Math 4320 — Prelim, Part I

1:25pm–2:15pm, Monday 12th March 2012

"Algebra is generous; she often gives more than is asked of her." *Jean-Baptiste le Rond D'Alembert*

This exam contains three questions. Choose ONLY TWO to answer — if you attempt more than two questions, you must indicate which two you would like to be graded. Calculators, cell phones, music players and other electronic devices are not permitted. Notes and books may not be used.

Write your name on all exam booklets. Do not hand in any scratch paper. Unless otherwise indicated, all answers should be justified.

1. (a) Suppose a and b are integers and are not both zero. Define

   - d_1 to be the greatest integer that divides both a and b, and
   - d_2 to be the least integer greater than or equal to 1 in the set $\{as + bt \mid s, t \in \mathbb{Z}\}$.

   Explain why d_2 is well defined and show that $d_1 = d_2$. (*Thus we have equivalent definitions of* $\gcd(a, b)$.)

   (b) i. A public key for RSA is pair of numbers N, s, where N is a product of two secret prime numbers p and q both congruent to 2 mod 3, and s (for the purposes of this question) is always 3. An associated private key is any number t such that $st \equiv 1 \mod (p-1)(q-1)$. Explain why if you can factorize N, then you can find t. (*You are not required to give the details of the workings of Euclid's algorithm.*)

   ii. On February 14th this year Arjen Lenstra and his coauthors released a paper in which they exposed a weakness in the implementation of RSA. They analyzed a large pool of public keys and showed that, while the public keys were all different, a significant proportion of pairs of the public keys had a common prime factor. Explain why this constitutes a weakness. Illustrate your answer with an appropriate calculation of the factorizations of 9167 and 11303, given that both are the products of two primes and they have a common prime factor.

   13 + 12 = 25 pts

2. (a) Show that permutations γ and γ' in S_n have the same cycle structure if and only if there exists $\alpha \in S_n$ such that $\gamma' = \alpha\gamma\alpha^{-1}$.

   (b) A standard deck of playing cards contains 52 cards. In a *perfect shuffle* we cut the deck in half exactly, and then riffle the two halves together, interleaving a card from the bottom half of the deck in between each pair of adjacent cards from the top half of the deck. There are two types of perfect shuffle: an *inner* shuffle and an *outer* shuffle; this question concerns the latter. In an outer shuffle the original top card stays on top, and (counting from the top) the original 27th card becomes the 2nd card, the original 2nd card becomes the 3rd card, the original 28th card becomes the 4th card, and so on. (In an inner shuffle, the original 27th card becomes the top card, the original top card becomes the 2nd card, the original 28th card becomes the 3rd card, and so on.)

   Calculate the cycle structure of a perfect outer shuffle. What is its order?

15 + (5 + 5) = 25 pts

3. Recall that a group is a set G with a binary operation $*$ and a special element e satisfying

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

   ii. $e * a = a$ for all $a \in G$,

   iii. for all $a \in G$ there exists $a' \in G$ such that $a' * a = e$.

   (a) Show carefully how it follows from the three axioms above that in a group G we have

   iii$'$. for all $a \in G$ there exists $a' \in G$ such that $a * a' = e$.

   (b) Show that there is a binary operation $*$ on the two–element set $G = \{e, g\}$ which does not yield a group, but which satisfies axioms i, ii and iii$'$.

12 + 13 = 25 pts

TRR, 3 March 2012

Math 4320 — Prelim, Part II

1:25pm–2:15pm, Wednesday 14th March 2012

"As long as algebra and geometry have been separated, their progress have been slow and their uses limited; but when these two sciences have been united, they have lent each mutual forces, and have marched together towards perfection." Joseph Louis Lagrange

This exam contains three questions. Choose ONLY TWO to answer — if you attempt more than two questions, you must indicate which two you would like to be graded. Calculators, cell phones, music players and other electronic devices are not permitted. Notes and books may not be used.

Write your name on all exam booklets. Do not hand in any scratch paper. Unless otherwise indicated, all answers should be justified.

