PLEASE HAND IN

THE FACULTY OF ARTS AND SCIENCE
University of Toronto

FINAL EXAMINATIONS, APRIL/MAY 2003

MAT 246Y1Y
Concepts in Abstract Mathematics

Examiner: Professor P. Rosenthal
Duration: 3 hours

LAST NAME: ______________________________

FIRST NAME: ______________________________

STUDENT NUMBER: ______________________________

- There are ten questions, each of which is worth 10 marks.
- This paper has a total of 12 pages, including this cover page.
- **No calculators, scrap paper, or other aids permitted.**
- Write your answer in the space provided. Use the back sides of the pages for scrap work.
- **DO NOT tear any pages from this test.**

FOR MARKERS ONLY	
Question	Mark
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
TOTAL	

1. For each of the following congruences, either find a solution or prove that no solution exists ("solution" means "integer solution"):

   (a) $39x \equiv 13 \pmod 5$.

   $\Uparrow$

   $3x \equiv 1 \pmod 5$

   Let $x = 2$

   $3x \equiv 1 \pmod 5$.

   (b) $95x \equiv 13 \pmod 5$.

   $\Downarrow$

   $0 \equiv 3 \pmod 5$ X

   so no sol'ns.

2. For which prime numbers p is $(p-2)! \equiv 1 \pmod{p}$?
Prove that your answer is correct.

Wilson: $(p-1)! \equiv -1 \pmod{p} \quad \forall p$

$$(p-1)! = (p-2)!\,(p-1) \equiv (p-2)!\,(-1)$$

$$\Rightarrow \quad (p-2)! \equiv (-1)(-1) \equiv 1 \pmod{p}$$

3. (a) Find the remainder when 2^{923} is divided by 15.

$2^4 \equiv 16 \equiv 1 \mod 15$

Note: $920 = 4n$

so $2^{920} = (2^4)^n \equiv 1^n \equiv 1 \mod 15$

$2^3 = 8$

so $2^{923} = 2^{920} \cdot 2^3 \equiv 1 \cdot 8 \equiv 8 \mod 15$

(b) Is there a positive integer x such that $7^{kx} - 1$ is divisible by 19 for every positive integer k? Justify your answer.

Fermat's little thm $\Rightarrow$

$7^{19-1} \equiv 1 \mod 19$

$\Rightarrow$ for $x = 18$ have $7^{18} \equiv 1 \mod 19$

$\Rightarrow$ for all k: $(7^{18})^k \equiv (1)^k \equiv 1 \mod 19$

$\Rightarrow$ $7^{k \cdot 18} - 1 \equiv 0 \mod 19$ all k.

4. (a) Write the greatest common divisor of 52 and 135 as a linear combination (with integer coefficients) of 52 and 135.

$$135 = 2 \cdot 52 + 31$$
$$52 = 1 \cdot 31 + 21$$
$$31 = 1 \cdot 21 + 10$$
$$21 = 2 \cdot 10 + \boxed{1} \leftarrow \text{g.c.d.}$$
$$10 = 10 \cdot 1 + 0$$

$$1 = 21 - 2 \cdot 10 = 21 - 2(31 - 21) = 3 \cdot 21 - 2 \cdot 31$$
$$= 3(52 - 31) - 2 \cdot 31 = 3 \cdot 52 - 5 \cdot 31$$
$$= 3 \cdot 52 - 5(135 - 2 \cdot 52)$$
$$= 13 \cdot 52 - 5 \cdot 135$$

(b) Prove that $\sqrt[3]{4} + \sqrt{7}$ is irrational.

Assume: $\sqrt[3]{4} + \sqrt{7} = \frac{m}{n}$ where m, n rel. prime.

$$\sqrt[3]{4} = \frac{m}{n} - \sqrt{7}$$

$$4 = \left(\frac{m}{n} - \sqrt{7}\right)^3 = \left(\frac{m}{n}\right)^3 - 3\left(\frac{m}{n}\right)^2 \sqrt{7} + 3\left(\frac{m}{n}\right) 7 - 7\sqrt{7}$$

$$4 - \left(\frac{m}{n}\right)^3 - 21\left(\frac{m}{n}\right) = \sqrt{7}\left(-3\left(\frac{m}{n}\right)^2 - 7\right)$$

$$\underbrace{\frac{4 - \left(\frac{m}{n}\right)^3 - 21\left(\frac{m}{n}\right)}{-3\left(\frac{m}{n}\right)^2 - 7}}_{\text{rational}} = \underbrace{\sqrt{7}}_{\text{irrational}} \qquad \times$$

5. Let $\mathcal{F}$ be the smallest number field containing π. Prove that $\mathcal{F}$ is countable.

$$\mathcal{F} = \left\{ \frac{p(\pi)}{q(\pi)} \;\middle|\; p, q \text{ polyn'ls with } \mathbb{Q}\text{-coeffs.} \right\}$$

$$|\mathcal{F}| \leq \left| \{ (p,q) \mid p, q \text{ polyn'l with } \mathbb{Q}\text{-coeffs} \} \right|$$

$$= \aleph_0 \times \aleph_0 = \aleph_0$$

$\uparrow$

we know {polyn's with $\mathbb{Q}$-coeffs} is countable.

