Elementary Algebra
Chinese Remainder Theorem
Euclidean Algorithm

April 11, 2010

1 Algebra

We start by discussing algebraic structures and their properties. This is presented in more depth than what we really need at this point.

Given set G and a binary operation $*$, if each element in the set obeys the following 4 properties, then the set and its operation $(G, *)$ is called a *group*.

(i) *Closure.* If $a, b \in G$, them $a * b* \in G$.

(ii) *Existence of an identity element.* Suppose $e \in G$ is the identity element, then $a * e = e * a = a$ for all $a \in G$.

(iii) *Associativity.* $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

(iv) *Inverse.* For every $a \in G$, there exists an $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

If, in addition, each pair of elements $a, b \in G$ satisfies the commutative property, $a*b = b*a$, then the group $(G, *)$ is called an *Abelian group*.

The integers form an (Abelian) group under addition as the rule of composition; and so do the rational, real, or complex numbers. The identity element e in these cases are the number 0, and the inverse of a is $-a$. Remainders formed by dividing by a polynomial do likewise. For example, if we take the remainder after dividing by say $x^3 + 2x^2 + 1$, we can get all polynomials of degree 2 as remainders, and the identity is the 0 polynomial ($p(x) = 0$ everywhere) and the inverse of $p(x)$ is $-p(x)$. If one leaves out zero, the additive identity element, the rational, real, and complex numbers each form an (Abelian) group under the operation of multiplication. We need to leave out zero since this element does

not have a multiplicative inverse. So do non-zero remainders of integers upon dividing by a prime p, again with the remainder of a product obtained by taking the product and taking the remainder of the result. If we take the non-zero remainders after dividing by a composite (i.e. not prime) p then this does not form a group since some elements do not have inverses (e.g. if $p = 10$ then 5 has no multiplicative inverse since $5k \neq 1 \bmod 10$ for any k). (Another example are remainders (other than zero) upon dividing by a primitive polynomial, but this requires some definition.) A structure in which one has additive and multiplicative commutative groups like this is called a *field*.

$(F, +, *)$ is a *field* if

1. $(F, +)$ is an Abelian group.
2. $(F - \{0\}, *)$ is an Abelian group.
3. *Distributive property.* For all $a, b, c \in F$, $a * (b + c) = (a * b) + (a * c)$.

Fields have the important property that the product of any two non-zero elements is not zero, from which the fundamental theorem of algebra follows.

Lemma 1. *If a and b belong to a field F and $ab = 0$. Then either $a = 0$ or $b = 0$.*

Proof. Suppose that neither a nor b is 0. Then a^{-1} and b^{-1} exist and $(b^{-1})(a^{-1})(ab) = 1$. This implies that ab has an inverse, but this cannot be true since $ab = 0$. A contradiction. □

Lemma 2. *If a is a solution of the polynomial equation $p(x) = 0$ with coefficients in a field, then $(x - a)$ divides $p(x)$.*

Proof. We can express $p(x) = q(x)(x - a) + r$ for some polynomial $q(x)$ and remainder r. Since $p(a) = 0$, this implies that $r = 0$. □

Theorem 1. *A polynomial of degree $d \geq 1$ with coefficients in a field F can have at most d roots in F.*

Proof. We will show this by induction on k. If $ax + b = 0$, then $x = -ba^{-1}$ is the unique solution, so the statement is true for $k = 1$. Let $p(x) = 0$ have degree d, $d > 1$, and let $x = a$ be one of its roots. By lemma 2, we have $q(x) = p(x)(x - a)^{-1}$, where the degree of $q(x)$ is $d - 1$, and by the induction hypothesis, $q(x)$ has at most $d - 1$ roots. Lemma 1 says that every root of $q(x)(x - a)$ is either a root of $q(x)$ or a root of $(x - a)$. Thus, this implies that $p(x) = q(x)(x - a)$ has at most $(d - 1) + 1 = d$ roots. □

Remainders of integers upon dividing by a prime p form the field Z_p, with addition and multiplication both defined modulo p. Suppose now we consider a number N that is the product of two primes, p and q. Suppose we now consider remainders upon dividing by N. Does Z_N form a field?

It does not. The remainders again form an additive group but, as mentioned earlier, even with zero left out they do not form a multiplicative group. For example, the remainder p times the remainder q has remainder zero. (Thus the nonzero elements are not closed under multiplication.) Actually it also violates the property that each element should have a multiplicative inverse (this is why we tried to have 0 left out); check for yourself that neither p nor q will have a multiplicative inverse in $Z_N - \{0\}$. Here is a way to salvage a multiplicative group here. The remainders that are relatively prime to N have the property that the product of any two is still relatively prime to N. These relatively prime remainders form a group called Z_N^* under multiplication modulo N. (Again, satisfy yourself that the multiplicative identity element 1 is in the group, and each element has a multiplicative inverse.) For example, if $N = 15$, the elements of Z_N^* are the non-zero remainders which are neither divisible by 3 nor by 5, i.e. $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. There are 8 elements in Z_{15}^*. In Z_{15}^*, 7 and 13 are multiplicative inverses to each other (since their product equals 1 modulo 15). We actually do not need that N is the product of two primes; for any integer N, the non-zero remainders that are relatively prime to N form the multiplicative group Z_N^*.

