Chapter 5

The Augmented Euclidean Algorithm

Let a and b be nonzero numbers, and let d be their greatest common divisor. Loosely speaking, d is the size of the smallest step one can take by combining steps of size a and steps of size b. The augmented Euclidean algorithm determines *how* to take a step of size d using steps of size a and steps of size b. More precisely, it determines *two* ways of taking a step of size d using steps of size a and steps of size b; the steps of size a predominate in one and the steps of size b predominate in the other.

In formulas, the algorithm finds solutions u, v, x, y of the pair of equations

$$d + ub = va \tag{1}$$
$$d + xa = yb$$

where a and b are given nonzero numbers and d is their greatest common divisor. One can take a step of size d to the right either by taking v steps of size a to the right and u steps of size b to the left, or by taking y steps of size b to the right and x steps of size a to the left.

The **augmented Euclidean algorithm** can be formulated in the following way:

Input: Two nonzero numbers a and b
Algorithm:
    Let $d = a$, $e = b$, $u = 0$, $v = 1$, $x = 0$, $y = 1$
    While $d \neq e$
        If $d > e$, change d to $d - e$, u to $u + y$, and v to $v + x$
        Else change e to $e - d$, x to $v + x$, and y to $u + y$
    End
Output: Equations $d + ub = va$ and $d + xa = yb$

If u, v, x, and y are ignored, the algorithm is simply the Euclidean algorithm "subtract the lesser from the greater" and it terminates with both d and e equal to the greatest common divisor of a and b as in Chapter 4. The equations $d + ub = va$ and $e + xa = yb$ hold at the outset because $d + 0 \cdot b = 1 \cdot a$ and $e + 0 \cdot a = 1 \cdot b$ hold at the outset. Each step preserves the truth of these equations, as can be seen in the following way. If $d + ub = va$ and $e + xa = yb$ both hold, their sum $d + (u + y)b = e + (v + x)a$ holds. If $d > e$, the step of the algorithm leaves e, x, and y unchanged, so the equation $e + xa = yb$ remains true, while $d + ub = va$ becomes $(d - e) + (u + y)b = (v + x)a$ which is true because it results when e is subtracted from both sides of the sum. In the same way, if $d < e$, the equation involving d is unchanged and the equation involving e is changed to the equation obtained by subtracting d from both sides of the sum. Thus, both equations are true at each step, including the last step, at which $d = e$, which shows that the output equations are true.

The working of the algorithm can be seen clearly if the steps are shown in tabular form, with one column for each of d, e, u, v, x, and y and with one row for each step of the algorithm.

For example, when $a = 23$ and $b = 14$, the table takes the form

d	e	u	v	x	y
23	14	0	1	0	1
9	14	1	1	0	1
9	5	1	1	1	2
4	5	3	2	1	2
4	1	3	2	3	5
3	1	8	5	3	5
2	1	13	8	3	5
1	1	18	11	3	5

ending with the equations $1 + 18 \cdot 14 = 11 \cdot 23$ and $1 + 3 \cdot 23 = 5 \cdot 14$.

One of the main facts of applied number theory is that *the augmented Euclidean algorithm is quite practical, even when the input numbers are enormous.* Thus, the solutions of (1) for any given pair of nonzero numbers a and b can be found with ease. However, this is true only after the algorithm is modified, as the Euclidean algorithm was modified in Chapter 4, so that it subtracts convenient *multiples* of the lesser from the greater:

Input: Two nonzero numbers a and b
Algorithm:
  Let $d = a$, $e = b$, $u = 0$, $v = 1$, $x = 0$, $y = 1$
  While $d \neq e$
    Let $k = 1$
    While $d > 2ke$ or $e > 2kd$
      Multiply k by 2
    End
    If $d > e$, change d to $d - ke$, u to $u + ky$, and v to $v + kx$
    Else change e to $e - kd$, x to $kv + x$, and y to $ku + y$
  End
Output: Equations $d + ub = va$ and $d + xa = yb$

This "speeded up" version of the basic algorithm simply finds the largest power of 2, call it $k = 2^e$, for which the basic algorithm will repeat the same step k times in a row, and performs these k steps all at once. In the example above, the speeded up algorithm produces the same calculation as the basic algorithm except that, at the end, instead of subtracting 1 from 4 three times in a row, the speeded up algorithm first subtracts it *twice* in a single step and then subtracts it once more. The effect in this case is simply to

skip the third line from the bottom in the table, which is scarcely an improvement in the computation. On the other hand, the speeded up algorithm is a huge improvement if at one point of the algorithm a step is encountered in which the smaller of d and e is *much* smaller, as is the case, for example, in the first step of the algorithm when it is applied to $a = 1002$ and $b = 5$.

Exercises for Chapter 5

Study Questions.

