

MAT246H1S Lec0101 Burbulla

Chapter 7 Lecture Notes The Euclidean Algorithm and Applications

Winter 2019

Chapter 7: The Euclidean Algorithm and Applications

7.1: The Euclidean Algorithm

7.2: Applications

What is a gcd?

Defintion: if m and n are two natural numbers, the largest natural number that is a factor of both m and n is called the *greatest common divisor* of m and n , and we denote it by $\gcd(m, n)$.

Examples:

- ▶ $\gcd(14, 18) = 2$
- ▶ $\gcd(27, 45) = 9$
- ▶ $\gcd(1292, 14440) = 76$ because

$$1292 = 2^2 \cdot 17 \cdot 19 \text{ and } 14440 = 2^3 \cdot 5 \cdot 19^2,$$

implying that $\gcd(1292, 14440) = 2^2 \cdot 19 = 76$.

This last example exhibits one way to find $\gcd(m, n)$, namely in terms of the prime factorizations of m and n . But there is another way, which employs repeated division.

The Euclidean Algorithm, An Example

We shall exhibit this other method, which is known as the Euclidean Algorithm, with the numbers $a = 14440$ and $b = 1292$.

$$14440 = 11 \cdot 1292 + 228 \quad (1)$$

$$1292 = 5 \cdot 228 + 152 \quad (2)$$

$$228 = 1 \cdot 152 + 76 \quad (3)$$

$$152 = 2 \cdot 76 \quad (4)$$

And $\gcd(1292, 14440) = 76$. What is particularly useful about this algorithm, as we shall see, is that it allows us to write $\gcd(a, b)$ as an integral linear combination of a and b : (3) $\Rightarrow 76 = 228 - 152$; (2) $\Rightarrow 76 = 228 - (1292 - 5 \cdot 228) = 6 \cdot 228 - 1292$; and finally, (1) $\Rightarrow 76 = 6(14440 - 11 \cdot 1292) - 1292 = 6 \cdot 14440 - 67 \cdot 1292$.

The Euclidean Algorithm, In General

How to calculate $\gcd(a, b)$ if $a > b$, by repeated divisions:

$$a = q_0 \cdot b + r_0, \text{ with } 0 \leq r_0 < b, \quad (5)$$

$$b = q_1 \cdot r_0 + r_1, \text{ with } 0 \leq r_1 < r_0, \quad (6)$$

$$r_0 = q_2 \cdot r_1 + r_2, \text{ with } 0 \leq r_2 < r_1, \quad (7)$$

$$r_1 = q_3 \cdot r_2 + r_3, \text{ with } 0 \leq r_3 < r_2, \quad (8)$$

$$\vdots \quad (9)$$

$$r_{k-2} = q_k \cdot r_{k-1} + r_k, \text{ with } 0 \leq r_k < r_{k-1}, \quad (10)$$

$$r_{k-1} = q_{k+1} \cdot r_k + 0, \text{ that is, divide until } r_{k+1} = 0 \quad (11)$$

Then

$$\gcd(a, b) = r_k,$$

and by successive backward substitutions, we can find integers x and y such that $\gcd(a, b) = x a + y b$.

Why Does the Euclidean Algorithm Work?

1. First of all, since the sequence of remainders is decreasing,

$$b = r_0 > r_1 > r_2 > \cdots > r_{j-1} > r_j > \cdots > r_k > r_{k+1},$$

eventually $r_{k+1} = 0$. Even if the remainder only decreased by 1 after each division, the remainder would be 0 after b steps.

2. r_k divides both a and b : by 'back substituting' we see that

$$r_k \mid r_{k-1}, r_k \mid r_{k-2}, \dots, r_k \mid r_2, r_k \mid r_1, r_k \mid r_0,$$

Then (6) implies $r_k \mid b$, and then (5) implies $r_k \mid a$.

3. Finally, if d is any divisor of a and b , we can 'forward substitute' to conclude that

$$d \mid r_0, d \mid r_1, \dots, d \mid r_{k-1}, d \mid r_k.$$

Thus r_k is the *greatest* common divisor of a and b .

