two squares. However, $3,\ 14$, and 21 are not. Which numbers are the sum of two squares? Which are not?
- Which numbers are the sum of 4 squares?

The above list consists of a few questions in number theory. Though simple to ask, some are questions, including two of the ones stated above, that nobody today still knows the answer to. (These are the twin prime problem as well as the problem of the sum of two primes.) The problem of factoring very large numbers turns out to be important in cryptography, where the fastest computers still have to spend many hours deciding if a number is prime. We shall analyze some of these problems in lecture and in lab to discover some of the methods used to solve these and similar problems.

[2] For example, 2 divides 6, 7 divides 35, and with the help of a calculator, or by "long division," you can find that 56,891 divides 5,582,827,612, and that 97 does not divide 312,681.

[3] For example, the first five primes are 2, 3, 5, 7, 11.

1 Division

Quotients and Remainders. We start by reviewing something probably learned in grade school: how to divide two number to get a quotient and remainder. We will want to do this on a calculator and on a computer. We first start with a simple example.

Example 1.1 *Divide 57 by 13 and find the quotient and remainder.*

Method:

$$\begin{array}{r r} & 4 \\ 13 & \overline{\big)\ \ 57} \\ & \underline{-52} \\ & 5 \end{array}$$

This is the way I did it in grade school. Since teaching methods change, you might not have seen this before!

So the quotient is 4 and the remainder is 5.

The method is as follows. To divide 57 by 13, we estimate 4 as the approximate integer quotient. Multiply 4 by 13 to get 52, subtract from 57 to get the remainder 5. Here, the relationship of the quotient q and remainder r is

$$57 = 13 \cdot 4 + 5 = 13q + r$$

Dividing this equation by 13, we obtain $57/13 = q + r/13$, where $r/13$ is the fractional part of the quotient 57/13. To do this with a calculator, we find $57/13 = 4.3846$, and we can read the quotient $q = 4$. The fractional part is .3846. As above, this is $r/13$, so we should get the remainder r if we multiply by 13. If we do this on the calculator we get 4.9998. We understand that this is only approximate, as most decimals are, and since we must have an integer for the answer, we make the sensible guess that $r = 5$. The recommended (and safe) way is to use whole numbers. Thus $57 = 13q + r$ and so $r = 57 - 13q = 57 - 52$ as before.

Let's illustrate with large numbers.

Example 1.2 *Divide 68,934 by 5,791 and find the quotient q and remainder r. Express the relationship between these numbers in a simple formula.*

Method: Using a calculator, we find $68,934/5,791 = 11.9036$. Therefore $q = 11$ and $r = 68,934 - 11(5,791) = 5,233$. The relationship is $68,934 = 5,791(11) + 5,233 = 5,791q + r$.

This computation can easily be set up on a spreadsheet. The lab for this course does this on an Excel spreadsheet called *Division*. In theory this can done without a calculator or computer, if you are willing to undergo a process called "long division." Happily we shall not do this.

Summarizing: If a and b are integers with $b > 0$, we can always find a quotient q and a remainder r such that

$$a = bq + r \text{ with } 0 \leq r < b \tag{1}$$

Equation (1) is called the Division Algorithm. The quotient q is called a div b in most computer languages. The remainder is called a mod b. The text introduced the "div" and "mod" notations on page 67. The notation a div b is supposed to remind you that you are dividing a by b but are conveniently dropping any remainder or fractional part. The spreadsheet Excel does not have a div function, but it uses INT(a/b) instead. (Think: the integer part of a/b.) In Excel, the remainder a mod b is written MOD(a, b).

Note that the remainder r is always less than the denominator b, and can be 0 (if the division "comes out even.")

Definition 1.3 *We say that b* divides *a, or that b* is a factor of *a, if a/b is an integer, or equivalently that $a = bq$ for some integer q. The standard way of writing this is $b|a$. (Read: b* divides *a.) We also say that a* is a multiple of *b*

Another way of putting this is that $r = 0$ in Equation (1).

