THE FACULTY OF ARTS AND SCIENCE
University of Toronto

TERM TEST, February 27, 2013

MAT246H1S
Concepts in Abstract Mathematics

Examiner: V. Kapovitch
Duration: 1 hour 50 minutes

NO AIDS ALLOWED. **Total: 80 marks**

Family Name: QIU
(Please Print)

Given Name(s): RUI
(Please Print)

Please sign here: Rui Qiu

Student ID Number: 999292509

You may not use calculators, cell phones, or PDAs during the exam. Partial credit will be given for partially correct work. 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 MARKER'S USE ONLY	
Problem 1:	10 /10
Problem 2:	0 /15
Problem 3:	3 /10
Problem 4:	17 /20
Problem 5:	0 /10
Problem 6:	14 /15
TOTAL:	44 /80

1. (10 pts) The pigeonhole principle states that if n items are put into m pigeonholes with $n > m$, then at least one pigeonhole must contain more than one item.

   Prove the pigeonhole principle by induction in m.

Proof: Let S be a set of any natural number that can be the m that satisfies the pigeonhole principle.

(Base Case) When $m=1$, all the n items can only be put into one same pigeonhole, so the principle holds automatically. Hence 1 is in S.

(inductive hypothesis) Suppose $m=k$, $k \in S$.
i.e. for k pigeonholes and n items, $n>k$, the pigeonhole principle still holds.
Then we want to show $k+1 \in S$ (it holds for $k+1$)

(inductive step). Then we have $k+1$ pigeonholes and n items
Since the principle holds for k, after putting one each in k pigeonholes, we still have $n-k$ items left.
As $k+1<n$, $n-k>1$
So for $k+1$ pigeonholes, although we have one more pigeonhole than k (last case), we cannot put all the items left into this only pigeonhole because $n-k>1$.
Therefore, the pigeonhole principles holds for $k+1$.
Then $k+1 \in S$.

Conclusion: If n items are put into m pigeonholes with $n>m$, then at least one pigeonhole must contain more than one item. ∎

Awesome! That was very clear!

2. (15 pts) Let a, b be relatively prime natural numbers bigger than 1.
Prove that

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$$

Hint: Use that $gcd(a, b)$ can be written as $gcd(a, b) = ax + by$ for some integer x and y.

Proof: According to Euler's Theorem
for a, b which are relatively prime natural numbers
bigger than 1. then $\gcd(a,b)=1 = ax+by$ for some $x, y \in \mathbb{Z}$

$a^{\varphi(b)} \equiv 1 \bmod b \equiv 1 \bmod ab$
$b^{\varphi(a)} \equiv 1 \bmod a \equiv 1 \bmod ab$?!

~~Then $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1+1 \bmod ab$~~
~~$\equiv (\gcd(a,b) \times 2) \bmod ab$~~
~~$\equiv 2ax+by \bmod ab$~~
~~=~~

The idea is like this:

Write out the whole idea.

This seems like the wrong idea.

$a^{\varphi(b)} + b^{\varphi(a)}$
$\equiv by + 1 + ax + 1$
$\equiv (\quad)^{\varphi(ab)} \bmod ab$ (By Euler's Thm)
$\equiv 1 \bmod ab$

Solution
Since $\gcd(a,b)=1$, $\exists x, y \in \mathbb{Z}$ such that $ax+by=1$
By Euler's thm $a^{\varphi(b)} \equiv 1 \bmod b$. Therefore $a^{\varphi(b)} \equiv 1-kb \pmod b$ for any $k \in \mathbb{Z}$
In particular $a^{\varphi(b)} \equiv 1-yb \pmod b$.
But $1-yb = xa \equiv 0 \bmod (a)$
Therefore $a^{\varphi(b)} - (1-yb) = a^{\varphi(b)} - xa \equiv 0 \bmod a$
Thus $a \mid a^{\varphi(b)} - (1-yb)$ and $b \mid a^{\varphi(b)} - (1-yb)$ and hence
$ab \mid a^{\varphi(b)} - (1-yb)$ since $\gcd(a,b)=1$
i.e. $a^{\varphi(b)} \equiv 1-yb \pmod{ab}$
Similarly $b^{\varphi(a)} \equiv 1-xa \pmod{ab}$
Then $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1-yb+1-xa \equiv 2-1 \equiv 1 \bmod ab$

3. (10 pts) Let $n \geq 2$ be a composite number.
Prove that there exists a prime number $p \leq \sqrt{n}$ which divides n.

