Modular Arithmetic and Elementary Algebra

Lecturer: Michel Goemans

These notes cover basic notions in algebra which will be needed for discussing several topics of this course. In particular, we will need them to describe the RSA cryptosystem, the primality testing algorithms, and for the material on error-correcting codes that we will be covering later in this course.

1 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

$$a = zb + c$$

where z is an integer 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. c is $a \bmod b$. (We will discuss the mod operation in greater details in the next section, but at this point, we only need the definition of c as the remainder of dividing a by 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 $d = b \bmod c$) 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*.

We now state an easy consequence of Euclid's algorithm

Lemma 1. *For any positive integers, there exist integers s and t such that* $\gcd(a,b) = sa + tb$.

Indeed, Euclid's algorithm also allows to find such integers s and t. 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:

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

There is another way to implement the extended Euclidean algorithm, which is a little easier to do on a spreadsheet. If you are finding $\gcd(a,b) = \gcd(a_0, a_1)$ and, after i steps, you have reduced to it to the calculation of $\gcd(a_i, a_{i+1})$ with $a_i \geq a_{i+1}$, you can keep track of two numbers x_i and y_i such that $x_i a + y_i b$ equals a_i. Initially, $x_0 = 1$ and $y_0 = 0$, as $a_0 = 1a + 0b$. To find x_i and y_i, we know that

$$a_{i-2} = x_{i-2}a + y_{i-2}b$$

and

$$a_{i-1} = x_{i-1}a + y_{i-1}b.$$

As $a_i = a_{i-2} - qa_{i-1}$ where q is the integer part of the quotient between a_{i-2} and a_{i-1}, we simply let $x_i = x_{i-2} - qx_{i-1}$ and $y_i = y_{i-2} - qy_{i-1}$. Indeed, we have:

$$\begin{array}{rcl}
x_i a + y_i b &=& (x_{i-2} - qx_{i-1})a + (y_{i-2} - qy_{i-1})b \\
&=& a_{i-2} - qa_{i-1} \\
&=& a_i.
\end{array}$$

For example, we have

gcd	x	y
$\gcd(365, 211)$	1	0
$\gcd(211, 154)$	0	1
$\gcd(154, 57)$	1	-1
$\gcd(57, 40)$	-1	2
$\gcd(40, 17)$	3	-5
$\gcd(17, 6)$	-4	7
$\gcd(6, 5)$	11	-19
$\gcd(5, 1)$	-26	45
$\gcd(1, 0)$	37	-64

Here we found that $6 = 11 * 365 - 19 * 211$ by subtracting twice the equation $17 = -4 \cdot 365 + 7 * 211$ from $40 = 3 * 365 - 5 * 211$.

2 Modular Arithmetic

We will now consider algebraic structures. Before going into the general definitions, we introduce a very important example called *modular arithmetic*, which is one of the most intuitive examples of algebraic structures. In fact, this is the example we shall need for the RSA cryptosystem.

First an easy definition: for integers a, b, m we say that

$$a \equiv b \pmod{m}$$

if $a - b$ is a multiple of m. That is, if

$$a - b = im$$

for some integer $i \in \mathbb{Z}$. Here, "mod" is short for "modulo".

For any integer $n \in \mathbb{Z}$ there is a unique integer r in $\{0, 1, \ldots, m-1\}$ such that $n \equiv r \bmod m$. Then r is called the *residue* of n modulo m, and by slight abuse of notation we will refer to it as $n \bmod m$. One can find the residue of a number n by taking the remainder when dividing by m. Although we will often us them interchangeably, there is a slight difference between $a = n \bmod m$ and $a \equiv n \pmod{m}$; in the former case, a is the residue and thus between 0 and $m - 1$. In later notes, however, we typically simply write $a = n \pmod{m}$ and the interpretation is usually clear.

We can then define binary operations $\oplus, \otimes$ on the set $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ as follows. For $a, b \in \mathbb{Z}_m$ we define $a \oplus b$ to be the residue of $(a + b)$ modulo m. Similarly, we define $a \otimes b$ to be the residue of $(a \times b)$ modulo m.

Example. In $\mathbb{Z}_5$, one has $3 \oplus 4 = 2$ and $3 \otimes 4 = 2$.