In high school algebra, it was usually taken for granted that variables such as a, b, x, y designated real numbers. However, throughout this course we shall assume that they represent integers, either positive, negative, or zero. This is an important change in usage. The word number will similarly refer to integers only.

Such basic ideas as "even" and "odd" are defined using the division algorithm. A number n is even if $2|n$; it is odd if $2 \not| n$ (read as 2 does not divide n). Equivalently, a number is odd if the remainder when divided by 2 is 1.

Do not confuse the "divides" sign | with the "divided by" sign /. Thus, we have $2|6$, but $6/2 = 3$.

Examples.
(a) Clearly $1|a$ since $a = 1 \cdot a$. Similarly $a|a$ when $a > 0$, since $a = a \cdot 1$.
(b) If $a, b > 0$ then $b|ab$.
(c) If $a > 0$, then $a|0$.
(d) If $c|b$ and $b|a$ then $c|a$. For we have $b = cq_1$ and $a = bq_2$ for integers q_1 and q_2. So $a = cq_1q_2$, and therefore $c|a$.

The statement in (d) is called *transitivity of division.*

For example, if a number is divisible by 21 then it is divisible by 7. This follows from (d). For suppose $21|n$. Since $7|21$, we get $7|n$ by transitivity.

The following result is useful and fairly easy to prove.

Theorem 1.4 *If $c|a$ and $c|b$, then $c|(ax+by)$ for any integers x and y.*

Proof: We have $a = cq_1$ and $b = cq_2$, so $ax + by = acq_1 + bcq_2 = c(aq_1 + bq_2)$. This gives the result.

A number of the form $ax+by$ is called a linear combination of a and b. So this result simply states that if a number divides two numbers a and b, it divides any linear combination of them. Note that in line with our previous statement, these letters refer to integers only.

For example, if x and y are any integers, $7|(21x - 35y)$. This is because $7|21$ and $7|35$.

The Greatest Common Divisor.
When we reduce a fraction to lowest terms, we find a divisor of the numerator and the denominator (a common divisor) and cancel it. Thus we have the familiar computation

$$\frac{35}{45} = \frac{5\cdot 7}{5\cdot 9} = \frac{\cancel{5}\cdot 7}{\cancel{5}\cdot 9} = \frac{7}{9}$$

To reduce the fraction a/b to lowest terms, it would be necessary to find the greatest common divisor of a and b. This is simply called $\gcd(a,b)$. This computation is very cumbersome if the numerator and denominator are large. For example, how would you reduce the fraction $28,841/33,043$ to lowest terms? The method we now show handles this problem very quickly, and was first done by Euclid. The technique is called the Euclidean Algorithm.

Lemma 1.5 *Let $a = bq + r$. Then any divisor of both a and b is also a divisor of b and r. Conversely, any divisor of both b and r is also a divisor of a and b. Thus $\gcd(a,b) = \gcd(b,r)$.*

Proof: First, suppose $d|a$ and $d|b$. Then since $r = a - bq$, we have $d|r$ since r is a linear combination of a and b. Thus $d|b$ and $d|r$.

Conversely, if $d|b$ and $d|r$, then since $a = bq + r$ is a linear combination of b and r, we see that $d|a$ and so $d|a$ and $d|b$. This proves the result.

In words, $\gcd(a,b)$ can be found by finding the remainder r when a is divided by b and computing $\gcd(b,r)$. We then use the same result to simplify $\gcd(b,r)$, and continue until we find the answer. Let's use this method to find gcd$(75, 55)$. (Of course this can immediately be done by most students, but let's illustrate the method.) Dividing, we have

$$\begin{aligned}
\underline{75} &= \underline{55} \cdot 1 + \underline{20} \\
\underline{55} &= \underline{20} \cdot 2 + \underline{15} \\
\underline{20} &= \underline{15} \cdot 1 + \underline{5} \\
\underline{15} &= \underline{5} \cdot 3 + 0
\end{aligned}$$

These equations show that

$$\gcd(75, 55) = \gcd(55, 20) = \gcd(20, 15) = \gcd(15, 5) = \gcd(5, 0) = 5$$

using the above theorem successively, and the fact that $\gcd(a, 0) = a$ when $a > 0$.[4] This is a general technique. Instead of finding $\gcd(a, b)$ we find the remainder r when a is divided by b and find $\gcd(b, r)$. We keep repeating the process until the remainder is 0, and then the last non-zero remainder is the required gcd. As noted above, this technique is called the Euclidean Algorithm.[5] For simplicity, we have assumed that a and b are positive in this statement of the Euclidean algorithm, and we will often make this assumption in what follows.