Proof: Let $n = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \geq 2$, p_i is prime, k_i is natural. $i \in N^+$

Since n is composite ($n \geq 2$)

① If n is even then it has a prime factor 2.
such that even for the smallest composite 4,
$2 \leq \sqrt{4} = 2$ verified
Then for large even composite numbers, 2 is such p.
$2 \leq \sqrt{n}$ since $n > 4$

② If n is a perfect square ($n \geq 2$) 36 is a perfect square
Then $n = (p^k)^2$ by definition, $\sqrt{36} = 6 = 2 \cdot 3$
So $p = \sqrt[2k]{n} \leq \sqrt{n}$ verified. ↑ Not a prime power.
Why is this prime? (odd, but not perfect square)

③ If n is other composite

$\sqrt{n} = p_1^{k_1/2} p_2^{k_2/2} \cdots p_n^{k_n/2}$

If any $k_i \geq 2$, then the corresponding p_i is such p
that $p_i = p_i^{k_i/2} \leq \sqrt{n}$.
confusing

Solution: A composite number contains at least 2 prime factors.
Therefore $n = pqc$ where p, q are prime and $c \geq 1$. assume $p \leq q$
Therefore $n = pqc \geq pq \geq p^2$
Hence $\sqrt{n} \geq p$

4. (a) (20 pts) Let $p > 1$ be a prime number.
Find $2^{(p!)^2} \pmod p$.

What if $p=2$?

Solution: 2 is prime. p is prime. then $\gcd(2,p)=1$

By Euler's Thm $2^{\varphi(p)} = 2^{(p-1)} \equiv 1 \bmod p$

$$2^{(p!)^2} \equiv 2^{((p-1)!p)^2} \equiv (2^{(p-1)!})^{(p-1)!p^2} \bmod p$$
$$\equiv 1^{(p-1)!p^2} \bmod p$$
$$\equiv 1 \bmod p$$

7/10

We have 2 situations.
① $\gcd(2,p)=1$
② $\gcd(2,2)=2$
here $p=2$.

(b) Find $(26!)^{143} \pmod{29}$. 29 is prime.

Solution: By Wilson's Thm,
$(29-1)! \equiv -1 \bmod 29$
$26! \times 27 \times 28 \equiv -1 \bmod 29$
$26! \times (-2) \times (-1) \equiv -1 \bmod 29$
$26! \times 2 \equiv 28 \bmod 29$
$26! \equiv 14 \bmod 29$
Then $(26!)^{143} \equiv 14^{143} \bmod 29$
Since $14^{28} \equiv 1 \bmod 29$ (By Euler's thm, $\gcd(14,29)=1$)
So $(26!)^{143} \equiv 14^{143} \equiv 14^{28\times 5+3} \bmod 29$
$\equiv 1^5 \cdot 14^3 \bmod 29$
$\equiv 18 \bmod 29$.

(c) Find $2^{3^{101}} \pmod{15}$

Solution: Since $\gcd(2,15)=1$.

By Euler's Thm:

$$2^{\varphi(15)} \equiv 2^{(3-1)(5-1)} \equiv 2^8 \equiv 1 \bmod 15$$

Again, since $\gcd(8,3)=1$.

