THE EUCLIDEAN ALGORITHM AND CONSEQUENCES

BURTON ROSENBERG
UNIVERSITY OF MIAMI

Contents

1. Groups and Rings

Definition 1.1. The pair $G, +$ with

$$+ : G \times G \to G$$

is a *group* when $+$ is an associative and for all $a, b \in G$ there exists a unique x solving $a + x = b$.[1] If $+$ is commutative the group is called *abelian*.

Example: The naturals[2] $\mathbb{N}$ are not a group for the operation addition, but adjoining the new elements 0 and a $-x$ for every x, we have the integers[3] $\mathbb{Z}$ which are a group with the operation addition.
Example: The naturals $\mathbb{N}$ are not a group for the operation multiplication, but adjoining the new elements $1/x$ for every x, we arrive at the rationals except for zero, which are a group with the operation multiplication.

Definition 1.2. The triple $G, +, \times$ is a *ring* when $G, +$ is an abelian group and

$$\times : G \times G \to G$$

Date: 27 October 2013.

[1] I might need one more axiom, see the appendix.

[2] The set of natural numbers is defined as $\mathbb{N} = \{1, 2, 3, \dots\}$

[3] The set of integers as defined as $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$

is an associative operation for which the distributive law holds,

$$\forall a, b, c \in G,\ a(b+c) = ab + ac \text{ and } (a+b)c = ac + bc.$$

Example: The integers are a ring with the typical and normal operating of addition and multiplication. Note the additional properties that the integers have an identity operator for multiplication and multiplication is commutative. This is called a *commutative ring with unit*.

Definition 1.3. For integer $a, b \in \mathbb{Z}$, a *divides* b, written $a \,|\, b$, if and only if there exists an integer $k \in \mathbb{Z}$ such that $ak = b$.

Example: The integers with multiplication $\mathbb{Z}, \times$ is not a group. For a given a, b, equation $a\,x = b$ is solvable over $\mathbb{Z}$ only if $a \,|\, b$.

Theorem 1.1. Suppose a, b are integers and the integer c divides a and b. Then c divides all linear combinations of a,

$$\forall s, t \in \mathbb{Z},\ c \,|\, (s\,a + t\,b).$$

Proof: The reader is encouraged to proof this for themselves. By the hypothesis, there exists $k_a, k_b \in \mathbb{Z}$ such that $a = k_a\,c$ and $b = k_b\,c$. Hence,

$$(s\,a + t\,b) = (s\,k_a\,c + t\,k_b\,b) = c\,(s\,k_a + t\,k_b).$$

□

Definition 1.4. Given a ring $R, +, \times$, an *ideal* is a subset $I \subseteq R$ that is a subgroup and conducts all of R into I, $R\,I \subseteq I$.

Motivation: An ideal is the kernel of any ring homomorphism to a quotient ring. As such, the zero must posses the power of the annihilator for multiplication.

Definition 1.5. Given a ring $R, +, \times$ and a subset $G \subseteq R$ of elements of S, the *ideal generated by* S, $I = \langle G \rangle$ is the minimal ideal containing G. The elements of G are said to be the *generators* of the ideal. An ideal that can be generated by a single generator is called a *principal ideal*.

Example: Given an integer a, the set of all multiples of a is an ideal,

$$\langle a \rangle = \{\, k\,a \,|\, k \in \mathbb{Z} \,\}.$$

The set of even integers is an ideal. The set of odd integers is not an ideal.

Theorem 1.2. In the ring of integers, all ideals are principal ideals.

This requires the Euclidean algorithm to prove. As a motivation, this algorithm uses repeated division to find the greatest common divisor among a set of elements. If the ideal is generated by this set, it is also exactly generated by the greatest common divisor.

Example: Given the unit interval $[0,1]$ the set of all subsets of $[0,1]$ is a ring with addition being set exclusive or and multiplication being set intersection. The zero is the empty set $\emptyset$ as $S \oplus \emptyset = S$; and the one is interval $[0,1]$, as $S \cap [0,1] = S$, for all $S \subset [0,1]$.
In this example divisibility is set inclusion, $s \mid u$ when $\exists t, s \cap t = u$.