We can now reduce $28,841/33,043$ to lowest terms! The following table systematically gives the numerator, denominator, quotient and remainders in the Euclidean Algorithm.

Numerator	Denominator	Quotient	Remainder
33,043	28,841	1	4,202
28,841	4,202	6	3,629
4,202	3,629	1	573
3,629	573	6	191
573	191	3	0

The gcd is 191. Note that in each line, the numbers move over one to the left, and the quotients are ignored. Finally, we reduce to lowest terms:

$$\frac{28,841}{33,043} = \frac{191 \cdot 151}{191 \cdot 173} = \frac{151}{173}$$

The Euclidean Algorithm computation will be done automatically in the lab, using the Excel spreadsheet called *GCD*.

Many facts about number theory were simply told to us at an early age, and so we take them for granted. For example, suppose you know that $5|7x$. Does it follow that $5|x$? We were taught to think somewhat as follows:

[4] Any number divides 0, so $\gcd(a, 0)$ is the greatest divisor of a, namely a itself.

[5] Euclid was looking for the "greatest common measure" of two lengths, but his idea and proof were essentially as described above.

> $\frac{7x}{5}$ is a whole number, and so there must be cancelations. There is no cancelation of 5 with 7, so all the cancelations are with x, and so $5|x$.

Here, the result is true, but the reasoning is suspect. Here is a real proof:

> We are given that $5|7x$. Also $5|5$. Therefore by the linear combination theorem, $5|(3 \cdot 7x - 4x \cdot 5)$, or using algebra, $5|x$.

Query: Suppose we are given that $6|15x$. Can we say that $6|x$? What can we say about divisors of x?

The correct proof given above is based on the simple observation that $1 = 7 \cdot 3 - 5 \cdot 4$. We were able to express 1 as a linear combination of 5 and 7. Here $\gcd(5, 7) = 1$. We shall now show that if $d = \gcd(a, b)$, then d is a linear combination of a and b.

Theorem 1.6 *Let $d = \gcd(a, b)$. Then there are integers x and y such that*

$$d = ax + by$$

Remark: The proof will show how to compute x and y. In the lab, the spreadsheet *GCD* also computes the values of x and y.

Proof: If we divide a by b to get $a = bq + r$, we know that $d = \gcd(b, r)$, and we note that $r = a - qb = a \cdot 1 + b(-q)$, a linear combination of a and b. If we continue the Euclidean Algorithm, we divide again we divide b by r to find $b = rq_1 + r_1$. Then the second remainder $r_1 = b - rq_1$ is also a linear combination of a and b since b and r are. Continuing in this way, we can show that every remainder is a linear combination of a and b. In particular d is, since it is the last non-zero remainder.

We illustrate this technique with a simple numerical example.

Example 1.7 *Find $d = \gcd(92, 17)$ and express it as a linear combination of 92 and 17.*

Method: The Euclidean algorithm gives

$$\begin{aligned} 92 &= 17 \cdot 5 + 7 \\ 17 &= 7 \cdot 2 + 3 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

Starting from the top, we get

$$7 = \underline{92} - 5 \cdot \underline{17}.$$

We underline the original numbers to keep track of them. Now use the second equation to get

$$3 = \underline{17} - 7 \cdot 2 = \underline{17} - (\underline{92} - 5 \cdot \underline{17}) \cdot 2 = \underline{17} - 2 \cdot \underline{92} + 10 \cdot \underline{17} = 11 \cdot \underline{17} - 2 \cdot \underline{92}.$$