For $a \in \mathbb{Z}_m$, we denote $\ominus a$ the residue of $-a$ modulo m. Here are a few very easy facts that the reader is invited to check. If $a \in \mathbb{Z}_m$ and $d = \ominus a$ then

$$a \oplus 0 = 0 \oplus a = a,$$

and

$$a \oplus d = d \oplus a = 0.$$

Moreover, for all $a, b, c \in \mathbb{Z}_m$,

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

In the next section we will define groups and see that the above relation are precisely the conditions showing that $(\mathbb{Z}_m, \oplus)$ is a group. If we consider the operation $\otimes$, the role of 0 for $\oplus$ is now played by 1 since $a \otimes 1 = 1 \otimes a = a$. 1 is the multiplicative identity, in the same way as 0 was the additive identity. However 0 never has a multiplicative inverse (in the same way as $\ominus a$ is playing the role of the additive inverse); the *multiplicative inverse* of an element a is defined as an element b such that $b \otimes a = 1$. Even if we exclude 0 and consider $\mathbb{Z}_m - \{0\}$, we will see that some nonzero elements may not have a multiplicate inverse. However, when m is a prime number, we will see that $(\mathbb{Z}_m - \{0\}, \otimes)$ is a group

Considering the general notion of group allows one to prove theorems that are valid for *all* groups, instead of doing a proof for each individual example. For instance we will prove Fermat's Little Theorem using general results about groups.

3 Groups

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

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

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

(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*.

Examples:
• The set 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 $-a$.
• The integers under multiplication, $(\mathbb{Z}, *)$, is not a group since the integers $a \neq 1, -1$ don't have an inverse.
• 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.
• Let Gl_n be the set of invertible $n \times n$ matrices with the usual matrix product as operation. Then $(Gl_n, *)$ is a group (with identity the identity matrix) which is not Abelian (as matrix multiplication is not commutative in general).

• 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 $-p(x)$.

In the previous section we have checked that for any integer m the set $(\mathbb{Z}_m, \oplus)$ is a group, with identity element 0. The additive inverse of an element $a \neq 0$ is $\ominus a = m - a$. Now we consider the more interesting question: for which integer m does $(\mathbb{Z}_m - \{0\}, \otimes)$ is a group? First of all closure and associativity are clear, and 1 is the identity. So the question is to know whether every element has a (multiplicative) inverse. First observe that 0 cannot have a multiplicative inverse (indeed $b \otimes 0 = 0 \neq 1$ for all $b \in \mathbb{Z}_m$) and that's why we excluded it from the start. Now suppose $a \in \mathbb{Z}_m$ is relatively prime with m. In this case, we know by Euclid's algorithm that there exist integers s, t such that

$$as + mt = \gcd(a, m) = 1.$$

Thus $1 = as \bmod m$. Hence taking $r \in \mathbb{Z}_m$ the residue of s modulo m one gets $a \otimes r = 1$. We have just proved that the elements $a \in \mathbb{Z}_m - \{0\}$ which are relatively prime with m have a multiplicative inverse. Thus *if m is a prime number*, every element in $\mathbb{Z}_m - \{0\}$ has a multiplicative inverse so that $(\mathbb{Z}_m - \{0\}, \otimes)$ is a group.

Now if m is not a prime. Consider an element $a \in \mathbb{Z}_m - \{0\}$ which is not relatively prime with m. Let $d = \gcd(a, m) \neq 1$. This means that, for any b, ab is an integer multiple of d and thus cannot give a residue of 1 modulo m. Thus a cannot have a multiplicative inverse. So the elements not prime with m have no inverse in $(\mathbb{Z}_m, \otimes)$. But we can still salvage a multiplicative group as we show now.

For any integer m we denote by $\mathbb{Z}_m^*$ the remainders that are relatively prime to m. For instance if m is prime then $\mathbb{Z}_m^* = \mathbb{Z}_m - \{0\}$ while for $m = 15$ one gets $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. The product of any two element relatively prime to m is still relatively prime to m, and every element has an inverse so it is easy to see that $(\mathbb{Z}_m^*, \otimes)$ is a group.

4 Subgroups and cosets

The number of elements in a group G is called the *order* of G, written $|G|$.

Example. The order of $(Z_N, \oplus)$ is N. The order of $(\mathbb{Z}_N^*, \otimes)$ is the number of remainders which are relatively prime to N. If N is a prime then $\mathbb{Z}_N^* = \mathbb{Z}_N - \{0\}$ and the order in $N - 1$. Now consider the situation where $N = pq$, where p and q are primes. In this case the order of $(\mathbb{Z}_N^*, \otimes)$ 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 $\mathbb{Z}_N^*$ is $(N-1) - ((p-1) + (q-1)) = N - p - q + 1$. For example, for $N = 15$, we have that the order of $\mathbb{Z}_{15}^*$ 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 1 (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 $\mathbb{Z}_7^*$ 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 (i.e. performing the group operation) x by each element of H. (In the example above, $3H$ corresponds to $\{3 \otimes 1, 3 \otimes 2, 3 \otimes 4\} = \{3, 6, 5\}$ where $\otimes$ corresponds to multiplication in $\mathbb{Z}_7^*$.)