2. The Euclidean Algorithm

It will turn out that generators form ideals by forming all possible linear combinations with the generators. For two generators in the ring of integers,

$$\langle a, b \rangle = \{ s\,a + t\,b \mid s, t \in \mathbb{Z} \}.$$

All these integers are necessarily in the ideal, as they are needed to be a subring, and the are also sufficient. This comes down to solving for an x in the ideal the equation $a + x = b$ where a and b are in the ideal.

Theorem 2.1. For all $a, b \in \mathbb{Z}$ in the ring of integers,

(1) $\langle a, b \rangle = \langle b, a \rangle$.
(2) $\langle -a, b \rangle = \langle a, b \rangle$.
(3) $\langle a, b \rangle = \langle a - b, b \rangle$.
(4) $\langle a, b \rangle = \langle b, r \rangle$ where $a \geq b > 0$ and r is the remainder of $a \div b$.

Proof. The first two facts are obvious. For the third, the computation,

$$i\,a + j\,b = i\,a - i\,b + (i + j)\,b = i\,(a - b) + (i + j)\,b,$$

implies that anything in $\langle a, b \rangle$ is in $\langle a - b, b \rangle$, and vice a versa. For $a \geq b > 0$, write $a = q\,b + r$ and apply fact three q times,

$$\langle a, b \rangle = \langle a - q\,b, b \rangle = \langle r, b \rangle = \langle b, r \rangle.$$

□

Definition 2.1. Let $a, b \in \mathbb{Z}$ be positive integers. A *common divisor* of a and b is any positive integer c such that $c \mid a$ and $c \mid b$. The collection of common divisors is ordered by divisibility with a greatest element is called the *greatest common divisor*.

Definition 2.2. Given integers a and b, define the integer $d = (a, b)$ as d is greatest common divisor of a and b when a and b are positive integers, and otherwise defined by $(a, b) = (b, a) = (-b, a)$ and $(0, a)$ for all a, including a equals zero. This d is also called without confusion the greatest common divisor.

Theorem 2.2 (Bézout's identity)**.** For a and b in the ring of integers,

$$\langle a, b \rangle = \langle d \rangle$$

where $d = (a, b)$.

Proof: Starting from $\langle a, b \rangle$, use the above properties to arrange things so that $\langle a, b \rangle = \langle s_0, s_1 \rangle$ and $s_0 \geq s_1 \geq 0$.

Let s_2 be the remainder of s_0 divided by s_1. In the case that s_1 is not zero, and repeat this process, getting a sequence of s_i such that $\langle s_{i-2}, s_{i-1} \rangle = \langle s_{i-1}, s_i \rangle$ and s_i is the remainder of s_{i-2} divided by s_{i-1}.

This process must terminate when $s_j = 0$, in which case we have,

$$\langle a, b \rangle = \langle s_{j-1}, 0 \rangle = \langle s_{j-1} \rangle.$$

Since $a, b \in \langle s_{j-1} \rangle$, $s_{j-1} \mid a, b$. So $s_{j-1} \mid (a, b)$.

Note that by the construction of s_{j-1}, there exists integers s and t such that,

$$s_{j-1} = s\, a + t\, b,$$

hence any common divisor of a and b divides s_{j-1}. Therefore $s_{j-1} = (a, b)$, the greatest common divisor of a and b. □

The above proof is an algorithm to arrive at integers s and t such that $(a, b) = s\, t + t\, b$. This is very valuable. It gives the value of (a, b) but also expresses that value as a linear combination of a and b.

Note well: In general, this process of reduction by repeated division need not end with a zero. This would be for non-principal ideals. For instance, in the ring of $\mathbb{Q}[x][y]$, polynomials in x and y with rational coefficients, then $\langle x, y \rangle$ ends with y being the remainder of x when divided by y, and x being the remainder when y is divided by x.

Terminology: The algorithm is called the *Euclidean algorithm*, and that it works in the ring of integers makes the ring of integers an *Euclidean domain*. The consequence of being an Euclidean domain is that every ideal is a principal ideal. When this is true, as it is for the integers, the ring is a *principal ideal domain*.

Theorem 2.3. The Euclidean algorithm is a polynomial time algorithm for solving Bézout's identity. That is, given integers a and b with greatest common divisor (a, b), calculate integers s and t such that,

$$(a, b) = s\, a + t\, b.$$

Proof: A ploynomial algorithm runs with the number of steps $O(n^c)$ for some integer c and n the problem size. The problem size here is the number of bits needed to write down the numbers a and b.