Finally, using the last equation and the previous expressions for the remainders 7 and 3, we obtain

$$1 = 7 - 3 \cdot 2 = (\underline{92} - 5 \cdot \underline{17}) - 2(11 \cdot \underline{17} - 2 \cdot \underline{92}) = \underline{92} - 5 \cdot \underline{17} - 22 \cdot \underline{17} + 4 \cdot \underline{92} = 5 \cdot \underline{92} - 27 \cdot \underline{17}.$$

Theorem 1.6 has an interesting corollary. We have defined $\gcd(a, b)$ as the greatest common divisor of a and b. Thus, if $d|a$ and $d|b$, then $d \leq \gcd(a, b)$. We can now state more.

Corollary 1.8 *If $d|a$ and $d|b$, then $d|\gcd(a, b)$*

For a proof, we can write $\gcd(a, b) = xa + yb$, so $d|\gcd(a, b)$, since $\gcd(a, b)$ is a linear combination of a and b. In words, any common divisor of a and b is also a divisor of their gcd.

For example, if two numbers have gcd 6, then 4 cannot divide both of these numbers.

Corollary 1.9 $\gcd(a, b) = 1$ *if and only if 1 is a linear combination of a and b.*

Proof: Theorem 1.6 shows that if $\gcd(a, b) = 1$, then 1 is a linear combination of a and b. Conversely, if 1 is a linear combination of a and b then any divisor of a and b must also divide 1, and so must equal 1. So $\gcd(a, b) = 1$.

Theorem 1.10 *Let $\gcd(a, b) = 1$ and $a|bn$. Then $a|n$.*

Proof: The proof parallels the example above, when $5|7x$. Since $\gcd(a, b) = 1$, we have $1 = ax + by$ for some integers x and y. Multiply by n to get $n = axn + bny$. Now since $a|a$ and $a|bn$, we have $a|n$ since n is a linear combination of a and bn.

Definition 1.11 *If $\gcd(a, b) = 1$, we say that a and b are relatively prime.*

Thus, we can restate the Theorem 1.10. If a and b are relatively prime, and $a|bn$, then $a|n$. A useful alternative is the following result.

Corollary 1.12 *If a and b are relatively prime, $a|n$ and $b|n$, then $ab|n$.*

Proof: Since $a|n$, we have $n = aq$ for some q. Thus $b|aq$. Since a and b are relatively prime, $b|q$ by the above result, and so $q = bq_1$ for some q_1. Therefore $n = aq = abq_1$. This shows that $ab|n$.

If we "divide out" the gcd of two numbers, the resulting quotients are relatively prime.

Theorem 1.13 *Let $d = \gcd(a, b)$. Then a/d and b/d are relatively prime.*

Proof: Write $d = xa + yb$. Divide by d to get $1 = x(a/d) + y(a/d)$. This shows that a/d and b/d are relatively prime by Corrolary 1.9.

Theorem 1.14 $\gcd(xa, xb) = x \cdot \gcd(a, b)$ *for any* $x > 0$.

Proof: Let $d = \gcd(a, b)$. Then since $d|a$ and $d|b$, we have $xd|xa$ and $xd|xb$, so xd is a common divisor of xa and xb. Therefore

$$\gcd(xa, xb) \geq xd$$

On the other hand, we know that x is a common divisor of xa and xb. Therefore by Corollary 1.8, $\gcd(xa, xb)$ is a multiple of x, say xD. Thus $xD|xa$ and $xD|xb$, and therefore $D|a$ and $D|b$. Since D is a common divisor of a and b, we must have $D \leq d$. Thus,

$$\gcd(xa, xb) = xD \leq xd.$$

These two inequalities prove the result.

We can give a useful test to decide whether two numbers a and b are relatively prime. Using Definition 1.11 and Theorem 1.6, we know that if two numbers are relatively prime, then 1 is a linear combination of them. The following theorem is a valid converse.