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 $x_1 = e$ (where e is the identity element) 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. □

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 $x^k = 1$ (indeed if there were two indices j, l with $j < l \leq k$ and $x^j = x^l$, then $x^{l-j} = 1$ contradicting the definition of k). Hence for all $x \in G$, we must have $x^{o(x)} = 1$, where $o(x)$ denote the order of x. 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 $G = \mathbb{Z}_p^*$ with p prime, we get Fermat's little theorem (since the order of $\mathbb{Z}_p^*$ is $p - 1$):

Theorem 2 (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 $G = \mathbb{Z}_N^*$ 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.

Cosets of normal subgroups.
Let G be a group and H be a subgroup with h elements. For any group element $x \in G$, the h

elements of G of the form xH 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 $\mathbb{Z}$ of integers under addition, and H is the subgroup consisting of those integers divisible by n (which we denote by $n\mathbb{Z}$), then the factor group has elements which correspond to the remainders upon dividing integers by n. This is called, as we remarked earlier, $\mathbb{Z}_n$, and is often referred to as the *integers mod n*. Thus $\mathbb{Z}_n$ can be seen as the factor group $\mathbb{Z}/n\mathbb{Z}$ of the group $(\mathbb{Z}, +)$.

5 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 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 3 (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 $r = t \bmod a$ and $s = t \bmod b$.*

Moreover, 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 $\bmod a$ and $\bmod b$ 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. Suppose the contrary. In this case, both a and b divide the difference $x - y$. Since we assumed that a and b are relatively prime, it implies that 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. This proves the first statement of the theorem. The second statement is easy to check and is left to the reader. □

By the above theorem, 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.

Now suppose that we want to find the remainder modulo ab that correspond to the pair (s, t). Let $x \in \{0, 1, \ldots, ab - 1\}$ be this remainder. We know that $s = x \bmod a$ and $t = x \bmod b$. In particular, $x = kb + t$ where $0 \leq k < a$. Moreover $s \equiv kb + t \pmod a$, hence $kb \equiv s - t \pmod a$. Now recall that b has a multiplicative inverse in the group $(\mathbb{Z}_a^*, \otimes)$, and that this inverse can be

found using Euclid's algorithm. Using this inverse we can compute $k = b^{-1}(s-t) \bmod a$, and then compute $x = kb + t$.

Now let us play a little bit with the remainder pairs representations. Let us try for instance to find the solutions of the equation $x^2 = 1 \bmod ab$ where a and b are relatively prime. Since the remainder 1 mod ab is represented by the remainder pair $(1,1)$ (where the pair represents the values modulo a and b), it is easy to see that this equation has four solutions: the remainder pairs $(1,1),(-1,1),(1,-1),(-1,-1)$. (Here, $(-1,1)$ is a convenient notation 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, $r \equiv \pm 1 \pmod 3$ and $r \equiv \pm 1 \pmod 5$ so that $r^2 \equiv (\pm 1)^2 \equiv 1 \pmod 3$ and $r^2 \equiv (\pm 1)^2 \equiv 1 \pmod 5$, so that $r^2 \equiv 1 \pmod{15}$. And indeed $1^2 = 1$, $4^2 = 16$, $11^2 = 121$, and $14^2 = 196$ are all $\equiv 1 \bmod 15$.

6 Fields and algebraic equations

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

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

From our previous discussion on $\mathbb{Z}_m$ it is easy to see that if $(\mathbb{Z}_m,\oplus,\otimes)$ is a field if and only if m is a prime. The rationals, real or complex numbers (with usual addition and multiplication) are also fields.

Fields have the important property that the product of any two non-zero elements is not zero.

Lemma 2. *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 3. *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 $r = 0$. □

We can now prove the fundamental theorem of algebra.

Theorem 4. *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 $p(x)$ be a polynomial of degree $d > 1$, and let $x = a$ be one of its roots. By lemma 3, we have $p(x) = (x - a)q(x)$, where $q(x)$ is a polynomial of degree $d - 1$, and by the induction hypothesis, $q(x)$ has at most $d - 1$ roots. Lemma 2 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. □

18.310 Principles of Discrete Applied Mathematics
Fall 2013