6. Let S denote the collection of all circles in the plane. What is the cardinality of S, c or 2^c? Justify your answer.

Circle $\longleftrightarrow (z, r) \qquad z \in \mathbb{C} = \mathbb{R}^2 \qquad r \geq 0$

$\{\text{circles in plane}\} \longleftrightarrow \underbrace{\mathbb{R}^2 \times \mathbb{R}_{\geq 0}}_{\text{cardinality is } = c.}$

7. Show that the set of all functions mapping $\mathbb{R} \times \mathbb{R}$ into $\mathbb{Q}$ has cardinality 2^{c}.

$S := \{ f : \mathbb{R}^2 \longrightarrow \mathbb{Q} \}$

a) $\{ f : \mathbb{R}^2 \longrightarrow \{0,1\} \} \subseteq S \Rightarrow 2^c \leq |S|$

b) $f : \mathbb{R}^2 \to \{0,1\} \longleftrightarrow \Gamma_f \subset \mathbb{R}^2 \times \mathbb{Q}$

graph of f.

so

$S \subseteq \{ \text{subsets of } \mathbb{R}^2 \times \mathbb{Q} \}$

$\Rightarrow |S| \leq 2^c.$

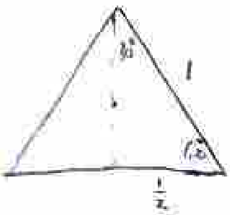
8. (a) Can the regular polygon with 36 sides be constructed with straightedge and compass? Prove that your answer is correct.

central angle = 10°

polygon constructible $\Leftrightarrow$ central angle constructible.

If 10° constructible then 20° constructible $\times$

(b) Prove the following by mathematical induction: for every integer $n \geq 2$, the regular polygon with $3 \cdot 4^n$ sides can be constructed with straightedge and compass.



constructible $\Rightarrow$ polygon with $3 \cdot 2$ constructible ($\because$ bisect)

$\Rightarrow$ polygon with $3 \cdot 2 \cdot 2$ constructible ($\because$ bisect)

- - -

9. You are receiving messages using the RSA system. You announce $N = 15$ and $e = 7$. If the encoded message you receive is 8, what was the actual message? [Anyone who knows RSA could decode the message, of course, since the numbers are so small.]

$N = 15 = 3 \cdot 5$

$\phi(N) = (3-1)(5-1) = 8$

$de + k\phi(N) = 1$

$(7)7 + (-6)8 = 1$

so $d = 7$ is O.K to use. (recall need $d > 0$ so $d = -1$ $k = 1$ not good!)

$R = 8$

$R^d = 8^7 \equiv M \mod 15$

$8^2 = 64 \equiv 4 \mod 15$

$8^4 \equiv 4^2 \equiv 1 \mod 15$

$8^7 = 8^4 \cdot 8^2 \cdot 8 \equiv 1 \cdot 4 \cdot 8 \equiv 32 \equiv 2 \mod 15$

10. (a) State whether each of the following numbers is constructible and justify your answer:

(i) $\cos\pi$ $= -1$ constructible

(ii) $\cos 60^0$

θ constructible $\Leftrightarrow$ $\cos\theta$ constructible

60° is constructible (e.g. see 8(b))

(iii) $\cos 5^0$

5° not constructible ($\because 20^\circ$ not constructible)

$\Downarrow$

$\cos 5^\circ$ not constructible.

(iv) $11^{\frac{2}{3}}$ $= x$

$$x^3 - 11^2 = 0$$

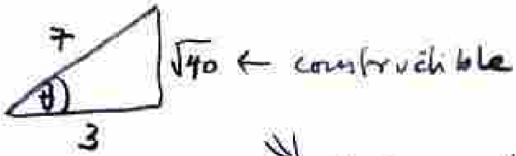
x constructible $\Rightarrow$ $x^3 - 10^2$ has rational soln $\times$

So $11^{2/3}$ not constructible.

(v) $11^{\frac{3}{2}}$ $= \sqrt{11^3}$ surd so constructible.

10. (b) Prove that the acute angle whose cosine is $\frac{3}{7}$ cannot be trisected with straightedge and compass.

$$\cos\theta = \frac{3}{7}$$



$\Rightarrow$ θ is constructible

$$\cos\theta = 4\left(\cos\frac{\theta}{3}\right)^3 - 3\left(\cos\frac{\theta}{3}\right)$$

If θ is trisectable then $\frac{\theta}{3}$ is constructible, so $\cos\frac{\theta}{3}$ is constructible

so $\frac{3}{7} = 4x^3 - 3x$ would have a constructible root

hence a rational root.

check no rational root:

$$28x^3 - 21x - 3 = 0$$

$$28\left(\frac{m}{n}\right)^3 - 21\left(\frac{m}{n}\right) - 3 = 0$$

$$28m^3 - 21mn^2 - 3n^3 = 0$$

$$\left.\begin{array}{l} m \mid 28m^3 - 21mn^2 \Rightarrow m \mid 3n^3 \underset{\text{why?}}{\Rightarrow} m \mid n \\ n \mid 21mn^2 - 3n^3 \Rightarrow n \mid 28m^3 \underset{\text{why?}}{\Rightarrow} n \mid m \end{array}\right\} \Rightarrow \frac{m}{n} = \pm 1$$

But ± 1 not a root.