Theorem 1.15 *Let $ax + by = 1$ for some integers x and y. Then a and b are relatively prime.*

Proof: Let d be a common divisor of a and b. Then, by Theorem 1.4, d divides any linear combination of a and b. Therefore $d|1$ and so $d = 1$ since the only positive divisor of 1 is 1. Therefore $\gcd(a, b) = 1$ and so a and b are relatively prime.

For example, all that's required to show that 5 and 7 are relatively prime is to observe that $3 \cdot 7 - 4 \cdot 5 = 1$.

Here's an example to use some of these results. It will be used in the next section.

Example 1.16 *Given:* $\gcd(a, b) = 1$. *Prove:* $\gcd(a + b, a - b) = 1$ *or* 2.

Method: Let $c = a + b$ and $d = a - b$. Add to eliminate b. This gives $c + d = 2a$. Similarly, by subtracting, we get $c - d = 2b$. Now let f be any common divisor of c and d. Thus $f|c$ and $f|d$. Therefore, by the above two equations, we find $f|2a$ and $f|2b$. Therefore $f|\gcd(2a, 2b)$. But by Theorem 1.14, $\gcd(2a, 2b) = 2\gcd(a, b) = 2$. Therefore, $f|2$ and so $f = 1$ or $f = 2$.

The Equation ax+by=c.
An equation such as

$$3x + 7y = 41 \tag{2}$$

is familiar to us as the equation of a line. In this section, we want to confine ourselves to integers, so the equation is not immediately accessible using algebraic techniques. What are the integer solutions to this equation? What solutions are non-negative?

To solve this equation, we first note that the coefficients 3 and 7 are relatively prime, so it is possible to find numbers r and s such that

$$3r + 7s = 1.$$

In fact, by observation, we see that we can take $r = -2$ and $s = 1$. Now multiply this equation by 41, the constant term in the equation we wish to solve. This gives

$$3(41r) + 7(41s) = 40$$

Thus, one solution of Equation 2 is $x = 41r = -82$ and $y = 41$. Having found one solution $(-81, 41)$, we can now find all solutions as follows. Let (x, y) be a solution of Equation 2. We also know that $(-82, 41)$ is a solution. Thus

$$3(-82) + 7(41) = 41 = 3x + 7y$$

Transposing, we get $3(x+82)+7(y-41) = 0$. It follows from this equation that $3|7(y-41)$. Now, since 3 and 7 are relatively prime, we have $3|(y - 41)$. So $y - 41 = 3t$ for some integer t. Substituting into $3(x + 82) + 7(y - 41) = 0$, we find $3(x + 82) + 21t = 0$. Solving for x, we find $x = -82 - 7t$. Thus the most general solution of Equation 2 is

$$x = -82 - 7t;\ y = 41 + 3t \text{ where } t \text{ any integer.}$$

How do we find the non-negative solutions? We must have

$$-82 - 7t \geq 0;\ 41 + 3t \geq 0$$

These two inequalities can be solved[6] for t:

$$t \leq -82/7 = -11.7;\ t \geq -41/3 = -13.6 \text{ or } -13.6 \leq t \leq -11.7$$

[6] Solving inequalities of this sort is very similar to solving equations. However a possible mishap can occur when multiplying or dividing an inequality by a number. If that number is negative, the inequality reverses from < to >, and vice versa.

or simply $-13 \leq t \leq -12$, since t must be an integer. So only two values $t = -12$ and $t = -13$ give non-negative solutions. These are $(x, y) = (2, 5)$ (for $t = -12$) and $(x, y) = (9, 2)$ (for $t = -13$.

We now generalize this procedure. We start with a necessary condition.

Theorem 1.17 *If the equation $ax + by = c$ has any integer solutions, then $gcd(a, b)|c$. Conversely, if $d = \gcd(a, b)$, and $d|c$, then the equation $ax + by = c$ has an integer solution.*

Proof: If this equation has a solution, then c is a linear combination of a and b, so since d divides both a and b, we have $d|c$. Conversely, we know that d is a linear combination of a and b: $d = ra + sb$. Multiplying by c/d, we obtain $c = r(c/d)a + s(c/d)b$. So a solution is given by $x = r(c/d)$ and $y = s(c/d)$.

