Solus

THE FACULTY OF ARTS AND SCIENCE
UNIVERSITY OF TORONTO
FINAL EXAMINATIONS, APRIL/MAY 2005

MATH246Y

Concepts in Abstract Mathematics

Examiners: J. Korman and 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 14 pages, including this cover page.
- **No calculators, scrap paper, or other aids are permitted.**
- Write your answers 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	Marks
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
Total	

1. (a) Let p be a prime number. Prove that

$$1^2 2^2 3^2 \cdots (p-1)^2 - 1 \quad \equiv 0$$

is divisible by p.

Wilson: $(p-1)! \equiv -1 \mod p$

$(p-1)!^2 \equiv 1$

(b) Suppose P is a polynomial with integer coefficients, and a and m are natural numbers. Prove that $P(a+m) - P(a)$ is divisible by m.

$$\cancel{P(a+m) \equiv P(a) \mod m}$$

$$\cancel{P(a+m) - P(a) \equiv 0 \mod m}$$

$$\cancel{a+m \equiv a \mod m}$$

$$(a+m)^k \equiv a^k \mod m \qquad \forall k \in \mathbb{N}$$

$$\Rightarrow P(a+m) \equiv P(a) \mod m$$

$$\Rightarrow P(a+m) - P(a) \equiv 0 \mod m$$

2. Determine whether or not $17^{2492} + 25^{376} + 5^{782}$ is divisible by 3. Prove that your answer is correct.

~~$a^2 \equiv a \mod 3$ $\forall a$ not div. by 3~~

~~$a^{\text{even}} \equiv a$ — " —~~

~~$17 + 25 + 5 \equiv -1 + 1 + 2 \equiv 2 \mod 3$~~

~~$\Rightarrow$ Not div. by 3.~~

$a^2 \equiv 1 \mod 3$ $\forall a$ not div. by 3

$\Rightarrow a^{\text{even}} \equiv 1 \mod 3$ — " —

$1 + 1 + 1 = 3 \equiv 0 \mod 3$

so is div. by 3.

3. Find the greatest common divisor of 291 and 573 in two different ways:

(a) by using the Euclidean algorithm,

$573 = 1 \cdot 291 + 282$

$291 = 1 \cdot 282 + 9$

$282 = 31 \cdot 9 + \boxed{3}$

$9 = 3 \cdot 3 + 0$

(b) by factoring both numbers into primes.

$573 = 3 \cdot 191$

$291 = 3 \cdot 97$

4. (a) Show that the following equation has no rational solutions:

$$(x^{29}+1)^4 - (x^{29}+1) + 1 = 0.$$

If $\exists x$ rational ~~solving~~ eqn

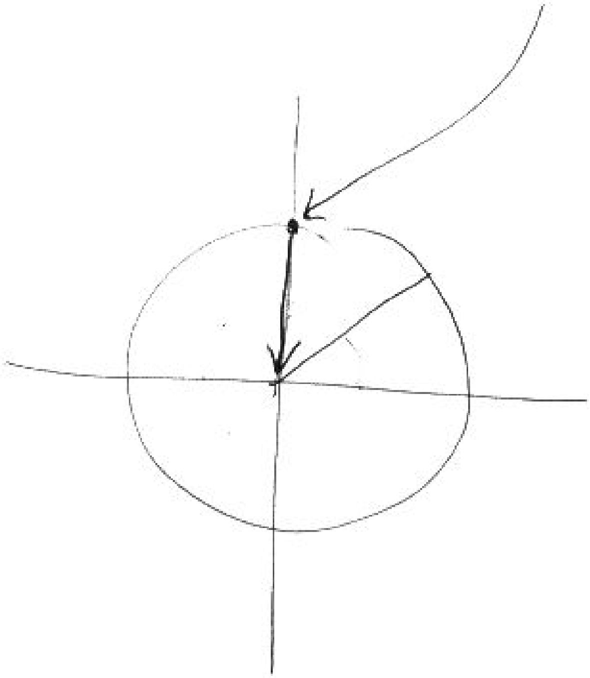
then $y = x^{29}+1$ is also ~~r~~rational and

a solⁿ of $y^4 - y + 1 = 0$

possible solns

~~[illegible]~~ no rational solns : ± 1

(b) Show that the real part of $(1+i)^{10}$ is 0.



$$1+i = e^{i\pi/4}$$

$$(1+i)^{10} = e^{i\,10\pi/4} = e^{i\pi/2} = i$$

$$Re(i) = 0$$

5. You are to receive a message using RSA system. You choose $p = 5$, $q = 7$ and $e = 5$. I send you an encoded message; the encoded version is 17. What is my actual (decoded) message ? Show all your work.