What Are Relatively Prime Natural Numbers?

Definition: the natural numbers m and n are *relatively prime* if $\gcd(m, n) = 1$. That is, their greatest common divisor is 1.

Example: let $m = 60, n = 13$. Then $\gcd(13, 60) = 1$; and

$$60 = 4 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1, \text{ so}$$

$$\begin{aligned} 1 &= 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3(13 - 8) = 5 \cdot 8 - 3 \cdot 13 = 5(60 - 4 \cdot 13) - 3 \cdot 13 = 5 \cdot 60 - 23 \cdot 13 \end{aligned}$$

Two Lemmas

Many of the results we proved in Chapter 4 can also be proved using gcd's.

Lemma 7.2.2: if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: if $p \mid a$ we are done. Otherwise p and a are relatively prime, i.e. $\gcd(a, p) = 1$. By the Euclidean Algorithm there are integers x and y such that $1 = ax + py$, implying $b = bax + bpy$. It is given that $p \mid ab$, so p divides the right side of this equation; hence it divides the left side: $p \mid b$.

Lemma 7.2.3: if the prime p divides the product of n numbers, then p divides at least one of the numbers.

Proof: by induction on n . Lemma 7.2.2 is the case $n = 2$. Now suppose $p \mid a_1 a_2 \cdots a_n$. If $p \mid a_1$ we are finished. If not, by Lemma 7.2.2, $p \mid a_2 \cdots a_n$. This is a product of $n - 1$ numbers, so by the induction hypothesis we can assume p divides one of the numbers $a_2, a_3, \dots, a_n$.

Fundamental Theorem of Arithmetic, Again

Theorem 7.2.4: the factorization of a natural number greater than 1 into primes is unique except for the ordering of the factors.

Proof: as before, if there were numbers with different prime factorizations, there would be a least such number N , by the well-ordering principle, such that

$$N = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s.$$

Since $p_1 \mid N$, p_1 must also divide $q_1 \cdot q_2 \cdots q_s$. By Lemma 7.2.3, $p_1 \mid q_j$, for some j . But since p_1 and q_j are both primes, we must have $p_1 = q_j = p$. Then $N/p < N$ would also be a number with at least two different prime factorizations, contradicting the fact that N was the least such number.

Finding Decryptors in RSA Cryptography

Another application of the Euclidean Algorithm is to finding the keys E and D for the RSA method of cryptography. Recall that the keys had to satisfy the condition $ED \equiv 1 \pmod{(p-1)(q-1)}$, for prime numbers $p, q, p \neq q$. We shall illustrate the procedure with our example from Chapter 6, in which $p = 7, q = 11$ and E was 43. Recall that E is the public key used to encrypt the message, and D is used to decrypt the message. Aside: of course, we must have $\gcd(E, (p-1)(q-1)) = 1$. In our example, $\gcd(43, 60) = 1$. After applying the Euclidean Algorithm, we obtain $1 = 7 \cdot 43 - 5 \cdot 60$. So

$$7 \cdot 43 \equiv 1 \pmod{60},$$

and we can take $D = 7$ as the decryptor. **Note:** if the coefficient x of 43 had not been between 0 and 60, we could have found D by adding to x a suitable multiple of 60. (Try starting with $E = 7$.) See additional calculations at the end of this section.

Linear Diophantine Equations

Definition 7.2.6: a *linear Diophantine equation* is an equation of the form $ax + by = c$, with a, b, c integers, for which we seek solutions (x, y) , with $x, y \in \mathbb{Z}$.

Theorem 7.2.8: the Diophantine equation $ax + by = c$ has integral solutions if and only if $\gcd(a, b) \mid c$.

Proof: let $d = \gcd(a, b)$. If there is a pair of integers x, y such that $ax + by = c$, then $d \mid a$ and $d \mid b$ together imply that $d \mid c$. For the converse: by the Euclidean Algorithm there are integers s and t such that $d = as + bt$. If $d \mid c$, then there is a integer k such that $c = kd$. Therefore

$$c = kd = a(sk) + b(tk),$$

and $x = sk$, $y = tk$ are integral solutions.