Not that each to steps the larger of the values is lessened by at least half. That is, one bit is lost in each two iterations, and each iteration is work polynomial in size (doing division). This then multiplies the per iteration work by the problem size, keeping the overall work polynomial. □

This is a worst case argument. The worse case time is required when a and b are neighboring Fibonacci numbers.

3. Modular Arithmentic

Definition 3.1. Let $R, +, \times$ be a ring, and $I \subset R$ an ideal in the ring. A *coset* is defined for $r \in R$ as,

$$r + I = \{\, r + i \,|\, i \in I \,\}$$

Theorem 3.1. Notation as above, two cosets are either identical or disjoint.

Proof: If cosets $a + I$ and $b + I$ intersect, then there are $i_a, i_b \in I$ such that $a + i_a = b + i_b$. Then for any $s \in a + I$,

$$s = a + i_s = (b + i_b - i_a) + i_s = b + (i_b + i_s - i_a) \in b + I,$$

because I is a group. Likewise, for any $s \in b + I$, then $s \in a + I$. Therefore $a + I = b + I$. □

Note: The cosets partition the ring. The above theorem shows the cosets are disjoint. For any $r \in R$, $r \in r + I$, since $0 \in I$. Hence the collection of coset covers all elements or R.

Definition 3.2. Given a ring $R, +, \times$ and an ideal $I \subseteq R$ of the ring, the collection of cosets is called R modulo I, written R/I.

Example: The collection of cosets $\mathbb{Z}/\langle\, m \,\rangle$ is commonly known as the integers modulo m, denoted $\mathbb{Z}_m$. A coset is represented by the smallest positive integer in the coset, and any integer is mapped to the representative for the coset in which the element resides.

Theorem 3.2. In the above notation, R/I is a ring. The ring operations in R/I are imposed upon it by the ring operations in R. The ring homomorphism $\phi : R \to R/I$ takes each $r \in R$ to the coset in which r resides.

Proof: The addition and multiplication operations in R/I are defined by the diagram,

$$\begin{array}{ccc} R \times R & \xrightarrow{\phi,\phi} & R/I \times R/I \\ {\scriptstyle\mathcal{O}}\downarrow & & {\scriptstyle\mathcal{O}'}\downarrow \\ R & \xrightarrow{\phi} & R/I \end{array}$$

by the mechanism,

$$(a + I) + (b + I) \xrightarrow{\phi^{-1}} (a + i_a) + (b + i_b) \xrightarrow{+} a + b + i \xrightarrow{\phi} (a + b) + I$$

and

$$(a + I)\,(b + I) \xrightarrow{\phi^{-1}} (a + i_a)\,(b + i_b) \xrightarrow{\times} a\,b + i \xrightarrow{\phi} a\,b + I.$$

What we are showing is that adding or multiplying representatives or adding any other element sharing the coset of the representative, gives the same answer. □

4. Units and Fields

Definition 4.1. Given a ring, $R, +, \times$ with a unit element 1 such that $1\,r = r$ for all $r \in R$, those r such that $r\,x = 1$ is solvable for x are called *units*, and is denoted R^*.

Example: In the ring $\mathbb{Z}_6$ of the six elements $0, 1, \ldots, 5$, the units are 1 and 5. That the other numbers are not units are show by considering $2 \cdot 3 = 4 \cdot 3 = 0$ in the ring (so inverting any of these would leave an non-zero element equating to zero).
Example: In the ring $\mathbb{Z}_7$ every non-zero element is a unit. This is demonstrated by $2 \cdot 4 = 3 \cdot 5 = 6 \cdot 6 = 1$.
Example: In the ring $\mathbb{Z}_9$ and non-nilpotent element is a unit, where *nilpotent* means at a power of the element equals 0.

Theorem 4.1. With the notation of the above definition, R^* is a group.

