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* $\gcd(a, b)$.)

   Answer. The set $\{a, -a, b, -b\}$ is a subset of $\{as + bt \mid s, t \in \mathbb{Z}\}$ and contains an integer greater than or equal to one since a and b are not both zero. So d_2 exists by the Least Integer Axiom.

   Take $s, t \in \mathbb{Z}$ so that $d_2 = as + bt$. By the Division Algorithm, $a = qd_2 + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < a$. But then

   $$r = a - qd_2 \;=\; a - q(as + bt) \;=\; (1 - qs)a - qbt,$$

   which must therefore be 0 by definition of d_2. So $d_2 | a$. Similarly, $d_2 | b$, and so d_2 is a common divisor of a and b.

   Now d_1, being a common divisor of a and b, must also divide $d_2 = as + bt$, and so $d_1 \leq d_2$. It follows that $d_1 = d_2$ since d_1 is the *greatest* common divisor of a and 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.*)

   Answer. Both $p - 1$ and $q - 1$, and so $(p-1)(q-1)$, are congruent to 1 mod 3, since p and q are both congruent to 2 mod 3. So $\gcd(s, (p-1)(q-1)) = 1$. So using Euclid's algorithm, we can find $t, u \in \mathbb{Z}$ such that $st + (p-1)(q-1)u = 1$. This t has the property that $st \equiv 1 \mod (p-1)(q-1)$.

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.

Answer. The reason this represents a weakness is that Euclid's algorithm can be used to find the gcd of pairs of the public keys and in a short amount of time ("polynomial time" to be more precise), and when the keys have a common factor, it will be the gcd. Long division can then be used to factor these keys.

Using Euclid's algorithm we calculate that $\gcd(9167, 11303) = 89$:

$$(9167, 11303) \to (9167, 2136) \to (623, 2136) \to (623, 267) \to (89, 267) \to (89, 0).$$

So the prime 89 divides both 9167 and 11303. Long division then gives $9167 = 89.103$ and $11303 = 89.127$.

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 $\gamma' = \alpha\gamma\alpha^{-1}$.

Answer. See Proposition 2.33 on page 118 of the textbook.

(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?

Answer. The cycle structure is:

(1) (2 3 5 9 17 33 14 27) (4 7 13 25 49 46 40 28) (6 11 21 41 30 8 15 29)
(10 19 37 22 43 34 16 31) (12 23 45 38 24 47 42 32) (18 35)
(20 39 26 51 50 48 44 36) (52).

The order is the lowest common multiple of the lengths of the cycles. The cycles here have lengths 1, 2 and 8, and so the order is 8.

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 $a * a' = e$.

Answer. See page 127 of the textbook.

(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$'$.

Answer. Define $*$ by

$$\begin{aligned} e * e &= e \\ e * g &= g \\ g * e &= e \\ g * g &= g. \end{aligned}$$

This operation does not give a group because, contrary to axiom iii, there is no $g' \in G$ such that $g' * g = e$. However it satisfies i by the calculation

$$\begin{array}{lllllllll}
(e * e) * e & = & e * e & = & e & = & e * e & = & e * (e * e) \\
(e * e) * g & = & e * g & = & g & = & e * g & = & e * (e * g) \\
(e * g) * e & = & g * e & = & e & = & e * e & = & e * (g * e) \\
(g * e) * e & = & e * e & = & e & = & g * e & = & g * (e * e) \\
(e * g) * g & = & g * g & = & g & = & e * g & = & e * (g * g) \\
(g * e) * g & = & e * g & = & g & = & g * g & = & g * (e * g) \\
(g * g) * e & = & g * e & = & e & = & g * e & = & g * (g * e) \\
(g * g) * g & = & g * g & = & g & = & g * g & = & g * (g * g),
\end{array}$$

and satisfies ii and iii$'$ self–evidently.

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 $T_{\mathbf{v}}$.

Answer. $R_{\theta,\mathbf{v}} = T_{\mathbf{v}} \circ R_\theta \circ T_{-\mathbf{v}} = T_{\mathbf{v}} \circ R_\theta \circ (T_{\mathbf{v}})^{-1}$.

(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.*

Answer. No. For example, when $\mathbf{v} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,

$$\begin{aligned} R_{\pi,\mathbf{v}} \circ R_{\pi,\mathbf{0}} \begin{pmatrix} x \\ y \end{pmatrix} &= R_{\pi,\mathbf{v}} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= R_{\pi,\mathbf{v}} \begin{pmatrix} -x \\ -y \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \left(\begin{pmatrix} -x \\ -y \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix} \end{aligned}$$

and so $R_{\pi,\mathbf{v}} \circ R_{\pi,\mathbf{0}}$ is a translation rather than a rotation. So composition is not a binary operation on the given set.

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

Answer. No. We will see in parts (d) and (e) that the product of two reflections can be a (non–trivial) translation or rotation, and so composition is not a binary operation on the set of reflections of the plane.

(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.

Answer. See below.

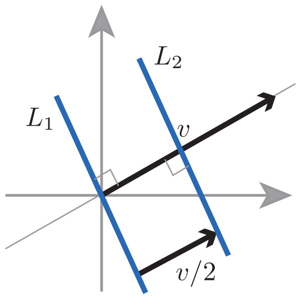
(e) Copy the right figure below. Draw two lines L_1 and L_2 on your copy such that R_θ equals reflection in L_1 followed by reflection in L_2.