Example 1

Consider the equation $6x + 15y = 123$. $\gcd(6, 15) = 3 \mid 123$. By the Euclidean Algorithm, $3 = 1 \cdot 15 - 2 \cdot 6$, and so

$$123 = 41 \cdot 3 = 41(15 - 2 \cdot 6) = 6(-82) + 15(41),$$

and $(x_0, y_0) = (-82, 41)$ is one integral solution to the equation. Of course, there are infinitely many more solutions, namely of the form

$$(x, y) = (-82 + 5m, 41 - 2m),$$

for any integer m , since

$$\begin{aligned} 6x + 15y &= 6(-82 + 5m) + 15(41 - 2m) \\ &= 6(-82) + 15(41) + 30m - 30m \\ &= 123 + 0 = 123. \end{aligned}$$

Solution to a Linear Diophantine Equation

Theorem 7.2.10: let $d = \gcd(a, b)$ and suppose that (x_0, y_0) is one integral solution to the Diophantine equation $ax + by = c$. Then the solutions to the equation consist of all the pairs

$$(x, y) = \left(x_0 + m \cdot \frac{b}{d}, y_0 - m \cdot \frac{a}{d} \right),$$

such that $m \in \mathbb{Z}$.

Proof: if (x_0, y_0) is one solution to the equation, then, as in Example 1, each of

$$(x, y) = \left(x_0 + m \cdot \frac{b}{d}, y_0 - m \cdot \frac{a}{d} \right),$$

for any $m \in \mathbb{Z}$, will also be a solution. The hard part of the proof is to show that *all* solutions have this form.

Assume that (x_0, y_0) is a solution to the equation $ax + by = c$, and let (x, y) be any other solution to the equation. Thus

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

Since $d = \gcd(a, b)$, the quotients a/d and b/d are relatively prime. Thus (see Lemma 7.2.9), $a/d \mid y_0 - y$ and $b/d \mid x - x_0$. So there are integers m, n s.t. $x = x_0 + m(b/d)$ and $y = y_0 - n(a/d)$. Substituting into the original Diophantine equation gives

$$\begin{aligned} & a \left(x_0 + m \cdot \frac{b}{d} \right) + b \left(y_0 - n \cdot \frac{a}{d} \right) = c \\ \Rightarrow & ax_0 + am \cdot \frac{b}{d} + by_0 - bn \cdot \frac{a}{d} = c \\ \Rightarrow & m \cdot \frac{ab}{d} = n \cdot \frac{ba}{d} \Rightarrow n = m \end{aligned}$$

and we are done.

Euler's ϕ Function

Definition 7.2.12: for any natural number m , $\phi(m)$ is defined to be the number of numbers in the set $\{1, 2, 3, \dots, m-1\}$ that are relatively prime to m .

Examples:

- ▶ $\phi(6) = 2$, since in the set $\{1, 2, 3, 4, 5\}$ only 1 and 5 are relatively prime to 6.
- ▶ $\phi(7) = 6$, since all numbers in the set $\{1, 2, 3, 4, 5, 6\}$ are relatively prime to 7.
- ▶ $\phi(8) = 4$, since in the set $\{1, 2, 3, 4, 5, 6, 7\}$ only 1, 3, 5, and 7 are relatively prime to 8.
- ▶ $\phi(12) = 4$, since in the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ only 1, 5, 7 and 11 are relatively prime to 12.

Properties of Euler's ϕ Function:

Theorem 7.2.14: if p is a prime, then $\phi(p) = p - 1$.

Proof: p does not divide any of the numbers $1, 2, 3, \dots, p-1$.

Problem 26: if p is a prime and k is a natural number, then

$$\phi(p^k) = p^k - p^{k-1}.$$

Proof: the only numbers m , $1 \leq m \leq p^k$, not relatively prime to p^k are the p^{k-1} multiples of p : $1p, 2p, 3p, \dots, p^{k-1} \cdot p = p^k$. Thus $\phi(p^k) = p^k - p^{k-1}$.