Proof The operation $\times$ is associative. Let $a\,x = b$ be an equation with $a, b \in R^*$. There exists an a' such that $a\,a' = 1$. There also exists a $x = a'\,b$, and

$$a\,x = a\,(a'\,b) = (a\,a')\,b = 1\,b = b.$$

□

Theorem 4.2. Given the ring $R, +, \times$ in a principal ideal domain, an ideal $\langle\, m \,\rangle \subseteq R$, and the modular ring $\phi : R \to M$ where $M = R/\langle\, m \,\rangle$. Then

$$M^* = \{\, u \in M \mid 1 = (\phi^{-1}(u), m) \text{ in } R \,\}.$$

They are recognized and their inverses in are calculated in polynomial time using the extended Euclidean algorithm.

Proof: Let $u' \in \phi^{-1}(u)$. The question of solvability of $u\,x = 1$ in M is equivalent to finding $s, t \in R$ such that,

$$1 = s\,u' + t\,m.$$

By Bézout's, this is solvable only if $(u', m) = 1$ and the extended Euclidean algorithm finds such s and t in polynomial time. Then,

$$\begin{aligned} \phi(s\,u' + t\,m) &= \phi(s)\,\phi(u') + \phi(t)\,\phi(m) \\ &= \phi(s)\,u + 0 \\ &= \bar{s}\,u = \phi(1) = 1. \end{aligned}$$

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

×	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

FIGURE 1. Arithmetic in the Galois field $\mathbb{F}_4 = \mathbb{F}_2[x]/\langle\, x^2+x+1 \,\rangle$

Hence $\bar{s}$ is the sought for x. □

Definition 4.2. The *Eulers totient function* $\varphi(n)$ is defined for the integers as the number of integers between 1 and n such that are relatively prime to n.

Theorem 4.3. With the above notation, $|\, M^* \,| = \varphi(m)$. In particular, if m is prime, all but one elements in M is a unit, that missing element being the zero element.

Definition 4.3. Let $R, +, \times$ be a ring with unit, and commutative multiplication. This ring is a *field* if all non-zero elements are units, $R^* = R \setminus \{0\}$.

Example: The set of rationals is a field. The reals are a field. The integers modulo a prime p, $\mathbb{Z}_p$, are a field, often denoted $\mathbb{F}_p$.
Example: Consider polynomials with coefficients in $\mathbb{F}_2$,

$$\mathbb{F}_2[x] = \sum c_i x^i.$$

These are a ring with a commutative multiplication and the unit element 1. By defining products of x properly, the ring becomes modulo this definition a field, called a *Galois field*.
The simplest case is to define $x^2 = x+1$. Create the ideal $I = \langle\, x^2+x+1 \,\rangle$ and the result of the homomorphism,

$$\begin{array}{rccc} \phi: & \mathbb{F}_2[x] & \to & \mathbb{F}_2[x]/I \\ & \sum c_i x^i & \mapsto & c_1 x + c_0 \end{array}$$

is a field with 4 elements.
Note that ϕ essentially maps x^2+x+1 to 0. This is equivalent to defining the inverse of x to be $x+1$. The inverse of x must be something. No other choice works. The case of $x\,x = 1$ is eliminated as the would result in $(x+1)(x+1) = 0$.
The full addition and multiplication tables are provided in Figure 1.

5. Number theory

Theorem 5.1. If integers m and n are relatively prime, $(m,n) = 1$, then $\varphi(m\,n) = \varphi(m)\,\varphi(n)$.

Proof: Let $c \in \mathbb{Z}^*_{m\,n}$. Then there exist s and t such that

$$1 = s\,c + t\,m\,n.$$

Setting $t' = tm$, the equation $1 = s\,c + t'\,n$ implies $\phi_n(c) \in \mathbb{Z}^*_n$. Likewise $\phi_m(c) \in \mathbb{Z}^*_m$. So we can define the map,

$$\begin{array}{rccc} \phi: & \mathbb{Z}^*_{m\,n} & \to & \mathbb{Z}^*_m \times \mathbb{Z}^*_n \\ & c & \mapsto & \phi_m(c), \phi_n(c) \end{array}$$