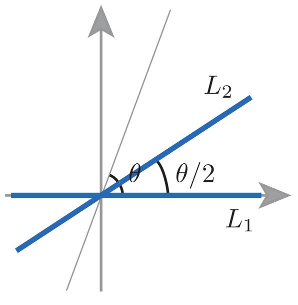
Answer. See below.

(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.*)

Answer. Suppose $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ is an isometry. Let $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ be three non–collinear points in $\mathbb{R}^2$. We will express Φ as a product of reflections by finding a sequence of reflections that take $\mathbf{x}$ to $\Phi(\mathbf{x})$, $\mathbf{y}$ to $\Phi(\mathbf{y})$, and $\mathbf{z}$ to $\Phi(\mathbf{z})$.

First carry $\mathbf{x}$ to $\Phi(\mathbf{x})$ using the translation $T_{\mathbf{v}}$ where $\mathbf{v} = \Phi(\mathbf{x}) - \mathbf{x}$ (which is a product of two reflections by part (d)). This carries $\mathbf{y}$ to the point $\mathbf{y} + \mathbf{v}$, which is the same distance from $\Phi(\mathbf{x})$ as $\mathbf{x}$ is from $\mathbf{y}$. So we can next rotate around $\Phi(\mathbf{x})$ to take $\mathbf{y} + \mathbf{v}$ to $\Phi(\mathbf{y})$. This can be achieved using reflections by parts (a), (d) and (e). Now $\mathbf{z}$ has either now been mapped to $\Phi(\mathbf{z})$, in which case we are done, or reflecting in the line through $\Phi(\mathbf{x})$ and $\Phi(\mathbf{y})$ completes its journey to $\Phi(\mathbf{z})$ (without moving $\Phi(\mathbf{x})$ and $\Phi(\mathbf{y})$).





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.*)

Answer. It is enough to show that every cycle can be expressed as a product of transpositions. Well,

$$(a_1 \;\; a_2 \; \dots \; a_r) \;=\; (a_1 \;\; a_r)(a_1 \;\; a_{r-1}) \cdots (a_1 \;\; a_3)(a_1 \;\; a_2).$$

(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 $\mathrm{sgn} : S_n \to \{1, -1\}$ by

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

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.*)

Answer. The problem is that conceivably a permutation could be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

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

Answer. We have to show that $\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$ for all $\alpha, \beta \in S_n$. Well, if α and β can be written as the product of m and n transpositions, then $\alpha\beta$ can be written as the product of $m + n$ transpositions. So if m and n are both even, then $m + n$ is even and

$$1 = \mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta) = 1^2,$$

and if m and n are both odd, then $m + n$ is even and

$$1 = \mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta) = (-1)^2,$$

and if m is even and n is odd, then $m + n$ is odd and

$$-1 = \mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta) = 1(-1),$$

and if m is odd and n is even, then $m + n$ is odd and

$$-1 = \mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta) = (-1)1.$$

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

Answer. If α and β are conjugate in S_n, then there exists $\gamma \in S_n$ such that $\gamma\alpha\gamma^{-1} = \beta$. And so as sgn is a homomorphism,

$$\begin{aligned} \operatorname{sgn}(\gamma\alpha\gamma^{-1}) &= \operatorname{sgn}(\gamma)\operatorname{sgn}(\alpha)\operatorname{sgn}(\gamma)^{-1} \\ &= \operatorname{sgn}(\alpha) \end{aligned}$$

since $\{1, -1\}$ under multiplication is abelian.

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

Answer. No, for example the identity and (1 2)(3 4) are not conjugate in S_4 (as the identity is only conjugate to itself), but both have sign 1.

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

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

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

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

$$S = \{x_0 + km_1 \dots m_n \mid k \in \mathbb{Z}\}\,.$$

(a) i. Explain why such x_i exist.

Answer. As m_i and M_i are coprime, there exist $s, t \in \mathbb{Z}$ such that $sm_i + tM_i = 1$, and so $a_i sm_i + a_i tM_i = a_i$. Take $x_i = a_i - a_i sm_i = a_i tM_i$. Then $x_i \equiv a_i \mod m_i$ and $M_i | x_i$.

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

Answer. $x_0 \equiv a_i \mod m_i$ since $x_i \equiv a_i \mod m_i$ and $x_j \equiv 0 \mod m_i$ for all $i \neq j$.

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

Answer. If $k \in \mathbb{Z}$ then $x_0 + km_1 \dots m_n$ is a solution to the simultaneous congruences since $x_0 + km_1 \dots m_n \equiv x_i \mod m_i$ for all i. And if x is a solution to the simultaneous congruences then $m_i|(x - x_0)$ for all i, and so $m_1 \dots m_n|(x - x_0)$ since $\gcd(m_1, \dots, m_n) = 1$. So $x \in S$.

(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.

Answer. Let m_i denote the square of the i–th prime number. Then $\gcd(m_i, m_j) = 1$ for all $i \neq j$ and the Chinese Remainder Theorem applies and tells us there is an integer x such that

$$\begin{array}{ll} x \equiv 0 & \mod m_1, \\ x \equiv -1 & \mod m_2, \\ \vdots & \vdots \\ x \equiv -999 & \mod m_{1000}. \end{array}$$

That is,

$$\begin{aligned} &m_1|x, \\ &m_2|(x+1), \\ &\qquad\vdots \\ &m_{1000}|(x+999). \end{aligned}$$

So none of $x, x+1, x+2, \dots, x+999$ are squarefree.

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

TRR, 3 March 2012