We now generalize the method we used for solution of Equation 2.

Theorem 1.18 *Let $d = \gcd(a, b)$. Suppose that $d|c$, and let (x_0, y_0) be a solution of the equation $ax + by = c$. Then the most general solution of this equation is given by*

$$x = x_0 + t(b/d);\ y = y_0 - t(a/d)$$

where t is an arbitrary integer.

Proof: To simplify, we divide the equation $ax + by = c$ by d to get the equivalent equation

$$a'x + b'y = c' \text{ where } a' = a/d,\ b' = b/d,\ c' = c/d$$

Then a' and b' are relatively prime, by Theorem 1.13. We are given that (x_0, y_0) satisfies the original equation, and so it satisfies the simplified version. Thus, $a'x_0 + b'y_0 = c'$. Now if (x, y) is any other solution, we have

$$a'x + b'y = c' = a'x_0 + b'y_0$$

Thus, $a'(x - x_0) + b'(y - y_0) = 0$. This implies that $b'|a'(x - x_0)$, and since a' and b' are relatively prime, $b'|(x - x_0)$, and so $x - x_0 = b't$ for some integer t. Substituting in $a'(x - x_0) + b'(y - y_0) = 0$, we find $a'b't + b'(y - y_0) = 0$, so $y - y_0 = -a't$. Rewriting, using $a' = a/d,\ b' = b/d$, we get the result.

For example, to completely solve the equation $6x + 9y = 30$, we first divide by $3 = \gcd(6, 9)$ to simplify the equation to $2x + 3y = 10$. By observation, this has a solution $x = 5,\ y = 0$. Therefore the most general solution is given by: $x = 5 + 3t,\ y = 0 - 2t = -2t$.

We end with a more complicated example.

Example 1.19 *Find positive (whole) numbers x, y, z such that $x + y + z = 50$ and $2x + 7y + 9z = 200$.*

Method: Eliminate x to get $x = 50 - y - z$, and $2(50 - y - z) + 7y + 9z = 200$. This gives

$$100 - 2y - 2z + 7y + 9z = 200 \text{ or } 5y + 7z = 100$$

Note that the coefficients 5 and 7 are relatively prime. One solution of this latter equation is seen to be $y = 20$ and $z = 0$. So the general solution is $y = 20 + 7t$, $z = -5t$ and $x = 50 - y - z = 50 - (20 + 7t) + 5t = 30 - 2t$. We now look for positive solutions. Since $z = -5t$, we must have negative t. But from $y = 20 + 7t$, we see that the only possibilities are $t = -1$ and $t = -2$. These values give the required answer: $(x, y, z) = (32, 13, 5)$ and $(x, y, z) = (34, 6, 10)$.

Equations with integer solutions are called Diophantine equations, named after the Greek mathematician Diophantus of Alexandria (c. 250 A.D.) whose text *Arithmetic* contained many algebraic problems calling for integer solutions. Today, equations with integer solutions are called Diophantine Equations. We have discussed linear Diophantine equations above. A familiar quadratic Diophantine equation is $x^2 + y^2 = z^2$. Solving this Diophantine quadratic equation amounts to finding a right triangle with integer sides. A familiar solution is $(x, y, z) = (3, 4, 5)$ (the 3–4–5 right triangle), since $3^2 + 4^2 = 9 + 16 = 25 = 5^2$. Do you know of other integer solutions? Later we shall find all solutions to this famous Diophantine equations.

Exercises on Divisors.

1. In each of the following, a number $a > 0$ is divided by a number $b > 0$ to obtain a quotient q and a remainder r.
(a) $a = 532$ and $b = 17$. Find q and r.
(b) $a = 3,467$ and $b = 1,045$. Find q and r.
(c) $a = 67,345$ and $bq = 54,000$. Find r.
(d) $a = 6,400$ and $b = 1$. Find q and r.
(e) $a = 17$ and $r = 0$ and $b > 1$. Find b and q.