Orders and Subgroups. If we have a group, G, the number of elements in G is called the *order* of G, written $o(G)$ or $|G|$. The order of $(Z_p, +)$ is p. The order of $(Z_p - \{0\}, \times)$ is $p - 1$. The order of Z_N^* is the number of remainders which are relatively prime to N, which if $N = pq$, where p and q are primes, is $(p-1)(q-1) = N - p - q + 1$. To see this, observe that the remainders in $\{1, \ldots, N-1\}$ that have a factor in common with N are multiples of either p or q but not of both. There are $q - 1$ of the former type, $p - 1$ of the latter. So the order of Z_N^* is $(N-1) - ((p-1) + (q-1)) = N - p - q + 1$. For example, for $N = 15$, we have that the order of Z_{15}^* is $2 \cdot 4 = 8$, and indeed, this is the number of elements we found.

A group G is said to have a *subgroup* H if H is a subset of G, and H is also a group (under the same operation $*$ as G). Check for yourself, that if we know G is a group, and we want to know if some subset H of G is a subgroup, the only group properties we really have to check are closure and inverses. We now are ready to state (and prove) one of the simplest and most fundamental facts about groups.

Theorem 2 (Lagrange's Theorem)**.** *Suppose $|G|$ is finite, and H is a subgroup of G. Then $|H|$ divides $|G|$.*

For example, take for G the multiplicative group Z_7^* with 6 elements, and consider H to be subgroup consisting of all the distinct powers of 2, that is $2, 2^1 = 2, 2^2 = 4, 2^3 = 1 \bmod 7$.

H is a subgroup (since it is closed and every element has an inverse), and the order of H is 3 which divides the order of G (equal to 6).

Proof. Suppose H has h elements. We will partition the elements of G into disjoint 'copies' of H. Each such copy will be of the form xH, where x is an element of G and $xH = \{xy : y \in H\}$ denotes the h elements obtained by multiplying x by each element of H. (In the example above, $3H$ corresponds to $\{3 \cdot 1, 3 \cdot 2, 3 \cdot 4\} = \{3, 6, 5\}$.)

Suppose we have already identified $x_1, \cdots, x_j$ such that all $x_k H$ are disjoint for $k = 1, \cdots, j$. So far, these sets cover precisely jh distinct elements of G. To initialize this process, we set $x_1 = e$ and $j = 1$. Now, either we have all elements of G or we don't. In the first case, we know that $|G| = j|H|$ and we are done. In the second case, let x_{j+1} be an element of G which is not of the form $x_k q$ for $k \leq j$ and some q in H.

We now add to our list the h additional elements $x_{j+1}H$ of G. We prove that these elements are all new and distinct: if $x_{j+1}h_1 = x_{j+1}h_2$ holds then by multiplying on the left of both sides of this equation by x_{j+1}^{-1} we find that h_1 and h_2 are equal; if $x_k g = x_{j+1}h$ holds for some g and h in H and $k \leq j$, then upon postmultiplying both sides of this equation by h^{-1} we get

$$x_k g h^{-1} = x_{j+1}$$

and therefore $x_{j+1} \in x_k H$ (since $gh^{-1} \in H$ by closure and the existence of inverse), a contradiction. We then increase j by 1 and repeat. If G is finite, this argument must come to an end which can only happen when the order of G is jh for some j. □

The h elements of G of the form xH listed at each step in the argument here form what is called a left *coset* of the subgroup H; a right coset is similarly defined as Hx. If the right and left cosets for each element are the same so that for all a in G we have $aH = Ha$, then H is said to be *normal*. In Abelian groups, all subgroups are normal.

If H is a normal subgroup of G, then its cosets form a group under the rule of composition $aHbH = abH$; this subgroup is called the *factor group* G/H of G with respect to H. For example, if G is the group Z of integers under addition, and H is the subgroup consisting of those integers divisible by n (which we denote by nZ), then the factor group has elements which correspond to the remainders upon dividing integers by n. This is called, as we remarked earlier, Z_n, and is often referred to as the *integers mod* n.

Those integers that have any one specific remainder r upon dividing by n (the coset of Z with respect to nZ corresponding to the remainder r) are said to form the class (or coset) of integers *congruent to* r mod n. These are of course the integers that differ from one another by multiples of n. We often say that any two such integers are congruent to one another modulo n, which we denote as $a \equiv b \bmod n$ or often simply as $a = b \bmod n$.