$\phi(5 \cdot 7) = 4 \cdot 6 = 24$

$e = 5$

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

$5 \cdot 5 - 1 \cdot 24 = 1$

$d = 5$

$R = 17$

$17^5 \equiv ?$ mod 35

$17^2 \equiv 9$

$9^2 \equiv 81 \equiv 11$

$17 \cdot 11 \equiv 12$

6. Find the cardinality of the set of all points in $\mathbb{R}^3$ all of whose coordinates are rational. Justify your answer.

$$|\mathbb{Q}^3| = \aleph_0$$

$$\{(x,y,z) \in \mathbb{R}^3 \mid x,y,z \in \mathbb{Q}\} = \mathbb{Q}^3$$

7. Call a complex number *complex-algebraic* if it is a root of a polynomial with integer coefficients. Prove that the set of complex-algebraic numbers is countable.

$\mathcal{A}_k = \{ z \in \mathbb{C} \mid z$ root of polyn. of deg k with integer coeffts $\}$

$\mathcal{A} = \bigcup_k \mathcal{A}_k$

$\aleph_0 = |\mathbb{Z}^{k+1}| \leq |\mathcal{A}_k| \leq |k \cdot \mathbb{Z}^{k+1}| = \aleph_0$

at least 1-root

at most k ~~roots~~ different complex roots for a poly. of deg k.

$\Rightarrow \mathcal{A}$ countable

8. Prove that the following equation has no constructible solutions:

$$x^3 - 6x + 2\sqrt{2} = 0.$$

Hint: You could use the theorem concerning roots of cubic polynomials with rational coefficients if you make an appropriate substitution.

Let ~~$x = 2y\sqrt{2}$~~ $x = y\sqrt{2}$

$$2y^3 \cancel{\sqrt{2}} - 6y\cancel{\sqrt{2}} + 2\cancel{\sqrt{2}} = 0$$

$$2y^3 - 6y + 2 = 0$$

$$(*) \quad y^3 - 3y + 1 = 0$$

x constructible $\Rightarrow$ y constructible

$\overset{\text{Thm}}{\Rightarrow}$ $(*)$ has rational root

check no rational root: ± 1

<u>Note</u>: cannot directly apply thm to eqn with irrational coeffs. as the one above

9. (a) For each of the following angles, write C if constructible, N if not constructible. There is no need to justify your answer.

10-sides polygon is constructible

$36 - 3^{\circ} \leftarrow$ constructible

C (i) 6°

$\frac{30}{4}$

C (ii) 37.5°

$30 + 7.5$

N (iii) An angle θ such that $\cos\theta = \frac{\pi}{6}$

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

$\Rightarrow$ $\cos\theta$ algebraic.

C (iv) An angle θ such that $\frac{\theta}{3}$ is constructible

$\theta = 3\left(\frac{\theta}{3}\right)$

C (v) An angle θ such that $\tan\theta = 0.1$

θ const. $\Leftrightarrow$ $\tan\theta$ is .

0.1 is rational, so constr.

(b) For each of the following numbers, write C if constructible, N if not constructible. There is no need to justify your answer.

C (i) $\cos \frac{\pi}{4}$

$\cos\theta$ const. iff θ const.

$\pi/4 = 45^\circ$ constructible.

C (ii) $\sqrt{7+\sqrt{5}}$

a surd, so const.

N (iii) $\sqrt[3]{\frac{9}{10}}$ $\qquad x^3 - 9/10 = 0$ $\qquad$ no rational roots

rationals so constr.

C (iv) $\sqrt[3]{\frac{\sqrt{2}}{4}} = \sqrt[3]{\frac{1}{\sqrt[3]{8}}} = \sqrt{2}$ $\qquad 8^{1/6}$ $\qquad \frac{\sqrt{2}}{2\cdot 2} = \frac{1}{2\sqrt{2}}$ $\qquad \sqrt{8}$

N (v) $\sqrt{(\sqrt{\pi}+1)^2 - (\sqrt{\pi}-1)^2} = 2\sqrt{\sqrt{\pi}}$ $\qquad$ transc. so not const.

$(\cancel{\pi} + 2\sqrt{\pi} \cancel{+1}) - (\cancel{\pi} - 2\sqrt{\pi} \cancel{+1})$

$4\sqrt{\pi}$

10. Let t be a transcendental number. Prove that t cannot be a root of any equation of the form

$$x^2 + ax + b = 0,$$

where a, b are constructible numbers.

$$t^2 + at + b = 0$$

$$\Rightarrow \underbrace{t}_{\text{transc.}} = \left.\frac{-a \pm \sqrt{a^2 - 4b}}{2}\right\} \text{constructible}$$

$$\Downarrow$$

algebraic.

contradiction.

<u>Note</u>: If $a^2 - 4b < 0$, the sol'n is not real and so cannot equal t ($\because$ t has to be a real number, since t is transc.)