1. Recall that $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ given by

$$R_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

is rotation through an angle θ about the origin, and $T_{\mathbf{v}} : \mathbb{R}^2 \to \mathbb{R}^2$ given by $T_{\mathbf{v}}(\mathbf{x}) = \mathbf{x} + \mathbf{v}$ is translation by the vector $\mathbf{v}$.

(a) Let $R_{\theta,\mathbf{v}}$ be the rotation of the plane through an angle θ about the point with position vector $\mathbf{v}$. Express $R_{\theta,\mathbf{v}}$ in terms of R_θ and $T_{\mathbf{v}}$.

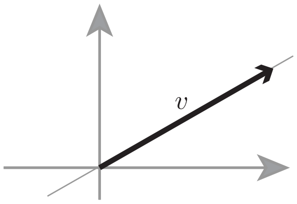
(b) Does the set $\left\{R_{\theta,\mathbf{v}} \mid \theta \in [0, 2\pi), \mathbf{v} \in \mathbb{R}^2\right\}$ form a group under composition? *Explain.*

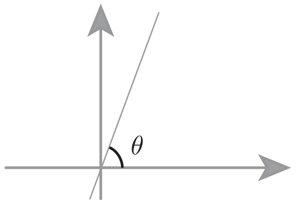
(c) Does the set of reflections of the plane form a group? *Explain.*

(d) Copy the left figure below. Draw and label two lines L_1 and L_2 on your diagram such that $T_{\mathbf{v}}$ equals reflection in L_1 followed by reflection in L_2.

(e) Copy the right figure below. Draw two lines L_1 and L_2 on your copy such that R_θ equals reflection in L_1 followed by reflection in L_2.

(f) Explain why the group $\mathrm{Isom}(\mathbb{R}^2)$ of isometries of the plane is generated by reflections. (*Hint: Use the fact that an isometry is determined by where it maps any three non–collinear points.*)





4 + 7 + 2 + 3 + 3 + 6 = 25 pts

2. (a) Explain why every permutation $\alpha \in S_n$ can be expressed as a product of transpositions. (*You may assume that every permutation can be expressed as a product of cycles.*)

(b) One definition of the parity of $\alpha \in S_n$ is that α is even (respectively, odd) when it can be expressed as a product of an even (respectively, odd) number of transpositions. Define $\text{sgn} : S_n \to \{1, -1\}$ by

$$\text{sgn}(\alpha) \;=\; \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ -1 & \text{if } \alpha \text{ is odd.} \end{cases}$$

Why might there be cause for concern about whether this is well defined? (*You are not asked to explain why it is, in fact, well defined.*)

(c) The set $\{1, -1\}$ forms a group under multiplication. Show that $\text{sgn} : S_n \to \{1, -1\}$ is a homomorphism.

(d) Show that if α and β are conjugate in S_n, then $\text{sgn}(\alpha) = \text{sgn}(\beta)$.

(e) Is the converse to part (d) true? *Explain.*

5 + 2 + 8 + 5 +5 = 25 pts

3. The Chinese Remainder Theorem gives all the integers x satisfying the simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \mod m_1, \\ &\vdots \qquad\quad \vdots \\ x &\equiv a_n \mod m_n, \end{aligned}$$

when $\gcd(m_i, m_j) = 1$ for all $i \neq j$. Specifically, if $x_i \equiv a_i \mod m_i$ and $M_i | x_i$, where $M_i = m_1 \dots m_{i-1} m_{i+1} \dots m_n$, then one solution is $x_0 := x_1 + \cdots + x_n$ and the full set of solutions is

$$S = \{x_0 + k m_1 \dots m_n \mid k \in \mathbb{Z}\}.$$

(a) i. Explain why such x_i exist.

ii. Show that x_0 is a solution to the simultaneous congruences.

iii. Show that S is the full set of solutions.

(b) An integer is *squarefree* when it is not divisible by the square of any integer other than ± 1. By applying the Chinese Remainder Theorem with $n = 1000$, with $a_i = -(i-1)$ for $1 \leq i \leq 1000$, and with $m_1, \dots, m_{1000}$ chosen appropriately, show that there exists $x \in \mathbb{Z}$ such that none of $x, x+1, x+2, \dots, x+999$ are squarefree.

(6 + 6 + 6) + 7 = 25 pts

TRR, 3 March 2012