Let x be an element of a finite group G. The powers of x form a subgroup of G called the group *generated by* x, and we define the *order* of an element x to be the order of that subgroup. One can see that the order of x is the smallest positive power k such that $x^k = 1$ (if there were two indices j, l with $j < l \neq k$ and $x^j = x^l$ then $x^{l-j} = 1$ contradicting the definition of k). Hence for all $x \in G$, we must have $x^{o(x)} = 1$. If we apply Lagrange's theorem to G and $x \in G$, then we see that $o(x)$ divides the order $|G|$ of G, and therefore $x^{o(x)} = 1$ implies that $x^{|G|} = 1$ for all $x \in G$. In particular, if we take $G = Z_p^*$ with p prime, we get Fermat's little theorem (since the order of Z_p^* is $p - 1$):
Theorem 3 (Fermat's little theorem)**.** *If p is prime and a is not divisible by p then $a^{p-1} = 1 \bmod p$.*

Also, if we take $G = Z_N^*$ with $N = pq$, p and q being prime, we get that $|G| = (p-1)(q-1)$ and thus $x^{(p-1)(q-1)} = 1$ for all x relatively prime with pq.

2 The Chinese Remainder Theorem

This theorem was discovered by the Chinese mathematician Sun Tzu in the 4-th century AD and written in his book the Sun Tzu Suan Ching. It says the following. If a and b are relatively prime (they contain no common factors except 1), then there is a bijection between the possible remainders modab and the pairs of possible remainders mod$a$ and mod$b$. In other words, the two numbers (the remainder of x upon dividing by a and the remainder of x upon dividing by b) uniquely determines the number x upon dividing by ab, and vice versa. Let's look at an example. Let $a = 7$ and $b = 13$, then $ab = 91$. Any arbitrary remainder, say 73 mod 91, is equivalent to the pair $(3, 8) = (73 \bmod 7, 73 \bmod 13)$. No other remainder mod 91 leads to the pair $(3, 8)$.
Theorem 4 (Chinese Remainder Theorem)**.** *Let a and b be integers that are relatively prime. Each pair of remainders (r, s) mod a and b separately corresponds to exactly one remainder t mod ab such that $t \equiv r \bmod a$ and $t \equiv s \bmod b$. If one adds or multiplies remainders with respect to ab, the corresponding remainders with respect to a and b separately add or multiply correspondingly.*

Proof. In order to show this, first note that the number of possible remainders modab is ab, while the number of pairs of possible remainders mod$a$ and mod$b$ is also ab. To any remainder t mod ab, there corresponds a pair $(t \bmod a, t \bmod b)$ of remainders mod$a$ and mod$b$. So we only need to show that there cannot exist two distinct remainders x and y upon dividing by ab, and that x and y have the same remainders upon dividing by a and by b. Then a divides the difference $x - y$, and b also divides xiy. Since we assumed that a and b are relatively prime, we have ab divides $x - y$. This implies that x and y have the same

remainder upon dividing by ab and are therefore equal. This is a contradiction. Thus, each remainder of ab corresponds to a unique pair of remainders for a and b separately. $\square$

We can now describe remainders with respect to ab by the corresponding pairs of remainders with respect to a and b separately: we let (s,t) represent the remainder that is s with respect to a and t with respect to b. Observe, that the fundamental theorem of algebra fails here (remainders mod ab are not a field, so a qth degree polynomial can have more than q roots.) Thus, the equation $x^2 = 1 \bmod ab$ has four solutions: the remainder pairs $(1,1), (-1,1), (1,-1), (-1,-1)$. (Here, $(-1,1)$ is a convenient notatiopn for $(a-1,1)$.) Why are these all solutions to $x^2 = 1 \bmod ab$? For any $x \in \{(1,1), (-1,1), (1,-1), (1,1)\}$, we have that x^2 gets represented by $((\pm 1)^2, (\pm 1)^2) = (1,1)$ and, by the Chinese remainder theorem, the only remainder $\bmod(ab)$ that corresponds to this is 1.

For example, consider $a = 3$ and $b = 5$. The remainders $r = 1$, 4, 11, and 14 are relatively prime to $ab = 15$, and correspond to the remainder pairs $(1,1)$, $(1,-1) = (1,4)$, $(-1,1) = (2,1)$ and $(-1,-1) = (2,4)$ respectively. In each case, $r \equiv \pm 1 \bmod 3$ and $r \equiv \pm 1 \bmod 5$ so that $r^2 \equiv (\pm 1)^2 = 1 \bmod 3$ and $r^2 \equiv (\pm 1)^2 = 1 \bmod 5$, so that $r^2 \equiv 1 \bmod 15$. And indeed $1^2 = 1$, $4^2 = 16$, $11^2 = 121$, and $14^2 = 196$ are all $\equiv 1 \bmod 15$.