By Euler's Thm

$$3^{\varphi(8)} \equiv 3^{(2^3-2^2)} \equiv 3^4 \equiv 1 \bmod 8$$

Therefore $3^{101} \bmod 8 \equiv 3^{4\times 25+1} \bmod 8$

$$\equiv (3^4)^{25} \cdot 3 \bmod 8$$

$$\equiv 1^{25} \cdot 3 \bmod 8$$

$$\equiv 3 \bmod 8$$

Then $2^{3^{101}} \equiv 2^{8k+3} \bmod 15$ for a certain integer k.

Therefore $2^{3^{101}} \equiv 2^{8k+3}$

$$\equiv (2^8)^k \cdot 2^3 \bmod 15$$

$$\equiv 1^k \cdot 8 \bmod 15$$

$$\equiv 8 \bmod 15$$

✓

5. (10 pts) Let n be a natural number. Prove that $\sqrt[10]{n}$ is rational if and only if n is a complete 10th power, i.e. $n = m^{10}$ for some natural number m.

Proof: $\Rightarrow$ Suppose $\sqrt[10]{n}$ is rational. say $\sqrt[10]{n} = \frac{p}{q}$ for p, q are relatively prime natural numbers

Then $(\sqrt[10]{n})^{10} = n = \frac{p^{10}}{q^{10}}$

Since n is a natural number. then $q = 1$

$n = p^{10}$

Hence n is a complete 10th power

Note that I used p instead of m in this proof.

That's fine.

$\frac{6}{3}$?

$(\Leftarrow)$ Suppose n is complete 10th power $\Leftrightarrow n = k^{10}, k \in \mathbb{Z}$

Then $n = \frac{p^{10}}{q^{10}}$ for $p, q \in \mathbb{N}^+$, $\gcd(p, q) = 1$

Therefore $\sqrt[10]{n} = \sqrt[10]{\frac{p^{10}}{q^{10}}} = \frac{p}{q}$

Since p, q are natural,

then $\frac{p}{q}$ is rational

Therefore $\sqrt[10]{n}$ is rational. $\sqrt[10]{n} = m$

Solution: If $n = m^{10}$ is a complete 10th power then $\sqrt[10]{n}$ is rational (obviously)

Conversely. sps $\sqrt[10]{n}$ is rational. Then $\sqrt[10]{n} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$.

Then $\frac{p}{q}$ is a rational solution of the equation $x^{10} - m = 0$.

Since $\gcd(p, q) = 1$

By the Rational Root thm $\Rightarrow p \mid n$ & $q \mid 1$.

Therefore $q = \pm 1$ & $\frac{p}{q} = m$ is an actual integer.

hence

This means $n = (\frac{p}{q})^{10} = m^{10}$ is a complete 10th power.

6. (15 pts) Let $p = 11, q = 3$ and $E = 13$. Let $N = 11 \cdot 3 = 33$. The receiver broadcasts the numbers $N = 33, E = 13$. The sender wants to send a secret message M to the receiver using RSA encryption. What is sent is the number $R = 2$.

   Decode the original message M.

Solution: We need to find the decoder D s.t.

$$DE \equiv 1 \bmod \varphi(N)$$

i.e. $13D \equiv 1 \bmod (11-1)(3-1)$

$\equiv 1 \bmod 20$

Try some D with last digit 7 we can easily find out $13 \times 17 = 221 \equiv 1 \bmod 20$.

Hence $D = 17$.

Then $M \equiv R^D \bmod N$

$\equiv 2^{17} \bmod 33$

Since $2^5 \equiv 32 \equiv -1 \bmod 33$

So $M \equiv 2^{17} \bmod 33 \equiv 2^{5\times 3+2} \bmod 33$

$\equiv (-1)^3 \times 2^2 \bmod 33$

$\equiv -4 \bmod 33$

So the original message M is 4.

Check: $M^E \bmod N \equiv 4^{13} \bmod 33$

$= 2^{26} \bmod 33$

$\equiv (2^5)^5 \cdot 2 \bmod 33$

$\equiv 2 \bmod 33$ verified.