

MATH 433  
Applied Algebra

**Lecture 37:**  
**Review for the final exam.**

## Topics for the final exam: Part I

- Mathematical induction, strong induction
- Greatest common divisor, Euclidean algorithm
- Primes, factorisation, Unique Factorisation Theorem
- Congruence classes, modular arithmetic
- Inverse of a congruence class
- Linear congruences
- Chinese Remainder Theorem
- Order of a congruence class
- Fermat's Little Theorem, Euler's Theorem
- Euler's phi-function
- Public key encryption, the RSA system

## Topics for the final exam: Part II

- Relations, properties of relations
- Finite state machines, automata
  
- Permutations
- Cycles, transpositions
- Cycle decomposition of a permutation
- Order of a permutation
- Sign of a permutation
- Symmetric and alternating groups
  
- Abstract groups (definition and examples)
- Semigroups
- Rings, zero-divisors
- Fields, characteristic of a field
- Vector spaces over a field

## Topics for the final exam: Part III

- Order of an element in a group
- Subgroups
- Cyclic groups
- Cosets
- Lagrange's Theorem
- Isomorphism of groups
  
- The ISBN code
- Binary codes, error detection and error correction
- Linear codes, generator matrix
- Coset leaders, coset decoding table
- Parity-check matrix, syndromes
  
- Division of polynomials
- Greatest common divisor of polynomials
- Factorisation of polynomials

**Problem.** Solve the equation

$$2x^{100} + x^{71} + x^{29} = 0 \text{ over the field } \mathbb{Z}_{11}.$$

The equation is equivalent to

$$x^{29}(2x^{71} + x^{42} + 1) = 0.$$

Hence  $x = 0$  or  $2x^{71} + x^{42} + 1 = 0$ . By Fermat's Little Theorem,  $x^{10} = 1$  for any nonzero  $x \in \mathbb{Z}_{11}$ .

Since 0 is not a solution of the equation

$$2x^{71} + x^{42} + 1 = 0, \text{ this equation is equivalent to} \\ 2x + x^2 + 1 = 0 \iff (x + 1)^2 = 0 \iff x = -1.$$

Thus the solutions are  $x = 0$  and  $x = 10$   
(note that  $-1 \equiv 10 \pmod{11}$ ).

**Problem.** Factorise  $p(x) = x^4 + x^3 - 2x^2 + 3x - 1$  into irreducible factors over the field  $\mathbb{Q}$ .

Possible rational zeros of  $p$  are 1 and  $-1$ . They are not zeros. Hence  $p$  is either irreducible over  $\mathbb{Q}$  or else it is factored as

$$x^4 + x^3 - 2x^2 + 3x - 1 = (ax^2 + bx + c)(a'x^2 + b'x + c').$$

Since  $p \in \mathbb{Z}[x]$ , one can show that the factorisation (if it exists) can be chosen so that all coefficients are integer.

Additionally, we can assume that  $a \geq 0$  (otherwise we could multiply each factor by  $-1$ ). Equating the corresponding

coefficients of the left-hand side and the right-hand side, we obtain  $aa' = 1$ ,  $ab' + a'b = 1$ ,  $ac' + bb' + a'c = -2$ ,

$bc' + b'c = 3$  and  $cc' = -1$ . The first and the last equations imply that  $a = a' = 1$ ,  $c = 1$  or  $-1$ , and  $c' = -c$ . Then

$b + b' = 1$  and  $bb' = -2$ , which implies  $\{b, b'\} = \{2, -1\}$ .

Finally,  $c = -1$  if  $b = 2$  and  $c = 1$  if  $b = -1$ . We can check that indeed

$$x^4 + x^3 - 2x^2 + 3x - 1 = (x^2 + 2x - 1)(x^2 - x + 1).$$

**Problem.** The polynomial  $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$  has how many distinct complex roots?

Let  $p \in \mathbb{C}[x]$  be a nonzero polynomial. We say that  $\alpha \in \mathbb{C}$  is a root of  $p$  of multiplicity  $k \geq 1$  if the polynomial is divisible by  $(x - \alpha)^k$  but not divisible by  $(x - \alpha)^{k+1}$ .

Equivalently,  $p(x) = (x - \alpha)^k q(x)$  for some polynomial  $q$  such that  $q(\alpha) \neq 0$ . If this is the case then

$$\begin{aligned} p'(x) &= ((x - \alpha)^k)' q(x) + (x - \alpha)^k q'(x) \\ &= k(x - \alpha)^{k-1} q(x) + (x - \alpha)^k q'(x) = (x - \alpha)^{k-1} r(x), \end{aligned}$$

where  $r(x) = kq(x) + (x - \alpha)q'(x)$ . Note that  $r(x)$  is a polynomial and  $r(\alpha) = kq(\alpha) \neq 0$ . Hence  $\alpha$  is a root of  $p'$  of multiplicity  $k - 1$  if  $k > 1$  and not a root of  $p'$  if  $k = 1$ .