3 Euclid's Algorithm

Euclid's algorithm (or the Euclidean algorithm) is a very efficient and ancient algorithm to find the greatest common divisor $\gcd(a,b)$ of two integers a and b. It is based on the following observations. First, $\gcd(a,b) = \gcd(b,a)$, and so we can assume that $a \geq b$. Secondly $\gcd(a,0) = a$ by definition. Thirdly and most importantly, if

$$a = zb + c$$

then $\gcd(a,b) = gcd(b,c)$. Indeed any divisor of a and b will divide c, and conversely any divisor of b and c will divide a. We can compute c by taking the remainder after dividing a by b, i.e. $a = c \bmod b$. But $c < b < a$ and thus we have made progress by reducing the numbers we have to compute their gcd of. And therefore, we can proceed and express b as:

$$b = yc + d,$$

(thus $b = d \bmod c$) and thus $\gcd(b,c) = \gcd(c,d)$. We continue until we express $\gcd(a,b)$ as $\gcd(g,0) = g$, and at that point, we have found the gcd.

Example. Let $a = 365$ and $b = 211$. Then $c = 154$ and we have that $\gcd(365, 211) = \gcd(211, 154)$. Continuing, we get:

$$\begin{aligned}
\gcd(365, 211) &= \gcd(211, 154) \\
&= \gcd(154, 57) \\
&= \gcd(57, 40) \\
&= \gcd(40, 17) \\
&= \gcd(17, 6) \\
&= \gcd(6, 5) \\
&= \gcd(5, 1) \\
&= \gcd(1, 0) \\
&= 1.
\end{aligned}$$

For example, 40 was found by taking 154 mod 57. The gcd of 365 and 211 is 1, which means that they are relatively prime.

Euclid's algorithm also allows to find integers s and t such that $\gcd(a, b) = sa + tb$. This clearly proves that no common divisor to a and b is greater than $\gcd(a, b)$ since any common divisor to a and b is also a divisor to $sa+tb$. To find s and t, we proceed bottom up. Suppose we have found u and v such that

$$\gcd(b, c) = ub + vc.$$

Then, knowing that $a = zb + c$ allows us to replace c by $a - zb$ and therefore get:

$$\gcd(a, b) = \gcd(b, c) = ub + v(a - zb) = va + (u - vz)b.$$

Thus, we have expressed the gcd as an integer combination of a and b, knowing it as an integer combination of b and c. Thus bottom up we can find s and t such that

$$\gcd(a, b) = sa + tb.$$

This procedure is often referred to as the *extended Euclidean algorithm.*

Example. Consider again the example with $a = 365$ and $b = 211$. We express their $\gcd(365, 211) = 1$ by going bottom up in the derivation above, and derive:

$$\begin{aligned}
1 &= 6 - 5 \\
&= 6 - (17 - 2 \cdot 6) = -17 + 3 \cdot 6 \\
&= -17 + 3 \cdot (40 - 2 \cdot 17) = -7 \cdot 17 + 3 \cdot 40 \\
&= 3 \cdot 40 - 7 \cdot (57 - 40) = 10 \cdot 40 - 7 \cdot 57 \\
&= 10 \cdot (154 - 2 \cdot 57) - 7 \cdot 57 = 10 \cdot 154 - 27 \cdot 57 \\
&= 10 \cdot 154 - 27 \cdot (211 - 154) = 37 \cdot 154 - 27 \cdot 211 \\
&= 37 \cdot (365 - 211) - 27 \cdot 211 = 37 \cdot 365 - 64 \cdot 211
\end{aligned}$$

Multiplicative inverses. Given two relatively prime numbers, this procedure allows us to find a multiple of one that differs from a multiple of the other by 1. This has a really neat use. We can find the multiplicative inverse of b mod a if a and b are relatively prime (if not, the multiplicative inverse does not exist). Since $\gcd(a, b) = 1$, the extended Euclidean algorithm gives us s and t such that $sa + tb = 1$. Taking mod a on both sides, we get that $t = b^{-1} \bmod a$.

Chinese remainder theorem. Multiplicative inverses in turn allow us to find the correspondence in the Chinese remainder theorem. Suppose a and b are relatively prime (thus $\gcd(a, b) = 1$). Suppose we know that $x = i \bmod a$ and $x = j \bmod b$ and we would like to find $x \bmod ab$. Express x as $x = kb + j$ for some integer k; we can assume that $0 \leq k < a$. Taking mod a on both sides, we get $i \equiv kb + j \bmod a$ and thus $k \equiv b^{-1}(i - j) \bmod a$. We have just seen how to calculate $b^{-1} \bmod a$ and thus we can find k, and then x.