We show this map is a set isomorphism.
Injectivity: The individual maps ϕ_n and ϕ_m are homomorphisms. So if $\phi(c) = \phi(c')$ then $\phi(c - c') = (0, 0)$. Therefore both m and n divide the difference $c - c'$ and so does the least common multiple of m and n. Since the least common multiple of m and n is the produce mn divided by $(m, n) = 1$, then $mn \,|\, c - c'$. Hence $c = c'$. So the map is injective.
Surjectivity: From $(m, n) = 1$ find m', n' such that,

$$1 = m'm + n'n.$$

Consider $c = i\,m'm + j\,n'n$. Then,

$$\begin{array}{rcl} \phi_m(c) & = & \phi_m(i\,m'\,m + j\,n'\,n) \\ & = & \phi_m(i\,m'\,m) + \phi_m(j\,n'\,n) \\ & = & 0 + \phi_m(j)\,\phi_m(n'\,n) \\ & = & \bar{j}1 = \bar{j} \end{array}$$

and likewise $\phi_n(c) = \bar{i}$.
Apply this construction to an arbitrary $(\bar{j}, \bar{i}) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n$ to show the map's surjectivity. □

We state this theorem for the integers, as we are concerned with number theory. However, it works in a general commutative group.

Theorem 5.2 (Generalized Little Fermat)**.** For all $g \in \mathbb{Z}^*_m$, $g^{\varphi(m} = 1$.

Proof: Let $s = \prod_{g \in \mathbb{Z}^*_m} g$. Then

$$h^{\varphi(m)} s = h^{\varphi(m)} \prod_{g \in \mathbb{Z}^*_m} g = \prod_{g \in \mathbb{Z}^*_m} h\,g = \prod_{g \in \mathbb{Z}^*_m} g = s.$$

Now cancel s. □

6. Appendix: Axioms for groups and rings

The standard definition of a group has as axioms a unique and universal left and right zero, and commuting inverses. To the single axiom for a group given in the this note, I believe I must add the additional axiom,

$$\forall a, b \in G, \exists\, x : x + a = b$$

where x is not necessarily unique.

Theorem 6.1. In a group $G, +$, the $x \in G$ solving $a + x = a$ is universal for all $a \in G$. The unique value is denoted 0 and is the (additive) identity for the group.

Proof: Given the unique solution to,

$$a + 0 = a,$$

extend to any $c \in G$ by solving $y + a = c$ for y. Then,

$$\begin{aligned} c + 0 &= y + a + 0 \\ &= y + a \\ &= c \end{aligned}$$

By uniqueness any x solving $c + x = c$ equals 0. Hence 0 is a universal zero for the group. □

Definition 6.1. Given 0, define the solution to $a + x = 0$ as the (additive) inverse of a, denoted $-a$.

Theorem 6.2. In a group, inverses necessarily commute, $a + (-a) = (-a) + a$.

Proof:

$$\begin{aligned} (-a) + a &= (-a) + a + 0 \\ &= (-a) + a + (-a) + (- - a) \\ &= (-a) + 0 + (- - a) \\ &= (-a) + (- - a) \\ &= 0 \end{aligned}$$

□

Corollary 6.1. The inverse operation is an involution, $- - a = a$ for all $a \in G$.

Proof: Since $a + (-a) = -a + a = 0$, then a is the unique solution to $-a + x = 0$. Therefore $-(-a) = a$. □

Corollary 6.2. Every $a \in G$ commutes with 0, $a + 0 = 0 + a$.

Proof:

$$\begin{aligned} 0 + a &= (a + (-a)) + a \\ &= a + (-a + a) \\ &= a + 0 \end{aligned}$$

□

Theorem 6.3. That there are unique solutions to $a + x = b$, for any $a, b \in G$, there are unique solutions to $x + a = b$ for any $a, b \in G$.

Notes: We had to assume that there exists solutions to $x + a = b$. Now with unique inverses the uniqueness of the solution is confirmed.

Theorem 6.4. Given the ring $R, +\times$, for $a \in R$, $a0 = 0a = 0$.

Proof:

$$a0 + a0 = a(0 + 0) = a0$$

The uniqueness of the solution to $a0 + x = a0$ implies $a0 = 0$, for any a in the ring. Likewise,

$$0a + 0a = (0 + 0)a = 0a.$$

□

Theorem 6.5. Notation as above, for any $a, b \in R$, $a(-b) = (-a)b = -ab$.

Proof:

$$ab + a(-b) = a(b - b) = a0 = 0$$

The uniqueness of the solution to $ab + x = 0$ implies $a(-b) = -(ab)$. Likewise,

$$ab + (-a)b = (a - a)b = 0b = 0$$

□