2. In each of the following, find the gcd of the two numbers with the help of a calculator. Show all intermediate steps.
(a) gcd(5135,3081)
(b) gcd(1141,6357)
(c) gcd(3820595,21823)

3. In each of the following, find the gcd of the two numbers and express it as a linear combination of the numbers. Use a calculator if necessary. Do not use the spreadsheet program.

(a) 23 and 75
(b) 9 and 69
(c) 101 and 23

4. Prove that the sum of two odd numbers is even.

5. Prove that the product of two consecutive numbers is even.

6. Prove if the square of an odd number is divided by 8, the remainder is 1. (*Hint*: Use the above exercise.)

7. Prove: If $d|a$ and $d|b$ then $d^2|ab$.

8. If $d|a$ and $e|b$, prove $de|ab$.

9. Prove: If $7|11n$ then $7|n$.

10. Prove: If $12|n$ and $20|n$ then $60|n$.

11. Prove: If $18|n$ and $12|n$ then $36|n$.

12. Let $a|n$ and $b|n$, and let $d = \gcd(a, b)$. Prove that $(ab/d)|n$. (This generalizes Theorem 1.10.)

13. Define the least common multiple of a and b, or $\text{lcm}(a, b)$ as a number m which is the smallest of the common multiples of a and b.[7] Letting $d = \gcd(a, b)$, prove, using the previous exercise, that $\text{lcm}(a, b) = ab/d$, and so $\text{lcm}(a, b)\gcd(a, b) = ab$.

14. Suppose a and b are relatively prime. Prove that $a + 2b$ and b are relatively prime.

15. Suppose a and b are relatively prime. Prove that $a + 2b$ and $a + 3b$ are relatively prime.

16. Suppose a and b are relatively prime. Prove that $a + 2b$ and b are relatively prime.

17. Suppose a and b are relatively prime. Prove that $3a+2b$ and $2a+b$ are relatively prime. *Hint*: Let $c = 3a + 2b$ and $d = 2a + b$. Now eliminate a algebraically, and then eliminate b to express both a and b in terms of c and d.)

18. Suppose a and b are relatively prime. Prove that the greatest common divisor of $3a+2b$ and $2a + 5b$ is either 1 or 11. *Hint*: Let $c = 3a + 2b$ and $d = 2a + 5b$. Now eliminate a

[7] The lcm is often used to add fractions, where it is called the "least common denominator" or lcd. Thus,

$$\frac{3}{20} + \frac{7}{12} = \frac{9}{60} + \frac{35}{60} = \frac{44}{60} = \frac{11}{15}$$

Here, the common denominator 60 is $\text{lcm}(20, 12)$, and the factor 4 which was canceled is gcd(44,60).

algebraically, and then eliminate b as in Example 1.

19. Suppose a and b are relatively prime. Let

$$\begin{aligned} c &= ra + sb \\ d &= ta + ub \end{aligned}$$

Show that $\gcd(c, d) | (ru - st)$. *Hint*: Eliminate a and eliminate b.

20. Suppose that a and b are relatively prime so that we have $ar + bs = 1$ for some integers r and s. Show that r and s are also relatively prime.

21. (a) Find the general solution to the Diophantine equation $11x + 17y = 246$.
(b) Find all positive solutions of this equation.

22. As in Exercise 1 for the equation $13x + 29y = 424$.

23. As in Exercise 1 for the equation $13x - 29y = 424$.

24. As in Exercise 1 for the equation $30x + 114y = 2784$.

25. As in Exercise 1 for the equation $91x + 329y = 9424$.

26. As in Exercise 1 for the equation $91x - 56y = 861$.

27. Does the Diophantine equation $134x + 298y = 3,679$ have a solution? Explain.

28. A manufacturing company needs two types of screws, costing \$1.31 and \$1.51 apiece. The buyer buys a bunch of these and paid \$174.31 for the lot. How many screws did the buyer purchase?

29. Three types of toys cost \$3, \$7, and \$12 respectively. A person is given \$400 to spend all, and to buy exactly 100 toys. She wants to get as many of the \$12 toys as possible. How many of each type does she buy?