

Due Thursday, Sept. 8, 2011.

Let us set the following notation:

- \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{R}_+ , \mathbb{R}_+^n , and \mathbb{C} respectively denote the positive integers, the integers, the rationals, the real numbers, the positive real numbers, the positive orthant (or **positive quadrant** when $n=2$), and the complex numbers.
- For any set S we denote its cardinality by $\#S$. (When S is finite, cardinality just means number of elements.)
- For any ring R , we let $R^* := R \setminus \{0\}$.
- For integers a and b writing $a|b$ simply means that a divides b .
- We'll frequently use **iff** or \iff as shorthand for "if and only if".

Problems

1: Recall De Moivre's formula: $e^{it} = \cos(t) + i \sin(t)$, where e is the natural log base, $i^2 = -1$, and $t \in \mathbb{R}$.

(a) Please give an explicit formula for all the complex roots of $x^d = c$, where $d \in \mathbb{Z}$ and $c \in \mathbb{C}$. Please make sure to include the cases where $d=0$ or $c=0$.

(b) Consider the line segment connecting the points $(0, -\log|c|)$ and $(d, 0)$. Please interpret the absolute values of the roots of $x^d = c$ in terms of the slope of this line segment.

2: Suppose now that $d \in \mathbb{Z}$ and $c \in \mathbb{R}$.

(a) Please find precise conditions on (c, d) under which $x^d = c$ has a *positive* root.

(b) Please find precise conditions on (c, d) under which $x^d = c$ has a *real* root.

3: Let $p \in \mathbb{N}$ be any prime and define \mathbb{F}_p — the finite field with p elements — to be $\mathbb{Z}/p\mathbb{Z}$, i.e., the integers mod p . Please find precise conditions on those (c, d) such that $x^d = c$ has a root in \mathbb{F}_p . Can your condition be checked in time polynomial in $\log(c) + \log(d)$?

Hint: If you remember the following 3 facts then this problem is not so bad:

Fermat's Little Theorem: $x \in \mathbb{F}_p^* \implies x^{p-1} = 1$.

Lagrange's Theorem: H a subgroup of a finite group $G \implies \#H | \#G$.

Bézout's Lemma: for any relatively prime integers a and b , there are integers r and s with $ra + sb = 1$.

4: Given any real $n \times n$ matrix $M = [m_{ij}]$ and $x \in \mathbb{R}_+^n$, let us define

$$x^M := (x_1^{m_{11}} \cdots x_n^{m_{n1}}, \dots, x_1^{m_{1n}} \cdots x_n^{m_{nn}}).$$

(a) Please prove that $x^{MB} = (x^M)^B$, for any real $n \times n$ matrix B .

(b) Please prove that $f(x) := x^M$ is invertible (as a function from \mathbb{R}_+^n to \mathbb{R}_+^n) $\iff \det M \neq 0$.

Hint: When $\det M \neq 0$ there is a very obvious choice for the inverse of f via Part (a). The harder direction is then f invertible $\implies \det M \neq 0$. A good approach is to prove the contrapositive: assume $\det M = 0$ and then prove that f must fail to be injective (which implies a failure of invertibility). In particular, when $\det M = 0$, you can use a nonzero vector in the left-null space of M to generate numerous *distinct* x with $x^M = (1, \dots, 1)$.

We usually call a substitution of the form $y := x^A$ a **monomial change of variables**.

5:

(a) Please show that if $|x| \geq 2$ and $d \in \mathbb{N}$ then $|x|^d > 1 + |x| + \dots + |x|^{d-1}$. **Hint:** Start from the identity $|x|^d - 1 = (|x| - 1) \frac{|x|^d - 1}{|x| - 1}$.

(b) Please show that if $x, a_0, \dots, a_{d-1} \in \mathbb{C}$ and $|x|^d > |a_0| + |a_1||x| + \dots + |a_{d-1}||x|^{d-1}$ then the polynomial $a_0 + a_1x + \dots + a_{d-1}x^{d-1} + x^d$ is nonzero. **Hint:** First note that by the triangle inequality, $|x^d + a_0 + a_1x + \dots + a_{d-1}x^{d-1}| \geq |x|^d - |a_0 + a_1x + \dots + a_{d-1}x^{d-1}|$.

(c) Please prove that if $f(x) := c_0 + c_1x + \dots + c_dx^d$ is a polynomial with complex coefficients and ζ is a complex root of f , then $|\zeta| < 2 \max_{0 \leq k \leq d} \left| \frac{c_{d-k}}{c_d} \right|^{1/k}$ (employing here the convention that

$1^{\frac{1}{0}} := 1$). **Hint:** Observe that for the right choice of C (depending on the c_i), you'll have $g(x) := \frac{1}{c_d C^d} f(Cx) = a_0 + a_1x + \dots + a_dx^d$ with $a_d = 1$ and $|a_i| \leq 1$ for all i . Once you've found a reasonable expression for C , can you then argue that for sufficiently large $|x|$, you'll have

$$|x|^d > 1 + |x| + \dots + |x|^{d-1} > |a_0| + |a_1||x| + \dots + |a_{d-1}||x|^{d-1}?$$

If so, then you'll have shown $g(x) \neq 0$ for the same x .

6: Please prove that, given any *finite* subset $X \subset \mathbb{R}^2$, the set $\mathbb{R}^2 \setminus X$ is path-connected. In particular, please outline your own method to build an explicit path in $\mathbb{R}^2 \setminus X$ connecting any two given points p and q . You should think of your construction as an algorithm you could actually implement.

Reading: The pdfs for the readings should have been e-mailed to you by now. If you don't have the pdfs then please let me know right away...

1. Please read Ch. 1, Ch. 3 (up and including to Sec. 3.3), and Ch. 4 (up to and including Sec. 4.4). This corresponds to Pages 1-25 of the first pdf excerpt, and Pages 11-23 of the second pdf excerpt, from [BS96].

2. Please read the pdf excerpt from [RS02].

NOTE: Please feel free to e-mail comments, questions, and/or corrections.

References

[BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms*, MIT Press, Cambridge, MA, 1996.

[RS02] Rahman, Q. I. and Schmeisser, G., *Analytic Theory of Polynomials*, London Mathematical Society Monographs 26, Oxford Science Publications, 2002.