Multiplicative Property: if m and n are relatively prime natural numbers, then $\phi(mn) = \phi(m)\phi(n)$.

Proof: exercise left for the student.

Problem 27: if $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$, then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

Proof: combine Problem 26 and the multiplicative property of ϕ .

Euler's Theorem

First we generalize Theorem 5.1.1: **Lemma 7.2.16:** if a and m are relatively prime and $ax \equiv ay \pmod{m}$, then $x \equiv y \pmod{m}$.

Proof: $m \mid ax - ay = a(x - y)$; m does not divide a ; and a and m have no common factors. Thus $m \mid x - y$ and $x \equiv y \pmod{m}$.

Theorem 7.2.17: suppose $a, m \in \mathbb{N}$, $m > 1$, and $\gcd(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof: see below.

Corollary 7.2.18: if $m = p$ is prime, and $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: $\phi(p) = p - 1$ and the result follows from Theorem 7.2.17.

Note: Corollary 7.2.18 is Fermat's Theorem; it is a consequence of Theorem 7.2.17, which is known as Euler's Theorem.

Proof of Euler's Theorem

The proof of Euler's Theorem is similar to the proof of Fermat's Theorem. Let $S = \{r_1, r_2, \dots, r_{\phi(m)}\}$ be the set of numbers in $\{1, 2, \dots, m-1\}$ that are relatively prime to m . Let

$$T = \{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\phi(m)}\}.$$

Since no two distinct elements in S are congruent to each other, neither are any two elements in T , by Lemma 7.2.16. Since a and m are relatively prime, so are m and each number $a \cdot r_j$ in T . Thus, each number in T is congruent to exactly one number in S . So

$$a \cdot r_1 \cdot a \cdot r_2 \cdots a \cdot r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Using Lemma 7.2.16 repeatedly we can cancel each r_j in the above congruency to conclude that

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Additional Calculations

$$60 = 1 \cdot 43 + 17$$

$$43 = 2 \cdot 17 + 9$$

$$17 = 1 \cdot 9 + 8$$

$$9 = 1 \cdot 8 + 1$$

$$8 = 8 \cdot 1 + 0, \text{ then}$$

$$1 = 9 - 8$$

$$= 9 - (17 - 9)$$

$$= 2 \cdot 9 - 17$$

$$= 2 \cdot (43 - 2 \cdot 17) - 17$$

$$= 2 \cdot 43 - 5 \cdot 17$$

$$= 2 \cdot 43 - 5(60 - 43)$$

$$= 7 \cdot 43 - 5 \cdot 60$$

$$60 = 8 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0, \text{ then}$$

$$1 = 4 - 3$$

$$= 4 - (7 - 4)$$

$$= 2 \cdot 4 - 7$$

$$= 2 \cdot (60 - 8 \cdot 7) - 7$$

$$= 2 \cdot 60 - 17 \cdot 7, \text{ so}$$

the multiplicative inverse, modulo 60, of 7 is -17 , or $-17 + 60 = 43$.

1. Calculate the multiplicative inverse of $3^{21} \pmod{16}$.

Solution: since 3 and 16 are relatively prime, Euler's Theorem implies

$$3^{\phi(16)} \equiv 1 \pmod{16} \Leftrightarrow 3^8 \equiv 1 \pmod{16}.$$

Thus $3^{24} \equiv 1 \pmod{16}$, which means the multiplicative inverse of 3^{21} is $3^3 = 27$. But

$$27 \equiv 11 \pmod{16},$$

so the answer is 11.

2. Calculate $\phi(675)$.

Solution: the prime factorization of 675 is $675 = 3^3 \cdot 5^2$, so

$$\phi(675) = \phi(3^3)\phi(5^2) = (3^3 - 3^2) \cdot (5^2 - 5) = 18 \cdot 20 = 360.$$