**Problem.** The polynomial  $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$  has how many distinct complex roots?

By the Fundamental Theorem of Algebra, any polynomial  $p \in \mathbb{C}[x]$  of degree  $n \geq 1$  can be represented as

$$p(x) = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

where  $c, \alpha_1, \dots, \alpha_n \in \mathbb{C}$  and  $c \neq 0$ . The numbers  $\alpha_1, \alpha_2, \dots, \alpha_n$  are roots of  $p$ , they need not be distinct. We have

$$p(x) = c(x - \beta_1)^{k_1}(x - \beta_2)^{k_2} \dots (x - \beta_m)^{k_m},$$

where  $\beta_1, \dots, \beta_m$  are distinct roots of  $p$  and  $k_1, \dots, k_m$  are their multiplicities. It follows from the above that

$$\gcd(p(x), p'(x)) = (x - \beta_1)^{k_1-1}(x - \beta_2)^{k_2-1} \dots (x - \beta_m)^{k_m-1}.$$

As a consequence, the number of distinct roots of the polynomial  $p$  equals  $\deg(p) - \deg(\gcd(p, p'))$ .



**Problem.** The polynomial  $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$  has how many distinct complex roots?

Let's use the Euclidean algorithm to find the greatest common divisor of the polynomials  $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$  and  $f'(x) = 6x^5 + 15x^4 - 15x^2 + 3$ . First we divide  $f$  by  $f'$ :

$$x^6 + 3x^5 - 5x^3 + 3x - 1 = (6x^5 + 15x^4 - 15x^2 + 3)\left(\frac{1}{6}x + \frac{1}{12}\right) + r(x),$$

where  $r(x) = -\frac{5}{4}x^4 - \frac{5}{2}x^3 + \frac{5}{4}x^2 + \frac{5}{2}x - \frac{5}{4}$ . It is convenient to replace the remainder  $r(x)$  by its scalar multiple

$\tilde{r}(x) = -\frac{4}{5}r(x) = x^4 + 2x^3 - x^2 - 2x + 1$ . Next we divide  $f'$  by  $\tilde{r}$ :

$$6x^5 + 15x^4 - 15x^2 + 3 = (x^4 + 2x^3 - x^2 - 2x + 1)(6x + 3).$$

Since  $f'$  is divisible by  $\tilde{r}$ , it follows that  $\gcd(f, f') = \gcd(f', r) = \gcd(f', \tilde{r}) = \tilde{r}$ . Thus the number of distinct complex roots of the polynomial  $f$  equals  $\deg(f) - \deg(\gcd(f, f')) = 6 - 4 = 2$ .

**Problem.** The polynomial  $f(x) = x^6 + 3x^5 - 5x^3 + 3x - 1$  has how many distinct complex roots?

As a follow-up to the solution, we can find the roots of the polynomial  $f$ . It follows from the solution that the polynomial  $g = f / \gcd(f, f')$  has the same roots as  $f$  but, unlike  $f$ , all roots of  $g$  are simple (i.e., of multiplicity 1). Dividing  $f$  by  $\tilde{r}(x) = x^4 + 2x^3 - x^2 - 2x + 1$ , we obtain

$$x^6 + 3x^5 - 5x^3 + 3x - 1 = (x^4 + 2x^3 - x^2 - 2x + 1)(x^2 + x - 1).$$

The polynomial  $g(x) = x^2 + x - 1$  has two real roots  $\beta_{1,2} = \frac{1}{2}(-1 \pm \sqrt{5})$ . Therefore  $f(x) = (x - \beta_1)^{k_1}(x - \beta_2)^{k_2}$ , where  $k_1$  and  $k_2$  are positive integers,  $k_1 + k_2 = 6$ . Note that  $\beta_1\beta_2 = -1$  (the constant term of  $g$ ) and  $\beta_1^{k_1}\beta_2^{k_2} = -1$  (the constant term of  $f$ ). Then  $\beta_1^{k_1-k_2} = (-1)^{k_2+1}$ , a rational number. This suggests  $k_1 - k_2 = 0$  (so that  $k_1 = k_2 = 3$ ). We can check by direct multiplication that, indeed,

$$x^6 + 3x^5 - 5x^3 + 3x - 1 = (x^2 + x - 1)^3 = (x - \beta_1)^3(x - \beta_2)^3.$$