1. (a) Find a multiple of 123 that is one more than a multiple of 458, and find a multiple of 458 that is one more than a multiple of 123, showing the working of the algorithm in full.

(b) Find a solution of the simultaneous congruences $x \equiv 100 \bmod 123$ and $x \equiv 300 \bmod 458$.

(c) Find the *smallest* solution of these simultaneous congruences.

2. (a) Show that if a and b are nonzero numbers and d is their greatest common divisor, then a solution (x, y) of $d+xa = yb$ implies a solution in which $x < b$. (b) Show that there is *at most one* solution (x, y) in which $x < b$. [Reduce to the case $d = 1$ and regard the equation as a congruence mod b.]

3. Experience with the augmented Euclidean algorithm leads one to expect that the solutions of equations (1) it produces are the smallest possible ones, which is to say that $x < b$ and $u < a$. That this is indeed the case can be seen by restating the augmented Euclidean algorithm in the following way:

Input: Two nonzero numbers a and b
Algorithm:
  Set $u = x = 0$ and $v = y = 1$
  While $\frac{a}{b} \neq \frac{u+y}{v+x}$
    If $\frac{a}{b} < \frac{u+y}{v+x}$ set $y = u + y$ and $x = v + x$
    Else set $u = u + y$ and $v = v + x$
  End
Output: The equations $d + ub = va$ and $d + xa = yb$ where d is the greatest common divisor of a and b

(In accordance with the definition of "number" in Chapter 1, the fractions $\frac{a}{b}$, $\frac{u+y}{v+x}$ are not numbers. The statements $\frac{a}{b} \neq \frac{u+y}{v+x}$ and $\frac{a}{b} < \frac{u+y}{v+x}$ are shorthand for the statements $a(v+x) \neq b(u+y)$ and $a(v+x) < b(u+y)$.)

(a) Prove that this algorithm produces the same (finite) sequences of values of u, v, x, and y that the augmented Euclidean algorithm does.

(b) Prove that if $xu + 1 = yv$ and if $\frac{p}{q}$ is a fraction satisfying $\frac{u}{v} < \frac{p}{q} < \frac{y}{x}$, then $q > v$ and $q > x$. (This is the fundamental fact in the theory of *Farey series.* See, for example, [**E1,** p. 264].)

(c) Use (b) to show that the final value of x is less than b and the final value of u is less than a.

4. Given just *one* of the equations of (1), there is an easy way to determine the other. Find it.

5. When a is relatively prime to b, the number v in (1) is called a *reciprocal of a mod b.* Explain. Thus, Exercise 3 of Chapter 4 states that if b is relatively prime to 6, then the reciprocal of 2 mod b is the sum of the reciprocal of 6 mod b and the reciprocal of 3 mod b.

6. How can a reciprocal of a mod b be used to solve a congruence of the form $ax \equiv c \bmod b$ for x when a, b and c are nonzero numbers and a and b are relatively prime?

7. Show that, when a and b are relatively prime, *division by a mod b is possible* in the sense that every congruence $ax \equiv c \bmod b$ has a solution x for every c and that any two solutions x are congruent mod b.

8. Exercise 3 implies that if a and b are relatively prime, then the number v, which is the reciprocal of a mod b, determines not only $u = \frac{va-1}{b}$ but also x and y in equations (1). Thus, the entire output of the augmented Euclidean algorithm can be deduced from the solution of the congruence $ax \equiv 1 \bmod b$. This can be accomplished by the following alternative algorithm:

Let the problem be to solve $ax \equiv c \bmod b$ when a, b, and c are given numbers and $a \leq b$. (If $a > b$, use the algorithm that follows to find the reciprocal of b mod a, from which the reciprocal of a mod b

can be deduced.) Let ma be the least multiple of a that is greater than b. The desired x satisfies $max \equiv mc \bmod b$, which is to say $a_1 x \equiv c_1 \bmod b$, where $a_1 = ma - b$ and $c_1 = mc$. If a does not divide b, then $a_1 < a$ and the new problem has the same form as the original problem, except that a is reduced. Repeated application of this reduction method must eventually reach a problem of this form in which a divides b. But $ax \equiv c \bmod qa$ has a solution if and only if a divides c, in which case the most general solution is $x \equiv \frac{c}{a} \bmod \frac{b}{a}$. (In particular, if $a = 1$, there is always a solution and the most general solution is $x \equiv c \bmod b$.)

Express this method of solving $ax \equiv c \bmod b$ as a formal algorithm.

Computations.

9. Implement the augmented Euclidean algorithm on a computer and see for yourself how well it works even with numbers that have many, many digits.

10. The number 200560490130 is the product $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \cdots \cdot 29 \cdot 31$ of the first 11 prime numbers. For various large numbers, find their greatest common divisors with this number. What is the largest number m for which it is true that "a number with m digits that is relatively prime to 200560490130 is prime"?